

UNBREAKABLE:

Designing for Trustworthiness in Private Messaging

October 2022



Dalberg

SUPPORTED BY

ON OMIDYAR NETWORK™

Executive Summary



INTRODUCTION

Private messaging platforms like WhatsApp, Signal and Telegram have become an integral part of our day-to-day lives and yet much of what is shared remains private when compared with open forums on the internet.

We know that these private messaging platforms have a profound impact on our digital behavior and emotional well-being, yet it is hard to step back and see the forest for the trees given their ubiquitous nature. While these platforms play an essential role in securing our privacy, they also expose users to a range of risks that undermine their sense of security and trust. This undermining of trust can affect their perceptions of peer platform users, corporations and even governments. We each have our own personal and evolving opinions about how private messaging platforms can be made more trustworthy based on our lived experience, whether through better design choices, more comprehensible policies or more transparent governance models.



"I no longer go by my old name, just because the internet is a place. You can't search me by my documented name, it's a decision I made long ago. Also weary about sharing photos and geotagging, I no longer post often as I used to. I try to keep my face hidden to strangers and mostly identifiable to family."



"I follow up with a phone conversation and see how true it is or go online to verify that story before I choose to re-broadcast it. But in some cases, many people don't verify, they just repost and repost and it causes panic and in a few hours they find out it's fake."



"Sometimes, especially when counseling, the information shared (with me) is very sensitive. For instance, if you are doing counseling and you (message someone that they) should separate from their husband, this (message) is sensitive and you need security."

It's not often we get to hear directly from a diverse cross-section of users spanning geographies about their lived experiences of private messaging platforms. That is the purpose of this research: to both share a cross-cutting view of the experiences and concerns of a diverse range of users – and to connect the dots back to specific design decisions that platform providers should make to improve trustworthiness.

Over the course of ten weeks, our team engaged a total of 185 diverse participants from Colombia, Nigeria and the US. While we have drawn our own conclusions in this report, **we hope that this research can serve as a resource to many different stakeholders as they consider ways that the design of these platforms can be improved, including:**

1 // Platform owners and providers: To negotiate competing product priorities and adjust product planning to address user concerns and diminishing perceptions of trust within messaging experiences.

2 // Policymakers: To better assess the risks that matter to residents and citizens related to security, democracy, and information integrity, understand and prioritize the harms that occur on private messaging platforms, and inform meaningful policy solutions.

3 // Advocacy, Civil society: To buffer advocacy efforts with data points and anecdotal evidence of the harms a diverse set of global users experience on private messaging platforms and examples of concrete changes that could improve trustworthiness.

4 // Researchers: To equip the trust and safety research field with actionable user-centered data, and offer a blueprint for mixed methods methodologies focused on user experiences of private messaging platforms. Researchers have the opportunity to replicate this approach in other markets and with other communities to further quantify these harms.

5 // UX designers: To augment their own user research and data analytics, and influence product priorities in line with user trustworthiness.

6 // Platform value chain players & governments offering services on private messaging platforms: To assess the potential impact of user concerns on the trustworthiness of services they offer on private messaging platforms. User perceptions of private messaging platform trustworthiness will shape their trust in services offered by governments and other value chain players on private messaging platforms, as we have seen during the pandemic. A lack of trust will likely lead to less engagement with both the messaging platforms and corresponding services offered on top.

FINDINGS

Since these markets are distinct and individual journeys within private messaging platforms are personal, there is always a risk of generalization when attempting to summarize this sort of user experience research. Nonetheless, there are some common patterns that seem to transcend these differences:

A// We found that people across very different markets have become incredibly sophisticated in how they understand and navigate the intricacies of these platforms.

Across geographies, most users have built up fairly complex ways of engaging and adapting to risks and concerns as they perceive them (for ex: switching into airplane mode so that other users won't be able to tell if they have read their messages). This finding in particular calls into question the assumption that people are not likely to adjust their preferences even if these options were made more easily accessible. Even with insufficient features, people are finding a myriad of workarounds to address gaps and minimize shortcomings.

B// Heightened perception of risk generally arises in response to specific situations, not all of which can be attributed entirely to the platform providers themselves.

The risks that are most top of mind vary by market (e.g., in Nigeria, it was fraud. In the US, it was corporate surveillance). While private messaging platforms are responsible for some of the vulnerabilities and design gaps which make the risks more likely to materialize into harm, some factors leading to risks – for instance, cultural norms or existence of bad actors – are not fully preventable by messaging service providers. Still, because platform design and governance can enable and exacerbate these harms, platform providers have a responsibility

to both understand them and take steps to mitigate them. Given these complexities, users generally do not have a full understanding of where to direct or who to attribute their concerns to. Often, they take on a sense of responsibility for themselves ("I should have known better") so their response choices bear little connection to the risk itself, and tend to fade over time. Regardless, perceptions of trust in messaging platforms change rapidly and irreversibly in response to these acute situations.

C// Users also face a huge gap in terms of recourse and redress, which is a critical element of trustworthiness.

The platforms themselves do not offer many clear affordances for seeking redress, particularly affordances that do not come with some reciprocal social costs (flagging another person's bad behavior or misinformation often leaves users more vulnerable to harassment).

D// Most users do not feel that they have real choice and can "venue-shop" based on personal preferences.

Even those with heightened awareness (human rights activists, for example) or high levels of technical knowledge find it practically challenging to avoid defaulting to the most common and pervasive platforms (WhatsApp in most cases). Because of this, choice alone cannot be held up as the silver bullet for ensuring better practices in the messaging platform market. While it's critical that new entrants prioritize trustworthy and safe platform design, existing platforms also need to take user concerns seriously and commit to enhancing trustworthiness with, inter alia, their design choices.

APPROACH

The user experience of platforms like WhatsApp have become second nature to users in Colombia, Nigeria and the US. The design choices of platform providers are something users work around every day, sometimes unaware of how they shape both their personal behavior and that of others, as well as their very expectations of what private messaging platforms can and should be. Human-Centered Design (HCD) approaches help us to make apparent dynamics and behaviors that are latent or under the surface.

For this reason, it was critical that we take a participatory, Human-Centered Design (HCD) approach to pierce this veil and bring forward the voices and cross-cutting concerns of private messaging platform users. What risks are they most aware of when using messaging platforms? Where and how do these risks show up in their day-to-day behavior? Who do they hold responsible, and do they feel that they have any opportunity for recourse or redress? What choices and tradeoffs are they comfortable making to safeguard their data privacy and security and where do they feel powerless?

To gain insight into these questions, our team engaged a total of 185 participants over the course of 10 weeks. We met with ecosystem experts from several countries in the context of co-creation workshops, and community leaders and platform users in 1-on-1 and small group discussions in Colombia, Nigeria and the US.

All sessions were conducted remotely due to COVID-19 except for the community-led sessions. A breakdown of our research is as follows:



Colombia
50 total participants,

- 10 in depth 1:1 remote sessions,
- 9 remote small group discussions,
- 31 in person interviews led by community leaders



Nigeria
64 total participants,

- 10 in depth 1:1 remote sessions,
- 4 remote small group discussions,
- 42 in person interviews led by community leaders



USA
54 total participants,

- 10 in depth 1:1 remote sessions,
- 4 remote small group discussions,
- 32 in person interviews led by community leaders

CONCLUSION

There is much that private messaging platform providers can do differently if they choose to prioritize trustworthiness in platform design. User choice is not a sufficient excuse to justify the current shortcomings. Our research suggested that few users feel that they have real choice in the market despite the availability of multiple private messaging platforms.

Pointing to the retention and engagement of users as a sign that they are satisfied with current interaction models and tradeoffs does not ring true. We heard consistently that the tradeoffs of leaving a dominant environment, – WhatsApp in most cases, – are incredibly daunting for all users, even the most security-conscious like human rights activists. Platform providers have a long way to go in bettering the design of their services, (though we are seeing discrete instances of intentional trustworthy design with recent changes by WhatsApp that allow users to leave group chats without alerting others, for example). We would also encourage private messaging service providers to be transparent in how they engage users in regular cycles of feedback using the sort of methods we employed for our research study – not just analyze user data behind closed walls.

The dialogue around trustworthiness has remained at a theoretical level for too long. We hope these findings will help those advocating for change (whether policymakers, researchers or activists) point to real and concrete design choices that can increase

REPORT CONTENTS

In such opaque and highly personal environments, how might we better understand opportunities to intervene to address a set of common concerns? What would a better experience look like? To fill in that picture, this report breaks down what we heard into the following areas of analysis:

- **EXPERIENCES:** It is critical to first contextualize these findings within a holistic view of people’s everyday experiences and patterns of behavior on private messaging platforms. This report shares three sets of representative experiences from each market we looked at as a way of highlighting commonalities and differences from user perspectives.
- **HARMS:** We identified the key risks leading to various harms that are most important to users across the three markets and are likely to have the biggest impact on their sense of trustworthiness. Any future design improvements should start by prioritizing the risks that are most important to the users themselves.
- **GAPS:** The lack of mental models (other than text messaging) for how private messaging platforms work creates many gaps for users as they navigate risks and experiences of harm. Users lack supporting resources to evaluate and attribute their growing sense of concern. Who should they trust (their group admin? WhatsApp customer support?) when they encounter these gaps? In most cases the platforms provide few paths to recourse in the moment and little to no feedback to understand how their concerns might be resolved.
- **DESIGN OPPORTUNITIES:** What can design really accomplish to minimize these risks, fill in these gaps and build trust once it is lost? Our research identified many pressing concerns regarding trustworthiness related to common elements of private messaging platform design, such as: group dynamics, misinformation and generalized anxiety relating to mental health. In each case, it is not hard to begin to see a path to provide users with better tools to manage risk and make informed choices – a number of which we illustrate with sample designs that were prototyped and tested with users to further inspire change. These designs are not prescriptive: they are meant to be representative of how a private messaging platform provider MIGHT address a specific gap or design opportunity. We recognize that any design changes are likely to come with tradeoffs and potentially impact business goals related to customer growth and engagement. **Some key areas where users responded most positively to potential design improvements include:**

- **Securing and/or modifying account information**
- **Providing accessible & tailored security & privacy controls**
- **Providing support mechanisms & emergency controls**
- **Improving verification & permission mechanisms**
- **Improving administrative & management tools**

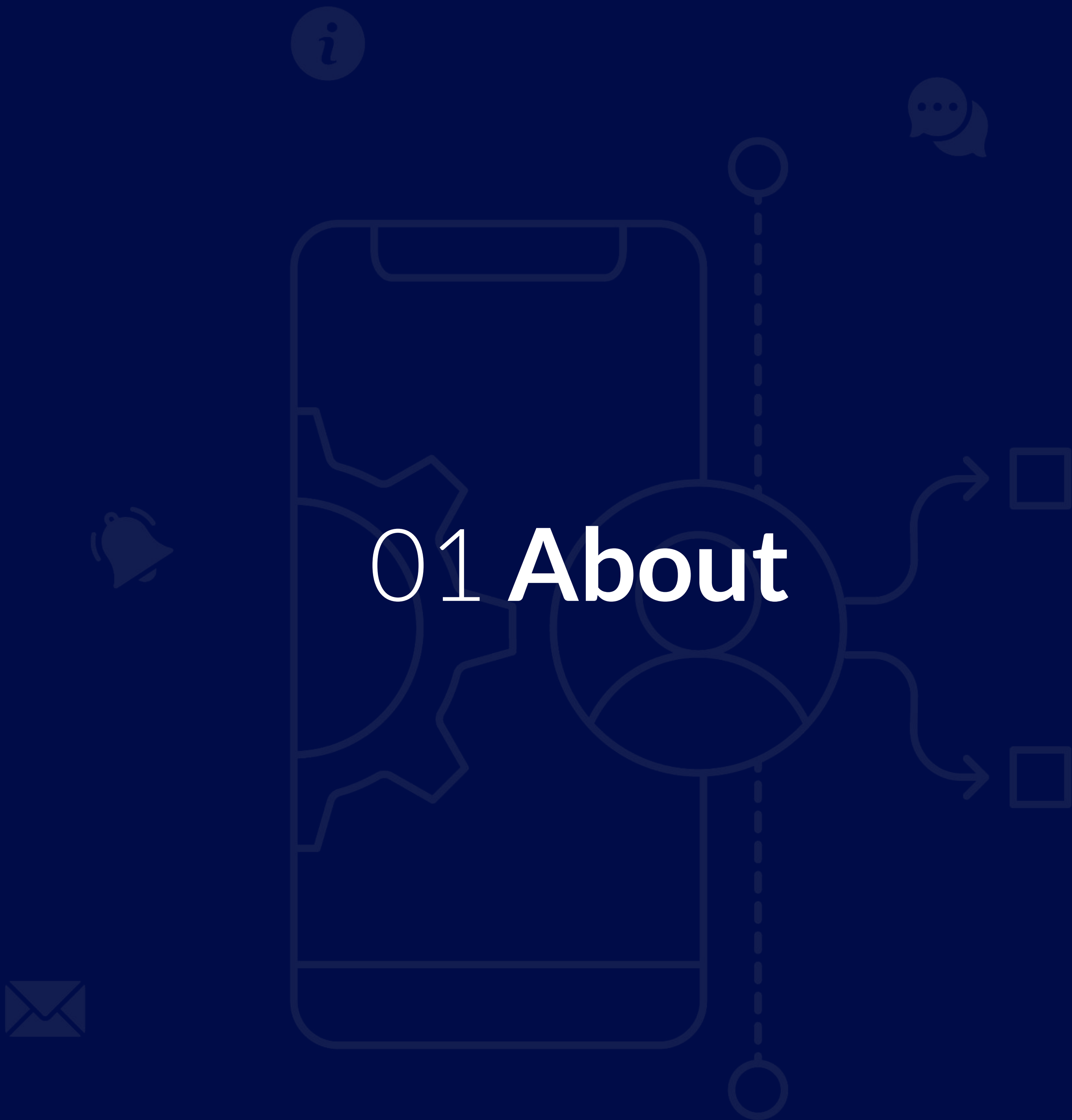
trustworthiness on private messaging platforms. We also hope this research offers stakeholders a provocation to consider more fundamental changes to the environments in which these platforms operate, whether it be business models or interoperability standards. In that sense, these recommendations are complementary to a number of related initiatives for fighting disinformation and dangerous speech on private messaging platforms – including research, technical partnerships, dialogue and convening with policymakers and technology leaders, and public advocacy — and should be seen as an integrated part of this broader effort.

The most distinctive outputs of this study– concrete, user-informed design recommendations – are just a starting point. To some, our design recommendations might seem incremental in the face of the scale and severity of user risks and concerns experienced on private messaging platforms. These recommendations do not point to a comprehensive end state which, if implemented, would satisfy all user needs and address all experiences of harm. Instead, the design recommendations in this report can provide a path towards beginning to address these harms if they are implemented within a user-centered and iterative process. They can help pave the way for a more trustworthy messaging future.

Table of contents

01 About	5
02 Country Insights	7
03 Harms	24
04 Design Opportunities	51
05 Approach	74

01 About



Project overview



“I no longer go by my old name, just because the internet is a s— place. you can't search me by my document name, it's a decision I made long ago. Also weary about sharing photos and geotagging, I no longer post often as I used to. I try to keep my face hidden to strangers and mostly identifiable to family.”

In the digital realm, end-to-end private messaging plays an important role in upholding individual rights to privacy and free speech. Platforms like WhatsApp and Signal allow residents to communicate with each other without the fear of governments, advertisers, or even snooping family members listening in or moderating the content of their communication. But these digital environments are not without many harms that undermine end user trustworthiness. Given their widespread adoption, it is critical that platform providers prioritize design choices that strengthen, not undermine, trust. That sounds great in principle, but where should they turn for guidance?

The goal of this report is to share design opportunities that address harms that exist on private messaging apps and matter the most to a globally diverse selection of individuals. These design opportunities aim to enhance individual experience to provide a safer and secure messaging environment.

What is at stake? For participants, private messaging can deliver offensive and inappropriate content, it can channel disinformation and “fake news”, and it can be used by nefarious actors to defraud unsophisticated or unsuspecting individuals. For example, our research reveals the rampant cases of hacking and scamming in both Nigeria and Colombia leading participants to look for alternative options (e.g., 3rd party apps) to protecting their accounts and verifying unknown contacts, even though these 3rd party apps compromise their privacy and security.

Platform providers may be tempted to view widespread adoption and high levels of engagement by individuals and groups as a reason to feel confident in current design choices. But our research participants are deeply concerned about their level of dependence on messaging services and their lack of control over the experiences within these messaging environments. Encryption alone does not confer a sense of safety and security, as it is poorly understood by almost everyone we spoke with. Participants are unsure of whom to trust – even scrutinizing the statements and reported behavior of senior executives like Mark Zuckerberg (Meta Platforms) or Pavel Durov (Telegram Messenger) as proxies for the relative integrity of Whatsapp or Telegram. It is only by investing in more effective and better-informed design choices that providers can help individuals and groups manage the risks inherent in these platforms; and work together to create chat environments that are safe, supportive and responsive to our changing needs.

This research looked to surface and test a preliminary set of design solutions that are likely to reduce the deleterious potential of private messaging platforms. As civil society organizations continue to push for more responsible technology, we hope our findings can be used by private messaging providers and other third-party players to build on the emerging ideas and test and implement potential solutions. While we do not expect our work to be the end-point in designing the right answer, we do hope it is an important step in that direction.



02 Country Insights

Country insights



Through our in-depth one-on-one sessions and small group discussions with participants in Nigeria, Colombia and the United States, we identified three main user archetypes in each country to communicate important individual preferences, behaviors and practices when using private messaging apps. These archetypes are by no means comprehensive, however, they highlight some important factors which can be used as a foundation to explore relevant gaps in addressing individual needs.

Below is a breakdown of the archetypes for each of the three countries:

Nigeria



1. Authoritative Admin

This archetype comprises administrators who are trusted by group members, seen as a point of authority and expected to resolve most group issues. This soft power, along with the ability on private messaging apps to add and remove participants; review and remove content; as well as make key decisions about group interactions and content that is allowed, empowers them to become dominant figures.



2. Citizen Journalist

This archetype comprises individuals who heavily depend on private messaging apps to share critical public/emergency information with others and to highlight important events that are unfolding and may not be available on mainstream media channels.



3. Low Tech Influencers

This archetype comprises traditional influencers (e.g., religious/community leaders) who typically rely on physical interactions with followers but are now moving their engagements/interactions to digital platforms for ease and wider reach.

United States



1. Advantaged Activist

This archetype comprises individuals who use private messaging apps for social and political activism. This group tends to have access to important support structures for information, and safer privacy and security practices, as well as the availability of different private messaging app options for more safer and private communications.



2. Globe Trotter

This archetype comprises individuals who conduct frequent international communications across multiple private messaging platforms (e.g., frequent travelers, international students).



3. Ceremonial Admin

This archetype comprises individuals who are admins in groups of larger than 100. They are viewed as regular members by other group participants and usually not expected to moderate interactions or make key group decisions (e.g., removal and reviewing of content).

Colombia



1. Concerned Activist

This archetype comprises activists in Colombia who have limited alternatives to dominant private messaging apps, and face increasing risks due to their activism and limited safety options (e.g., legal protection, effective safety practices) to leverage in order to counter growing risks (e.g., surveillance, hacking etc).



2. At Risk Adolescent

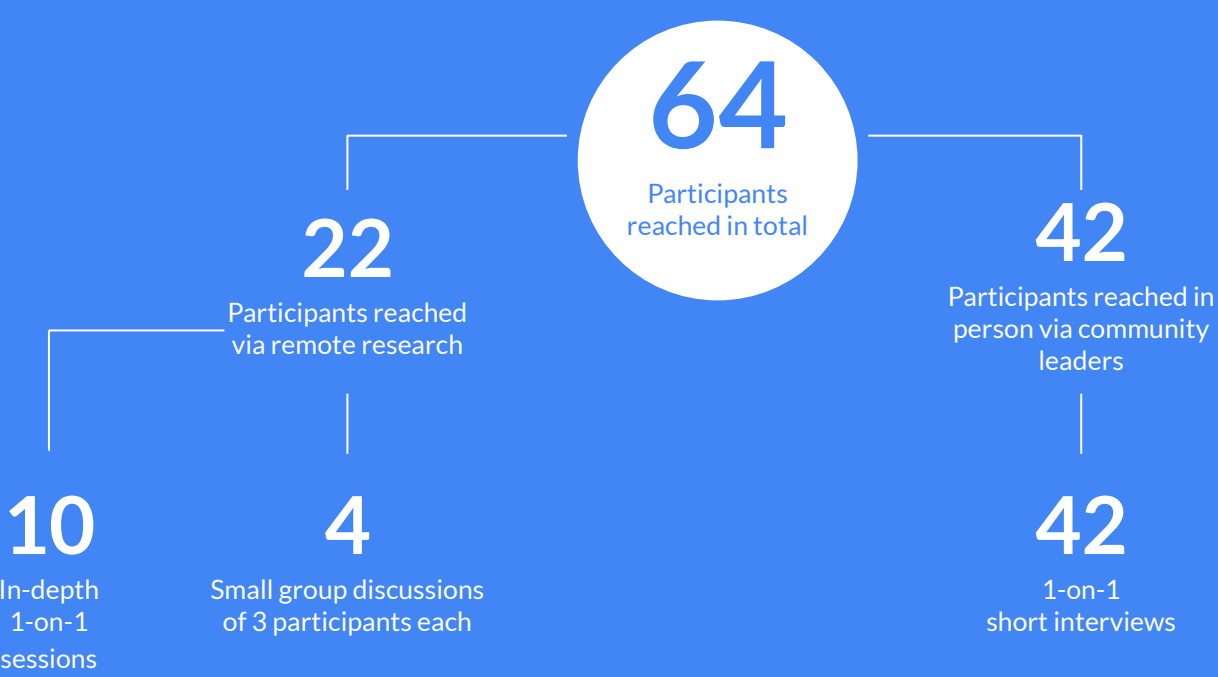
This archetype comprises individuals who are below legal adult age or who have recently become adults. This group faces particular challenges due to their susceptibility, and limited awareness/knowledge of risks as well as limited safety options to mitigate these risks.



3. Low Tech Entrepreneur

This archetype comprises entrepreneurs (e.g., transport service, plumbing) who have started to significantly leverage private messaging apps for communications and operations but have limited know-how of how to effectively use private messaging platforms to safeguard their businesses from hacking while maximizing communications.

Nigeria



The Nigerian Context

Nigeria has a population of 216 million¹ of which about 51% access the internet through mobile devices, as of the beginning of 2022.² It is a multi-ethnic and culturally diverse country with strong collective bonds. This general social context manifested in a stronger short and long-term commitment to membership within ‘groups’ at various levels of society³ relative to the other two countries studied, and as reported by our research participants. These foundational values and beliefs directly influence the approach, usage and mental models of the majority of the private messaging app users in Nigeria.

Currently, the private messaging market in Nigeria is dominated by WhatsApp, with a 91.9% penetration as of mid 2021 among private messaging platform users.² Our research suggests that the majority of private messaging communications tend to happen in group spaces (compared to P2P) with members entrusting group admins with a great deal of authority to manage and make important decisions in the best interest of the group.

Adoption and usage of messaging apps in Nigeria

WhatsApp is the most common private messaging platform in Nigeria. It is especially popular for a range of individuals, such as community workers, parents of international students, religious leaders and young adults. Adoption of WhatsApp in Nigeria is driven by its popularity among individuals’ social circles as well as the low cost of communication due to affordable mobile data, compared to regular calls and SMS, for both business and personal use. Our research also suggests that the adoption and use of Telegram is on the rise, especially with tech enthusiasts, and for use by groups of 300+ members.

Private messaging in Nigeria is commonly used for:

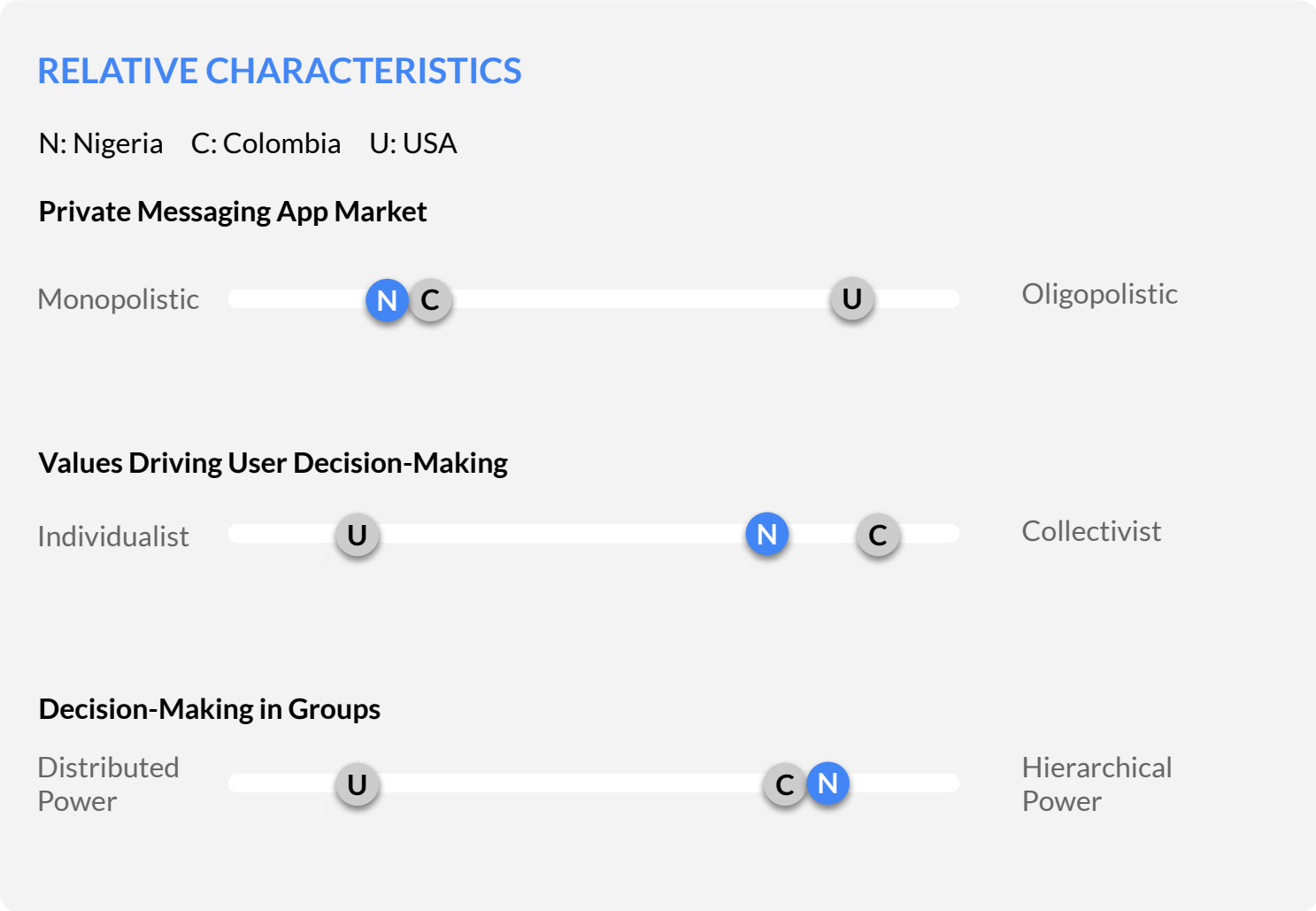
- In-country and cross-border communications
- Business/work communications tool
- Marketing and outreach
- Reporting of emergencies/breaking news, especially for communities living in conflict regions
- Social political organizing
- Entertainment
- Training and educational content
- Socializing and entertainment via status and story updates

Perceptions and concerns about privacy and security

Due to widespread cases of hacking of accounts and increases in emergency scams, participants in Nigeria were acutely worried about their security. They reported that they were less worried about their privacy with respect to surveillance and data mining, whether by governments or corporations. Although, some individuals were also strongly concerned about other factors that might infringe on their privacy including: spamming, exposure to graphic/offensive content, and misinformation.

Most participants expressed gratitude for the benefits that private messaging apps (WhatsApp mainly) brought (e.g., connecting with family that’s far away or in conflict zones, promoting work). Still, the following three concerns were commonly mentioned by the participants we spoke to:

- Hacking and scamming related to their accounts (e.g., cloning of private messaging apps account)
- Spamming or exposure to offensive/ graphic content (e.g., violence, pornography)
- Quick circulation of erroneous or deceiving information (e.g., false emergency reports on WhatsApp stories)



Sources: [1] WorldBank [2] Statista [3] Hofstede insights

Representative archetypes in Nigeria

The participants we interviewed in Nigeria exhibited some overall commonalities regarding their mental models, usage behaviors and choice of private messaging platform. This was likely influenced by cultural and societal values and beliefs. But we also observed meaningful differences based on personal experience. We selected three archetypes in Nigeria, to represent the different behavioral and social influencing factors to the adoption and usage of private messaging platforms which emerged from our research.



Authoritative Admin

This archetype comprises administrators who are trusted by group members, seen as a point of authority and expected to resolve most group issues. This soft power, along with the ability on private messaging apps to add and remove participants; review and remove content; as well as make key decisions about group interactions and content that is allowed, empowers them to become dominant figures.



Citizen Journalist

This archetype comprises individuals who heavily depend on private messaging apps to share critical public/emergency information with others and to highlight important events that are unfolding and may not be available on mainstream media channels.



Low Tech Influencers

This archetype comprises traditional influencers (e.g., religious/community leaders) who typically rely on physical interactions with followers but are now moving their engagements/interactions to digital platforms for ease and wider reach.

Authoritative Admin

Meet Blessing

Blessing is passionate about educating and empowering youth. She believes technology has the potential to unlock opportunities for young people. However, she is concerned about the growing threats and risks in the digital space in Nigeria.



Blessing’s story

Blessing is a 34-year-old female photojournalist and educator. She lives in Abuja, Nigeria, where she runs a foundation that is primarily focused on education and social impact among youth and children. She uses WhatsApp, Telegram, Discord and Zoom to communicate, conduct training sessions as well as community outreach. Blessing is also the admin of several groups on private messaging platforms. As an admin she is seen as a point of authority and is expected by group members to resolve disputes and address misbehavior and serve the best interests of the group.

“ One of the main things I'm interested in is education, especially for children in underserved communities. I take pictures to tell their stories. [through public spaces on private messaging apps, e.g., status/stories, groups]

“ During the lockdown, we used Discord a lot because the children had laptops and tablets. It helped disseminate the info we wanted them to know... [using discord], they could do their projects and they could send it back on files.

Online interactions through private messaging has become a very important part of her day-to-day community engagement, especially with the significant limitation of in-person interactions due to the Covid-19 pandemic, and the high adoption of private messaging platforms by Nigerian youth. Her use of private messaging apps has evolved from pure communications, to running training sessions, organizing outreach programs and distributing program information such as photographs across several groups on different platforms. This has also brought significant challenges to her in managing these interactions across several groups and different messaging platforms.

ABOUT BLESSING

Conforming to groups

(e.g., thinking, practices)

MODERATE

Comfort with technology

(e.g., use of private messaging platforms)

HIGH

Privacy & security vulnerability

HIGH

Perceived exposure to risks

HIGH

Challenges & concerns

Due to the increase in hacking of private messaging platforms and social media accounts in Nigeria, Blessing is concerned not only about her safety but also the safety and privacy of her students, especially in the group spaces on private messaging platforms. Personally, she has activated two-step authentication for her private messaging platforms accounts to prevent unauthorized access, although she admits that it’s not 100% secure.

Related Global Harms

- Vulnerability to targeted harassment for youth and young adults [view harm](#)
- Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment [view harm](#)
- Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content [view harm](#)

Needs

Blessing feels a lot of pressure as her role comes with a huge responsibility to manage group affairs and she is often expected to resolve contentious issues as well as taking action on members who misbehave in the group. She wishes for more streamlined options that would allow her to act on group issues (e.g., misbehavior, conflicts, suspicious links) and maintain a positive discourse in group spaces.

Related Global Design Opportunities

- Improving administrative & management tools (e.g., verification of unknown hyperlinks, protection of copyrighted images, Group restriction options ‘e.g., message forwarding & screenshots’) [view design opportunity](#)
- Providing support mechanisms & emergency controls (e.g., new contact verification options) [view design opportunity](#)

Citizen Journalist

Meet Victor

Victor is a community leader who places the best interests of his community at the center of his work. He relies on private messaging apps to connect with community members and distribute critical information on an urgent basis. At the same time, he is also concerned that these private messaging platforms have become important communication tools for individuals who cause instability in his region.



Victor’s story

Victor is a 38-year-old development manager and community leader. He resides in northern Nigeria, where he works with religious and refugee organizations in remote areas in assisting locals in empowerment initiatives and emergency support interventions. He primarily uses WhatsApp alongside Facebook Messenger and sometimes Telegram to communicate and organize community activities.

“ We use WhatsApp for meetings and [to] share documents: reports, pictures, videos, etc. As a result of insecurity (e.g., banditry and terrorism) which we have encountered in our region, [in order to increase reach] we try to ensure other forms of communication to engage.”

“ I follow up with a phone conversation and see how true it is or go online to verify that story before I choose to re-broadcast it. But in some cases, many people don't verify, they just repost and repost, and it causes panic, and in a few hours they find out it's fake.”

Social media and private messaging platforms have become crucial communication channels for individuals in regions with significant unrest, like Northern Nigeria. Victor often lends his phone to community members who do not have WhatsApp-enabled phones to communicate with their loved ones in and outside the country. Victor, and other community members who have access to a private messaging app (e.g., WhatsApp), play a critical role in sharing emergency news (e.g., when there is a bandit attack) to warn others and mobilize emergency support. Victor prefers to use WhatsApp because it is used by many, offers more media sharing options (e.g., video, audio, image support), and costs less than regular calls/SMS due to low data costs.

ABOUT VICTOR

Conforming to groups

(e.g., thinking, practices)

HIGH

Comfort with technology

(e.g., use of private messaging platforms)

MODERATE

Privacy & security vulnerability

MODERATE

Perceived exposure to risks

MODERATE

Challenges & concerns

Even though the benefits offered by private messaging apps outweigh the problems, Victor still feels that there are a few significant risks that impact his communications on private messaging platforms.

Related Global Harms

- Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content [view harm](#)
- Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment [view harm](#)

Needs

Victor believes that private messaging platforms have a significant role to play in connecting people, and circulating critical public information to the masses. Although, with all of these benefits, he is also worried about the use of these platforms to plan for violent attacks. He wishes that certain support tools could be introduced to better manage the information and accounts on private messaging apps.

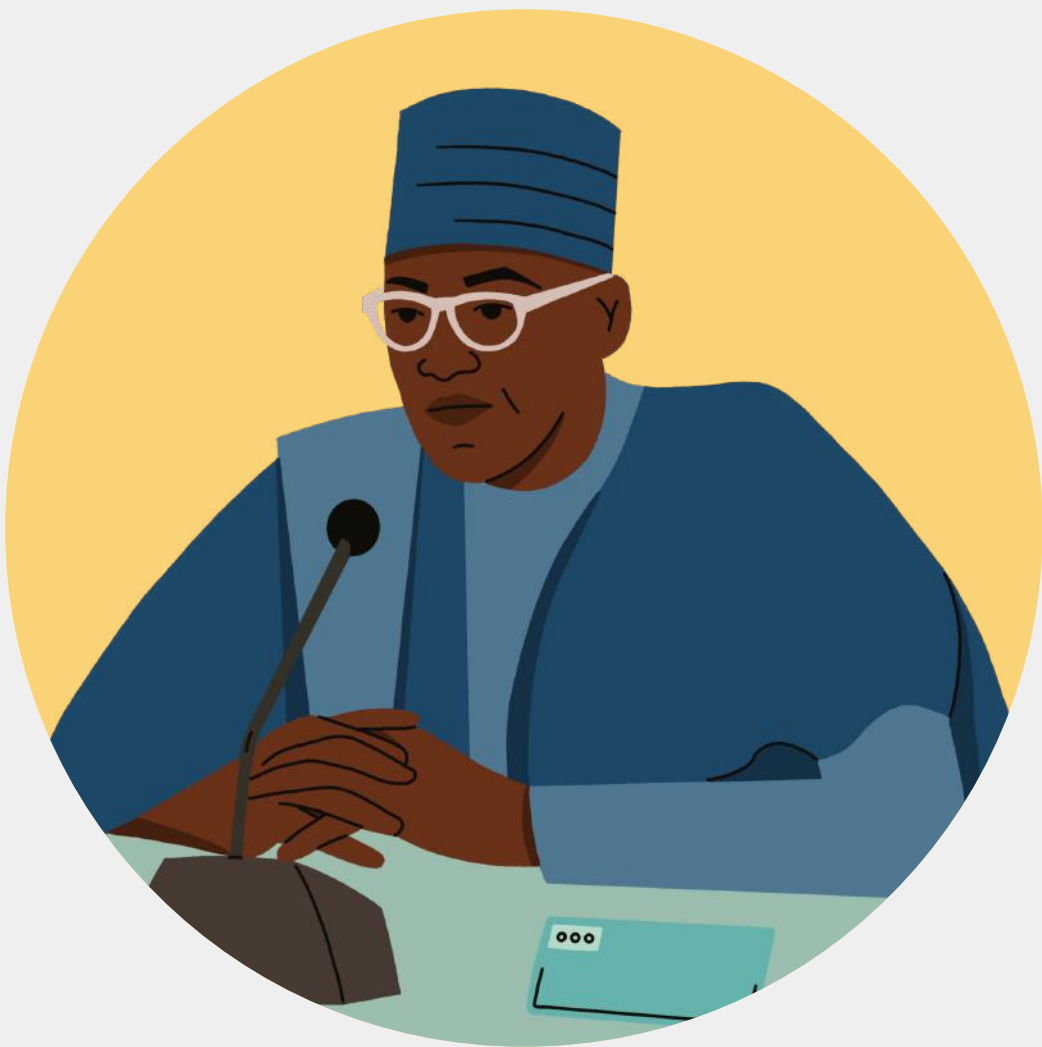
Related Design Opportunities

- Improving verification & permission mechanisms (e.g., notifications of offensive content before viewing) [view design opportunity](#)
- Providing user support mechanisms & emergency controls (e.g., Tagging and reporting of false information & content authentication tools) [view design opportunity](#)

Low Tech Influencer

Meet Emmanuel

Emmanuel is a trusted leader and a deeply religious man. He has a significant following in his hometown, where he offers his teachings and inspirations. He usually meets with his followers at a local church that he has helped set up, as well as other community gatherings and spaces.



Emmanuel’s story

Emmanuel is a 48- year-old church leader who lives in Lagos, Nigeria. He runs a local church and is also an inspirational speaker and life coach to his followers. He often meets his followers through scheduled public gatherings, however after he started using a private messaging app, he quickly realized the convenience it offered through individual and group communications, so he now heavily uses private messaging apps to engage his followers. He primarily uses WhatsApp to communicate, but he also connects on other platforms like Telegram in order to reach as many followers as possible, wherever they are most comfortable.

“For WhatsApp, I have a broadcast group where I put content on a daily basis. Inspirational content. People get to react directly.

“Sometimes, especially when counseling, the information shared is very sensitive. For instance, if you are being counseled that you should separate from your husband, this is sensitive and you need security. [to prevent unauthorized access by a third-party]

Private messaging platforms have become an important tool in his communication arsenal. These allow him to reach as many people as possible from the comfort of his home, particularly during the Covid-19 pandemic. Although, with the increase in different messaging platforms and the ever-changing features and risk factors, he is admittedly struggling to understand which platform best suits his need to engage with his followers in a safe, efficient and effective manner outside of in-person church gatherings.

ABOUT EMMANUEL

Conforming to groups <small>(e.g., thinking, practices)</small>			HIGH
Comfort with technology <small>(e.g., use of private messaging platforms)</small>	LOW		
Privacy & security vulnerability			HIGH
Perceived exposure to risks		MODERATE	

Challenges & concerns

Many of Emmanuel’s interactions with his followers happen on social media and preferred private messaging apps. These interactions include marriage counseling, inspirational talks and the sharing of sensitive documents and information. Due to the nature of his interactions, he is primarily worried about the privacy of his communications and the security of his account.

Related Global Harms

- Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content [view harm](#)
- Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment [view harm](#)
- Vulnerability to digital surveillance and monitoring [view harm](#)

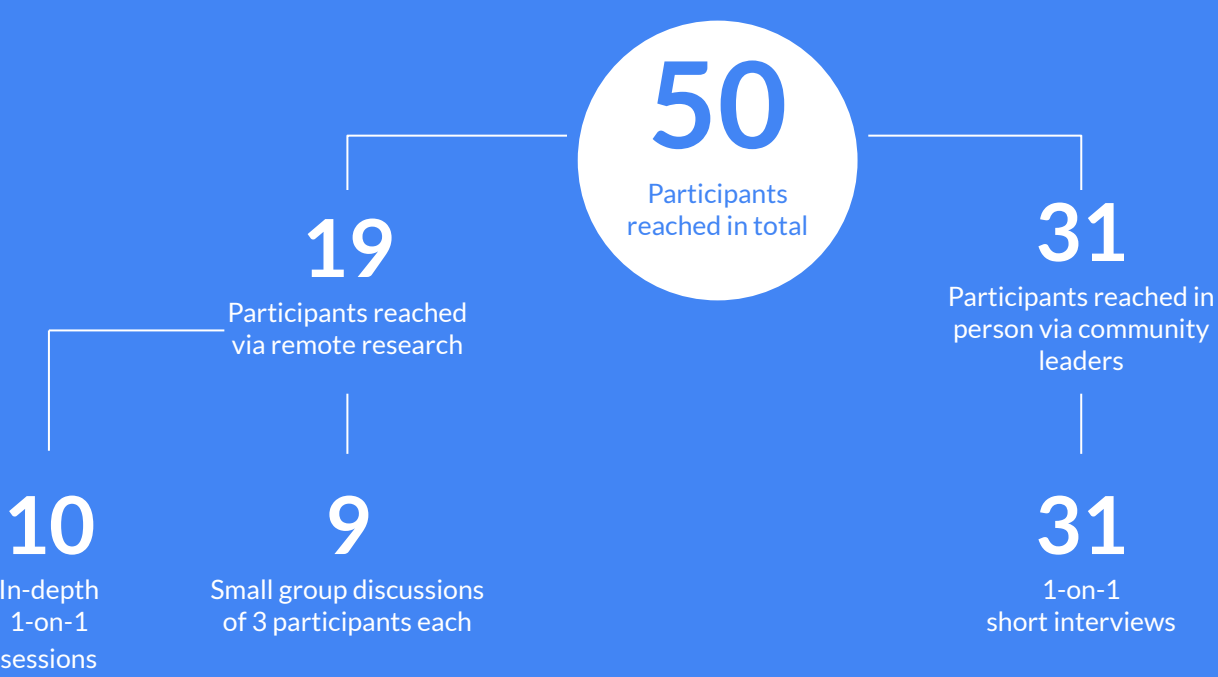
Needs

Even though Emmanuel has deep concerns about private messaging apps, especially with an increase in hacking of private messaging accounts, his low understanding of tech impacts his ability to troubleshoot and resolve critical account issues (e.g., blocking and recovery of hacked account) so that he might feel more secure in managing his fears. He would require very user-friendly solutions to help him to manage or mitigate these risks.

Related Global Design Opportunities

- Providing accessible & tailored security & privacy controls (e.g., Security options to lock chats / conversations within the messaging app) [view design opportunity](#)
- Providing support mechanisms & emergency controls (e.g., Restrict screenshot & forwarding of messaging, Blocking and recovery of hacked accounts) [view design opportunity](#)

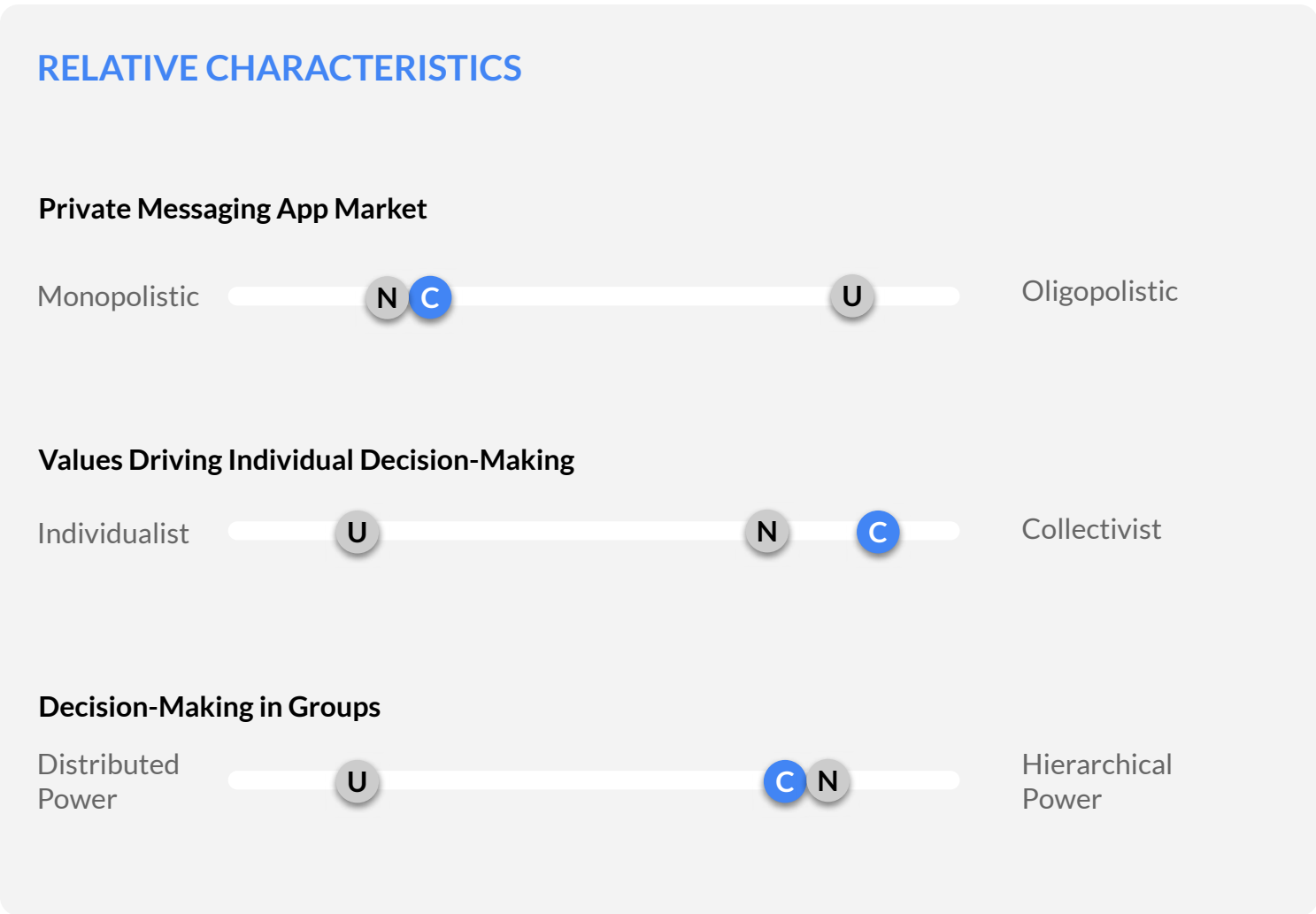
Colombia



The Colombian Context

Colombia has a population of about 51 million people, with 66% internet penetration as of 2022.¹ It has a strong collectivist culture relative to the other countries we studied. Belonging and aligning yourself with a group’s values and opinions is very important at many different levels in Colombian society, as reported by our research participants. This often shapes structures in social and professional circles and reflects how power is concentrated² e.g., participants expressed support for the role of government in the surveillance of criminal activities. These foundational values and beliefs significantly influence the mental models and adoption and usage of private messaging apps by participants.

Currently, the private messaging app market share in Colombia is dominated by WhatsApp at 55% as of 2019³. Our research suggests that the majority of interactions on private messaging apps tend to happen in group spaces where admins are perceived as strong authority figures and entrusted with making important group decisions.



Adoption and usage of messaging apps in Colombia

The majority of participants we spoke with in Colombia used WhatsApp for personal communications and socializing. Telegram showed up as the second most common platform often used for business and larger group communications. The adoption and usage of private messaging platforms among participants was driven by:

- Pre-installed private messaging app (e.g., WhatsApp on new phones)
- Social and current trends (e.g., migration due to private messaging app connection outages as a result of internet shutdowns as well as unreliable internet connectivity)⁴
- Popularity of specific private messaging apps among different social circles
- Customizations features and other advanced options of particular private messaging app

Other uses of private messaging apps in Colombia include:

- Communications with friends and family in and outside the country
- Socializing and sharing entertainment content on status/stories
- Business communications and large group interactions
- Distributing emergency information, especially during protests and civil unrest

Perceptions and concerns about privacy and security

Participants in Colombia were most worried about the security of their accounts and personal information from hackers and fraudulent contacts. A small group of participants were also concerned about government surveillance, but these views did not seem to be widespread (e.g., activists). This is due to the widespread awareness of cases of hacking, emergency scams, blackmailing and increased crackdown on dissenters and government critics. Some participants were also concerned about certain privacy features (e.g., read receipts, last online) that are leading to increased social pressures and anxiety. Other privacy issues and concerns raised by the participants include:

- Account hacking and cloning
- Extortion and fraud
- Child and adult pornography
- Spams
- Protection of minors
- Surveillance, especially by government operatives, a concern primarily shared among activists
- Interference of private messaging app connections by government, also a concern primarily shared among activists

Sources: [1] WorldBank [2] Statista [3] Hofstede insights [4] Reddit

Representative user archetypes in Colombia

The participants we interviewed in Colombia exhibited some overall commonalities regarding their mental models, usage behaviors and choice of private messaging apps. This is likely influenced by cultural and societal values and beliefs. But we also observed meaningful differences based on personal experience. We selected three user archetypes in Colombia that best represent the different behavioral and social influencing factors to the adoption and usage of private messaging apps that emerged from our research.



Concerned Activist

This archetype comprises activists in Colombia who have limited alternatives to dominant private messaging apps, and face increasing risks due to their activism and limited safety options (e.g., legal protection, effective safety practices) to leverage in order to counter growing risks (e.g., surveillance, hacking etc).



At Risk Adolescent

This archetype comprises individuals who are below legal adult age or who have recently become adults. This group faces particular challenges due to their susceptibility, and limited awareness/knowledge of risks as well as limited safety options to mitigate these risks.



Low Tech Entrepreneur

This archetype comprises entrepreneurs (e.g., transport service, plumbing) who have started to significantly leverage private messaging apps for communications and operations but have limited know-how of how to effectively use private messaging platforms to safeguard their businesses from hacking while maximizing communications.

Concerned Activist

Meet Barbara

Barbara is a passionate human rights champion and activist. She wants to bring about social change through organized protests/rallies. She leverages the reach of private messaging platforms to plan and mobilize, even though she faces serious threats both online and offline, and has limited alternatives to mitigate risks.



Barbara’s story

Barbara is a 24-year-old Colombian who is self-employed and lives in Bogota. She is passionate about human rights and actively involved in protests and championing the rights of others. She is very concerned and protective of her privacy when using private messaging platforms which deeply influences her adoption and usage of different platforms. Also, due to her activism, Barbara has become a target of government surveillance from time-to-time, so her safety is also becoming a cause for concern. She used to use WhatsApp as her primary private messaging app but switched to Telegram when WhatsApp updated its privacy policies, which made her distrustful of the platform.

“ I got a message for an update on WhatsApp where I had a number of days to update to the conditions that WhatsApp imposed, otherwise it would stop working. That was the reason why I installed Telegram because I did not like some of the conditions and did not know what was going to happen.

“ During the protests, WhatsApp helped a lot because people who were lost in the streets could easily locate us because Facebook would get blocked and the networks were blocked as well.

WhatsApp and other private messaging apps like Telegram have become a cornerstone of communications amongst activists in Colombia. The ability to use live locations to pull together protesters; share real-time emergency information via their WhatsApp status during protests, and leverage encryption in groups chats are especially valued by Barbara and others like her.

ABOUT BARBARA

Conforming to groups

(e.g., thinking, practices)

MODERATE

Comfort with technology

(e.g., use of private messaging platforms)

HIGH

Privacy & security vulnerability

HIGH

Perceived exposure to risks

HIGH

Challenges & concerns

Barbara and others like her are very sensitive about the privacy of their communications, and their safety in general, since most have become targets of surveillance by government operatives. However, they have limited alternatives to more mainstream private messaging platform e.g., WhatsApp. Options like Telegram are preferred, but do not offer comprehensive privacy/protection of individuals and their information.

Related Global Harms

- Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment [view harm](#)
- Vulnerability to encryption and data breaches via modified and third-party supporting platforms [view harm](#)
- Vulnerability to digital surveillance and monitoring [view harm](#)

Needs

Due to her activism against the government and other powerful organisations, Barbara increasingly feels a heightened need for better privacy and security tools among individuals like herself and others. This group is acutely aware of features they believe would be useful to mitigate existing risks.

Related Global Design Opportunities

- Providing support mechanisms & emergency controls (e.g., emergency account access point to deactivate/recover compromised account) [view design opportunity](#)
- Providing accessible & tailored security & privacy controls (e.g., concealing & locking chats in user inbox) [view design opportunity](#)
- Improving verification & permission mechanisms (e.g., unknown contact verification) [view design opportunity](#)
- Improving administrative & management tools (e.g., enhanced user controls for screenshots and forwarding messages) [view design opportunity](#)

At Risk Adolescent

Meet Carlos

Carlos is a young, aspiring web developer who is passionate about technology and coding. He interacts with many digital platforms and is often quick to learn about and adopt new digital tools. He stays updated on news and information regarding technology through tech-oriented groups on private messaging apps as well as following tech influencers and tech companies on social media.



Carlos’ story

Carlos, who just turned 18, has been actively using WhatsApp since he was a 14-year-old. He was introduced to WhatsApp by his parents so that they could communicate with one another. He remembers that it was fairly easy to set up an account and start using WhatsApp. Over time, it has become his primary means of communication, not only with his parents but also with friends, school administrators and others. Because of his love for technology, Carlos currently uses several platforms including WhatsApp, Telegram and Discord alongside other social media platforms for communication and socializing/learning.

“When you download an app, you never check what instructions or terms and conditions it has, you just install it and that's because you need it.

Carlos recalls that when he started using WhatsApp, things were relatively simple and straightforward. However, he believes that now, younger individuals like him face ever-increasing risks/threats when using private messaging apps. Although he feels confident with his capabilities and understanding of the space to take necessary precautions, Carlos believes his less tech-savvy peers are at a higher risk. He especially sees public group spaces on private messaging platforms as being a high-risk touch point for unsuspecting young users. These spaces are where malevolent individuals target impressionable or naive individuals for explicit selfies, sexual exploitation and sometimes kidnappings.

ABOUT CARLOS

Conforming to groups

(e.g., thinking, practices)

		HIGH
--	--	------

Comfort with technology

(e.g., use of private messaging platforms)

		HIGH
--	--	------

Privacy & security vulnerability

		HIGH
--	--	------

Perceived exposure to risks

		HIGH
--	--	------

Challenges & concerns

Carlos believes younger individuals are susceptible to many risks on private messaging apps, especially those who lack guidance, clear information and general tech-savviness.

Related Global Harms

- Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment [view harm](#)
- Vulnerability to targeted harassment for youth and young adults [view harm](#)
- Vulnerability to encryption and data breaches via modified and third-party supporting platforms [view harm](#)
- Vulnerability to adverse mental health impacts [view harm](#)

Needs

Carlos understands that it would be difficult to create a haven for younger groups where they are 100% safe. However, he believes that there are certain actions that can enable younger individuals like him to use private messaging apps more safely.

Related Global Design Opportunities

- Managing access to modified & third-party supporting platforms (e.g., increased control for screenshots and forwarding messages)
- Providing support mechanisms & emergency controls (e.g., emergency account access point to deactivate/recover compromised account) [view design opportunity](#)
- Providing accessible & tailored security & privacy controls (e.g., concealing & locking chats in user inbox) [view design opportunity](#)
- Improving verification & permission mechanisms (e.g., unknown contact verification) [view design opportunity](#)

Low Tech Entrepreneur

Meet Diego

Diego is a budding entrepreneur who wants to build a national transport company in Colombia. He has been driving delivery trucks for many years and is very passionate about his work and making his clients happy.



Diego’s story

Diego is 44 years old, and runs a small transport company in Villeta. Due to the nature of his job, he is constantly multi-tasking, chasing payments, coordinating and resolving transportation issues. He heavily relies on WhatsApp and Telegram for the day-to-day operations of his business. He belongs to many groups on WhatsApp and he finds these groups to be very valuable to him in marketing his business. He also uses private messaging apps to receive and share important traffic/emergency information with other drivers in his region.

“I use an app called Troller. I don't have a good memory.... and with this can identify if a call that comes to my cell phone is reliable. It only works with calls, and there I can see if it is reliable or a scam or robbery.”

“On WhatsApp I notice that there is no good security, anyone who takes your cell phone can check your messages, whether it is a robbery or another person whom you may have lent your cell phone.”

Diego admits that even though he uses these private messaging apps daily, he still does not understand many features of the platform. He primarily uses them to communicate and does not share anything else besides his basic profile information. Because many people have his contact, Diego receives a lot of spam messages and is added to groups that he is unfamiliar with and does not want to join. He also gets annoyed by people who spam groups by posting offensive and irrelevant information/misinformation in group chats, which disrupts more important conversations.

ABOUT DIEGO

Conforming to groups

(e.g., thinking, practices)

HIGH

Comfort with technology

(e.g., use of private messaging platforms)

LOW

Privacy & security vulnerability

HIGH

Perceived exposure to risks

MODERATE

Challenges & concerns

Even though he finds value in group chats, Diego also feels that it can be very frustrating and stressful to keep up with the updates, notifications and spam. Diego also believes his lack of technical understanding of private messaging apps is hindering his ability to fully utilise the platforms for his business.

Related Global Harms

- Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment [view harm](#)
- Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content [view harm](#)

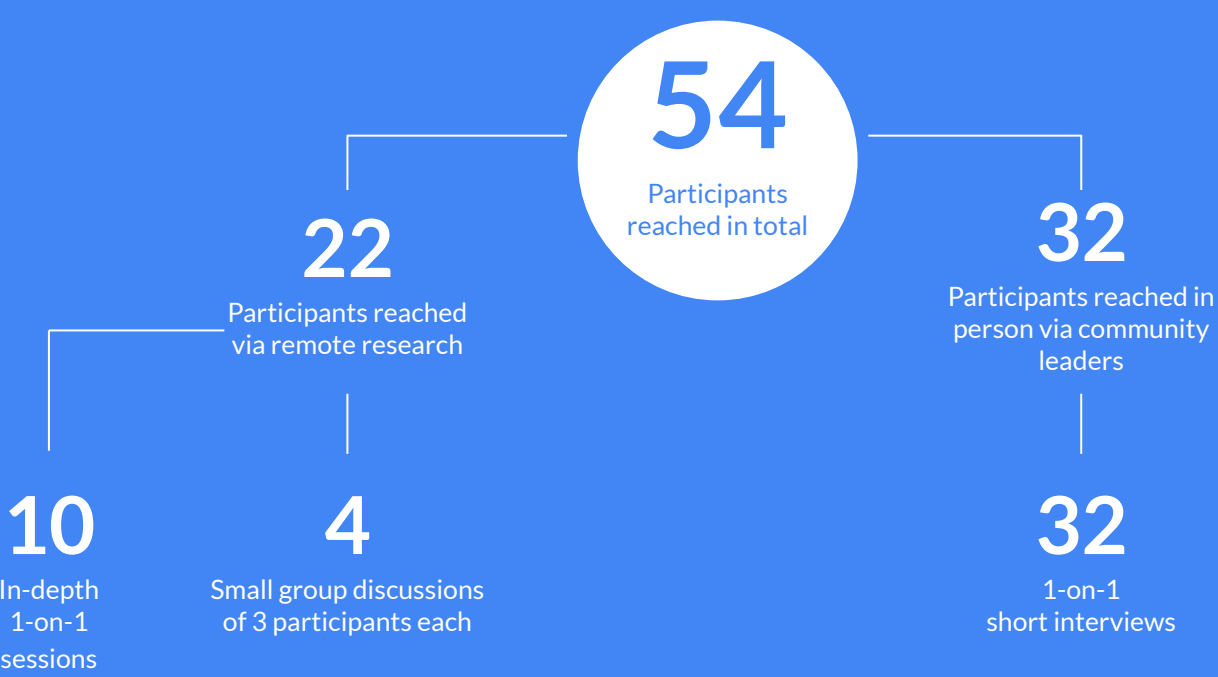
Needs

Due to his increasing dependency on technology and low familiarity with technology, Diego wishes for more forgiving and easily accessible features to customize his experience on private messaging apps. He believes that user education is critical to narrowing the knowledge/skill gap.

Related Global Design Opportunities

- Providing support mechanisms & emergency controls(e.g., discoverability of important features/settings) [view design opportunity](#)
- Improving verification & permission mechanisms (e.g., content verification and blocking, new contact & group verification) [view design opportunity](#)
- Providing accessible & tailored security & privacy controls (e.g.,custom group privacy settings [view design opportunity](#)

United States

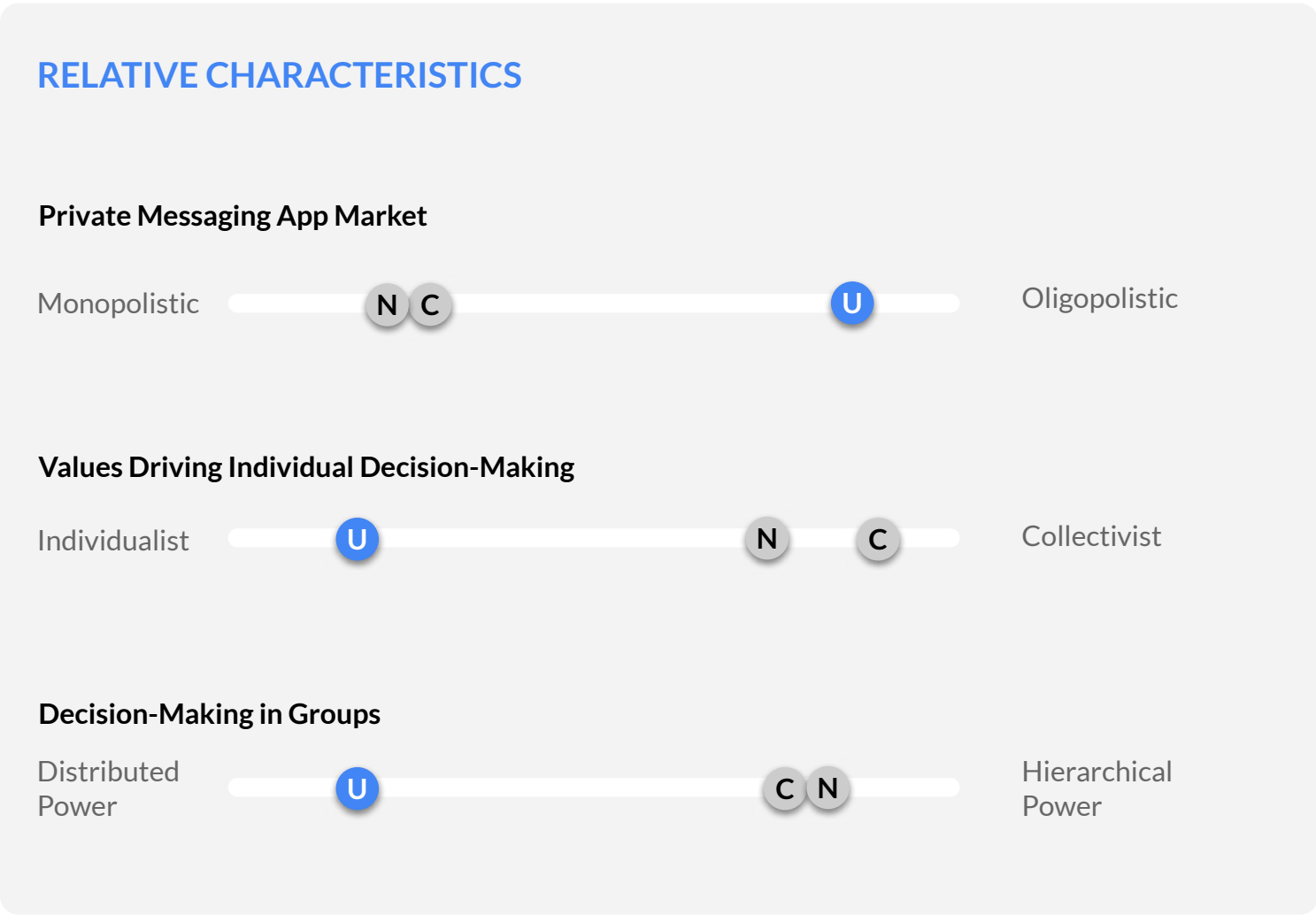


The American Context

The US has a population of 331 million people as of 2020¹, of which around 72% accessed the internet through mobile devices as of 2021². American society is shaped by a strong libertarian streak, with individual privacy and freedom being highly valued by the participants we spoke with. The behaviors and experiences that surfaced in our research suggested a stronger individualistic mindset relative to Nigeria or Colombia. US participants tended to believe that they should look after themselves and their immediate families or friends while relying less on authorities and the broader community for support³.

This belief system plays a significant role in individuals’ mental models, adoption and usage of private messaging apps, with the majority of participants more strongly believing that autonomy and digital privacy should be a fundamental right than we heard in Nigeria or Colombia. For instance, based on our observations, admins are not seen as similarly strong authority figures with absolute decision-making powers in group spaces. Flagging of content and participants by admins is perceived as violating freedom of speech by a number of our US participants. Anonymity is also more valued over identification and verification than what we heard from participants from other markets.

Currently, WhatsApp with over 25 million subscribers, has a much larger market share in the US than Telegram and Signal. From our observations, many conversations on private messaging platforms tend to happen via P2P as opposed to groups. In group spaces, most participants we spoke with were reluctant to cede more control to admins and responded more positively to distributed decision-making approaches that might apply to all members.



Adoption and usage of messaging apps in the US

Many of the participants we spoke with from the United States used a mix of private messaging apps to communicate with family, friends and colleagues, with some individuals using 3-5 messaging apps concurrently. Although very privacy-oriented, participants tend to use 1-2 trusted messaging apps to reduce their exposure to risks. The adoption and usage of private messaging apps by participants was driven by:

- Social/current trends
- Popularity of a private messaging app among individuals circles
- Privacy and security options
- Level of encryption
- Values and missions of private messaging app founders

Their primary uses of private messaging app included:

- Communicating with friends and family in and outside the country
- Socializing with family and friends
- Business communications and large group interactions
- Planning and organizing rallies and community initiatives

Perceptions and concerns about privacy and security

The participants in the US that we spoke with were very concerned about their privacy. The level of concern varied depending on the individual, although most of them generally agreed that the privacy of individuals should be a basic expectation. We observed that many participants distrust messaging apps that have a clear commercial objective (e.g., selling ads). They see these apps as having an incentive to infringe upon individuals’ privacy. To a large extent, privacy and safety in communications is perceived as an individual responsibility (e.g., being aware of risks and taking necessary steps) because privacy and security is believed not to be 100% guaranteed on all platforms. Other privacy and concerns raised by participants include:

- Government surveillance
- Monitoring of conversations for targeted ads
- Physical access of accounts by government operatives
- Spies in group chats
- Anonymity/access to personal information

Sources: [1] WorldBank [2] Statista [3] Hofstede insights

Representative user archetypes in the US

The participants we interviewed in the US exhibited a higher degree of diversity than our Colombian or Nigerian participants regarding their mental models, usage behaviors and choice of private messaging apps. This is likely influenced by migration patterns, cultural and political beliefs as well as the less dominant role that a platform like Whatsapp plays in day-to-day life in the US relative to the other markets. We selected three user archetypes that best represent different behavioral and social influencing factors to the adoption and usage of private messaging apps that emerged from our US research.



Advantaged Activist

This archetype comprises individuals who use private messaging apps for social and political activism. This group tends to have access to important support structures for information, and safer privacy and security practices, as well as the availability of different private messaging app options for more safer and private communications.



Globe Trotter

This archetype comprises individuals who conduct frequent international communications across multiple private messaging platforms (e.g., frequent travelers, international students).



Ceremonial Admin

This archetype comprises individuals who are admins in groups of larger than 100. They are viewed as regular members by other group participants and usually not expected to moderate interactions or make key group decisions (e.g., removal and reviewing of content).

Advantaged Activist

Meet Jake

Jake is passionate about championing the rights of others and driving positive change in his community through community mobilization and peaceful activism.



Jake’s story

Jake is a 25-year- old artist and community mobilizer living in Florida. He works closely with community members to champion their rights and seek justice when necessary. Due to the nature of his work, he has become a target of local authorities and other community members. He is very careful and takes extra precautions when communicating or sharing information that is sensitive with others. He admits that technology has made it easy to connect with others, especially like-minded people, but he is also concerned about leaving a trail of evidence that can be used against him by others, especially those in positions of power.

“A password in this day and age feels rudimentary, because if someone really wants to, they can still access your account.”

“I no longer go by my old name, just because the internet is a s— place. You can't search for me by my legal name, it's a decision I made a long time ago. I try to keep my face hidden to strangers and mostly identifiable by family.”

Jake is extremely cautious with his mobile devices and seeks to hide his personal information whenever he uses private messaging apps. He believes that mobile devices can easily be used to eavesdrop, monitor movements and community gatherings by authorities. Although he uses several messaging apps to keep in touch with family and friends, Jake only uses one app that he trusts [Signal] to receive and share sensitive/confidential information. He especially sees the advances in surveillance technology by government operatives as being a serious threat to his personal safety.

ABOUT JAKE

Conforming to groups

(e.g., thinking, practices)

LOW		
-----	--	--

Comfort with technology

(e.g., use of private messaging platforms)

		HIGH
--	--	------

Privacy & security vulnerability

		HIGH
--	--	------

Perceived exposure to risks

		HIGH
--	--	------

Challenges & concerns

Jake is extremely distrustful of communication devices/platforms. He generally prefers to do things in person and away from devices. However, this is not possible all the time and he is forced to use digital messaging platforms regularly. So he always takes extreme safety precautions with private messaging apps.

Related Global Harms

- Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment [view harm](#)
- Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content [view harm](#)

Needs

Due to increased surveillance and sophistication of tools used to surveil, Jake would like to see changes not only in pro-privacy/security features but also policies that push for standardizing and upholding individual privacy and security on all messaging apps. He strongly believes that individual privacy should be a fundamental right when using digital apps.

Related Global Design Opportunities

- Providing support mechanisms & emergency controls (e.g., blocking personal accounts remotely) [see design opportunity](#)
- Improving verification & permission mechanisms (e.g., enhanced permissions especially for location services) [view design opportunity](#)
- Securing personal data & account information (e.g., better tools that support anonymity of individuals) [view design opportunity](#)
- Providing accessible & tailored security & privacy controls (e.g., tailored privacy options) [view design opportunity](#)

Globe Trotter

Meet Jennifer

Jennifer is an experienced interior designer passionate about traveling the world, having new experiences and making new friends. She actively communicates on several platforms with contacts across the globe for business & social reasons.



Jennifer’s story

Jennifer is an interior designer and loves to travel the world. She has friends across continents whom she keeps in touch with often. She also manages many groups on private messaging apps that stretch across different time zones and continents. She uses several platforms in order to stay in touch with all of her contacts. She often uses WhatsApp because many of her contacts are on it, but she prefers to use Signal because it’s simple and has fewer distractions.

“I mainly use these platforms for personal communications. I am open to the opposites person’s preference because I don't really mind [regarding messaging apps]”

“When I was in Bali I connected with some people on WhatsApp there, and when I got back to Sweden, Facebook tried to connect me to those people. Then I realized okay this is how it is connected together. This was not a coincidence.”

Jennifer finds it overwhelming to keep in touch with all of her contacts across several different platforms. It takes a lot of time and energy to respond to chats and keep up with group interactions. She sees organizing her contacts as one of the important challenges she faces, especially when it comes to separating business, personal and other connections. Even though she is not particularly worried about the privacy of her communications, Jennifer is still careful about sharing sensitive information over messaging apps and often prefers to either use email or Signal for such exchanges.

ABOUT JENNIFER

Conforming to groups

(e.g., thinking, practices)

HIGH

Comfort with technology

(e.g., use of private messaging platforms)

HIGH

Privacy & security vulnerability

MODERATE

Perceived exposure to risks

LOW

Challenges & concerns

Jennifer admits that she is not worried about her privacy because she has nothing to hide. She is mostly concerned with streamlining her communications and managing her contacts.

Related Global Harms

- Vulnerability to adverse mental health impacts [view harm](#)
- Vulnerability to encryption and data breaches via modified and third-party supporting platforms [view harm](#)

Needs

While she is generally happy with her private messaging app usage, Jennifer would prefer to streamline her experience by using fewer features – as she can barely keep up with all of the messaging apps she uses. She identified a few features that would help resolve some of the challenges she faces.

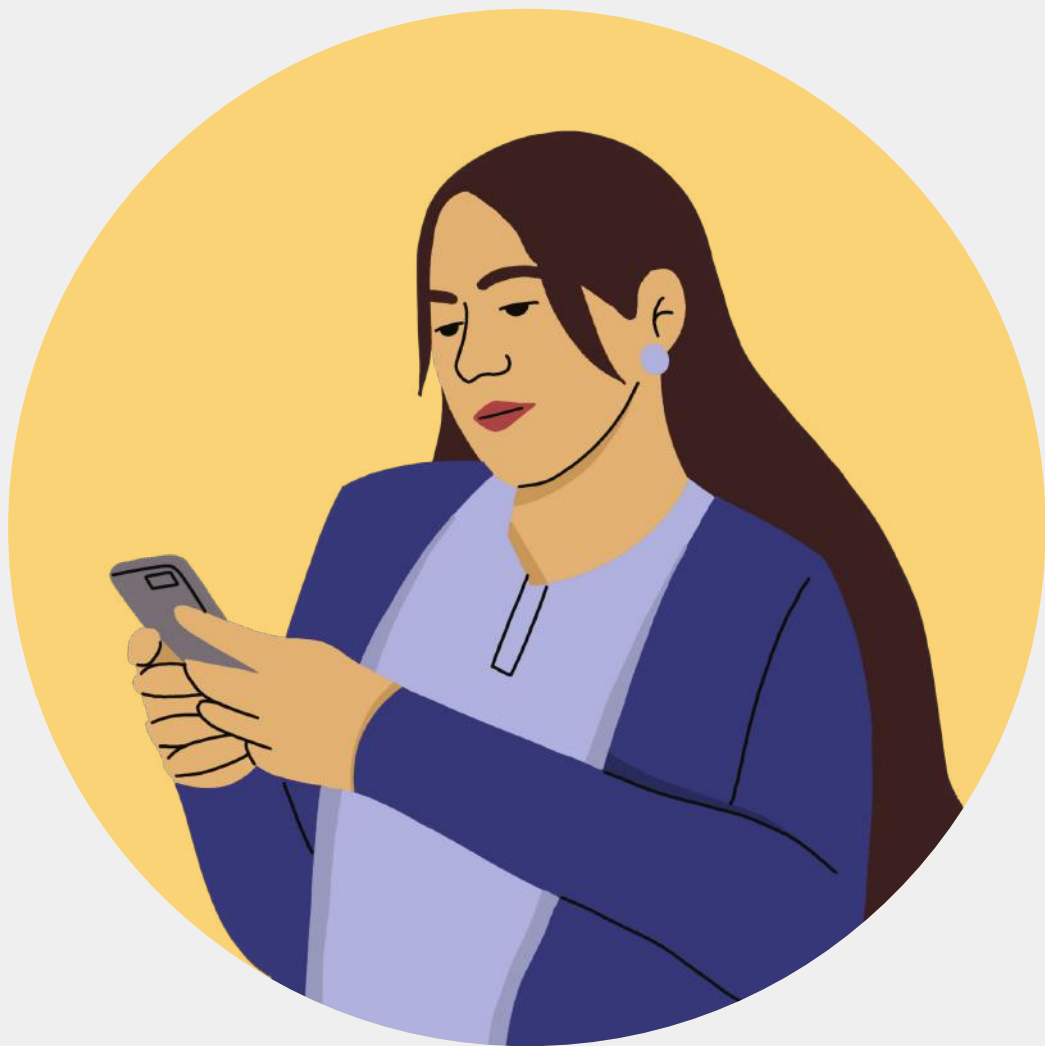
Related Global Design Opportunities

- Improving administrative & management tools (e.g., contact management tools) [view design opportunity](#)
- Improving verification & permission mechanisms (e.g., group/contact permissions and verification) [view design opportunity](#)
- Providing accessible & tailored security & privacy controls (e.g., tailored contact / group privacy options) [view design opportunity](#)

Ceremonial Admin

Meet Kelly

Kelly manages several groups on different private messaging platforms and is often faced with many challenges when managing these groups. Even though she has access to some admin tools, she is generally unable to use them due to resistance by group members who believe control and management of groups should not belong to one person.



Kelly’s story

Kelly is a 34-year-old community manager and a customer service representative. She supports and manages multiple groups in different messaging applications on a daily basis for social and work purposes. Her choice of private messaging platforms is mainly influenced by popularity within her work and social circles and available features. She is less concerned about her privacy and security when using private messaging platforms so those features do not directly drive her decision-making process.

“On Telegram you can regulate the people who text you, who views your number and who calls you. Telegram has lots of people and maybe you don't want everyone to contact you.”

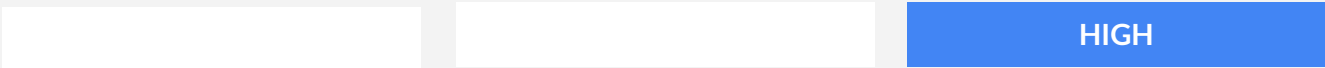
“Being in these groups means there's more notifications on your phone and more phone anxiety in general.”

Kelly admits that being a group admin is not as privileged as others might think, especially when you are the admin of several groups. Besides constant notifications and the demand to respond to urgent group matters, she does not feel recognized or appreciated as a voice of authority when it comes to group matters. Often members want more autonomy and democracy in decision-making in the group. She believes that more tools to help groups in planning, decision-making and reaching a consensus would be helpful to allow all group members to feel more involved in group management and governance.

ABOUT KELLY

Conforming to groups

(e.g., thinking, practices)

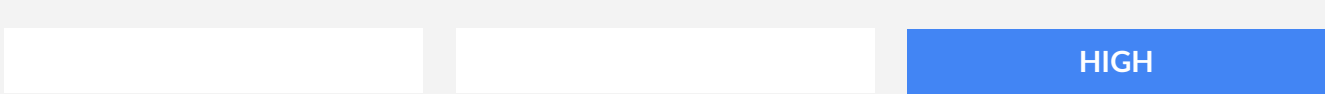


Comfort with technology

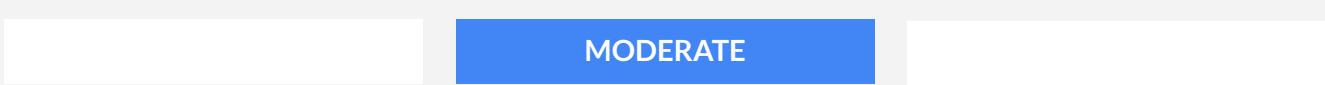
(e.g., use of private messaging platforms)



Privacy & security vulnerability



Perceived exposure to risks



Challenges & concerns

As an admin of several groups, Kelly deals with group flare-ups, misbehaviors and malicious links from time to time. She admits that it is usually difficult to resolve these issues as group members have differing opinions on the matter. So reaching a consensus becomes a problem.

Related Global Harms

- Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment [view harm](#)
- Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content [view harm](#)

Needs

Kelly believes that an average admin role is very demanding and that it would help to have access to tools that can assist with managing conversations in a group. She would also welcome tools that might allow group members to play active roles in management and decision-making in groups.

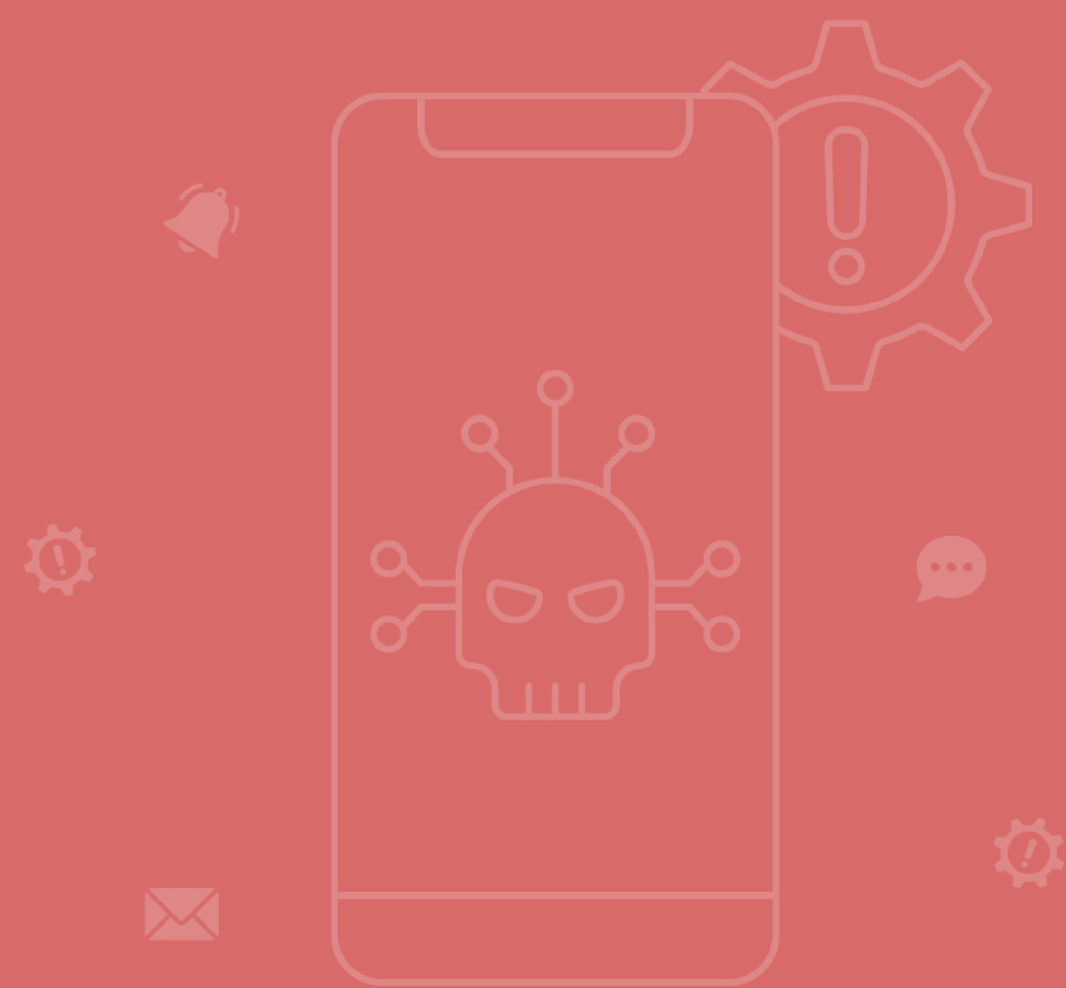
Related Global Design Opportunities

- Improving administrative & management tools (e.g., planning & polling tools) [view design opportunity](#)
- Improving verification & permission mechanisms (e.g., content/hyperlink verification) [view design opportunity](#)

03 Harms



Harms



The use of private messaging platforms can expose individuals to a range of harms that impact trustworthiness.

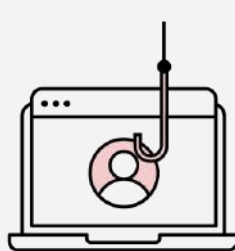
In this section, we cover six harms that were most frequently mentioned by the participants we spoke to in Nigeria, Colombia and the United States. For each one, we explore the different ways that these impact the user experience as well as the platform design gaps that can amplify these harms.

1. Vulnerability to adverse mental health impacts



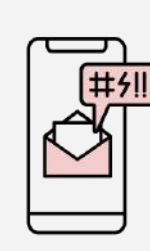
The negative psychological impacts that arise from using private messaging platforms.

2. Vulnerability to targeted harassment for youth and young adults



The use of private messaging platforms to exploit the vulnerability of youth and minors.

3. Vulnerability to manipulation or exposure to offensive content



The use of private messaging platforms to knowingly or unknowingly circulate content that can be perceived as being hateful, offensive and/or misleading.

4. Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment



The direct misuse of private messaging platforms by adults as distinct from those affecting youth and children.

5. Vulnerability to encryption and data breaches via modified and third-party supporting platforms



The different ways that private messaging platforms' security, privacy and encryption features are bypassed by individuals through the use of modified and third-party supporting private messaging platform apps.

6. Vulnerability to digital surveillance and monitoring



The potential use of private messaging platforms by governments and corporations to survey or monitor individuals.

Design gaps that enable these harms

Sitting across all six harms we found a total of seven product design gaps that seem to have the biggest impact on platform trustworthiness for the participants we spoke with.

A

Easy access to personal identifying data

Personal information on most private messaging platforms is easily accessible, while the use of phone numbers as account identifiers makes it easy to connect with any contact.

B

Limited verification and consent focused features for contacts and groups

There is a lack of mechanisms for verifying contacts or groups, while permissions for new contacts and groups are either not set by default or are non-existent.

C

Generalized and hidden privacy and security controls for contacts and groups

Security and privacy controls are presented as generic settings applied equally to all contacts and groups while also remaining hidden behind multiple steps within complex menu structures.

D

Infringement by modified (MOD) and third-party supporting apps ecosystem

There are multiple modified (MOD) and third-party supporting private messaging platform apps that offer individuals additional features that they can use in combination with or in replacement of their private messaging platform app.

E

Limited support and lack of adequate reporting mechanisms

From tech literacy and customer support to emergency and reporting tools, there are limited to no support mechanisms available. Those that exist are not perceived as being useful or adequately functional.

F

Limited content management tools

There are very few features that help individuals manage and organize the content they receive. This can cause some individuals, mainly those who participate in large groups and/ or receive large amounts of content, to feel overwhelmed.

G

Lack of transparency regarding access to personal data

There are gaps around who can access, use, and potentially misuse personal data (e.g., how and if companies and governments can access personal data). And private messaging platforms don't communicate transparently and in a user-friendly way how they manage and protect individuals' data.

Not all design gaps are relevant to all harms. But our research indicates that each of these design gaps has an adverse effect on more than one harm leading to a cumulative effect that raised deep concerns among every user we spoke with. The chart below presents a summary view of the specific design gaps and their negative impacts across the primary harms that emerged from our discussions across the three countries.

<div><div>HARMS IMPACTING USER TRUSTWORTHINESS</div><div>PRODUCT DESIGN GAPS</div></div>	1. Vulnerability to adverse mental health impacts	2. Vulnerability to targeted harassment for youth and young adults	3. Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content	4. Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment	5. Vulnerability to encryption and data breaches via modified and third-party supporting platforms	6. Vulnerability to digital surveillance and monitoring
A. Easy access to personal identifying data	✓	✓	✓	✓		✓
B. Limited verification and consent focused features for contacts and groups	✓	✓	✓	✓		
C. Generalized and hidden privacy & security controls for contacts and groups	✓	✓	✓	✓	✓	
D. Existence of modified (MOD) and third-party supporting apps ecosystem	✓	✓	✓	✓	✓	
E. Limited support and lack of adequate reporting mechanisms	✓	✓	✓	✓		
F. Limited content management tools	✓	✓	✓		✓	
G. Lack of transparency regarding access to personal data	✓				✓	✓

1.

Vulnerability to adverse mental health impacts

This harm covers the negative psychological impacts that arise from using private messaging platforms. This includes psychological difficulties such as screen-time fatigue, overdependence on private messaging platforms, impact of large volumes of notifications and content, unclear or uncertain exposure to digital surveillance, impact of exposing digital behaviors to other individuals (e.g., user is online, read receipts), and social pressures from other contacts, whether real or perceived.



Individual's experience of this harm

The adverse impact of platforms on mental health was expressed as being of medium to high concern for many of the participants we spoke to in all three countries, particularly for participants in Colombia and the US. Most participants described their concern as being connected to a distrust of technology which in turn stems from worries related to increases in:

- Digital surveillance and monitoring by both corporations and governments
- Frequent security breaches and the difficulty of guaranteeing privacy
- Overdependence on using private messaging platforms in general
- Anxiety related to the expanding use of private messaging platforms in their day-to-day lives

Participants in all three countries shared some common mental health concerns, often tied to features that are meant to increase platforms' stickiness. For example, in all three countries (particularly in Colombia) features that communicate user behavior to others (e.g., user is online, read receipts, user is writing) were frequently pointed to as the cause of unwelcome social pressures. In addition, individuals vulnerable to privacy and security concerns, such as activists and dissenters, shared the cumulative mental stress that resulted from concerns that they might be targeted at any time for surveillance by the government and police. Other less-vulnerable individuals similarly expressed feeling a heightened sense of surveillance concerns in relation to the misuse of their data by corporations, particularly in the US. Due to this, some participants turned to modified (MOD) or third-party supporting private messaging platform apps to access workarounds that could relieve these pressures.

The map on the next page presents a cross-country perspective on the impact of platforms on mental health from participants in Colombia, Nigeria and the United States. Particular attention is paid to the design gaps that contribute to the widespread experience of this harm by the participants we spoke with.

“ It happens to me with my clients that sometimes I leave my computer on and they say I wrote to you at 2am and I saw you were online and you didn't answer me.... Sometimes I have to do everything so that they don't see me online, like putting it in airplane mode.

38-year-old Colombian man, using WhatsApp, Telegram and FB Messenger

Level of concern expressed by participants

The scales below reflect the relative range of concern that participants we spoke with expressed for this harm across different countries.

Nigeria

Low medium High

Colombia

Low medium to high High

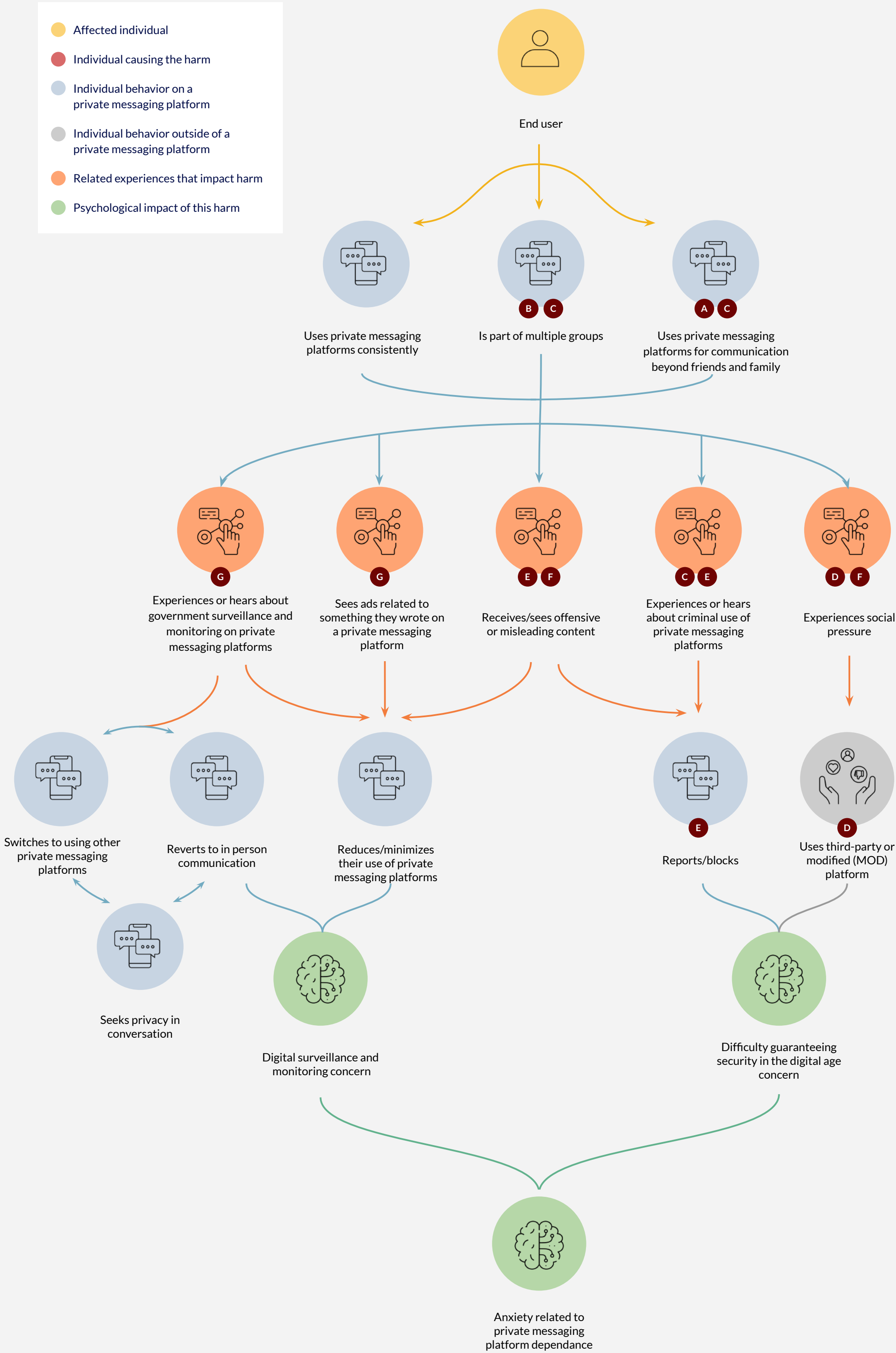
USA

Low medium to high High

“ My phone notification gets clogged up, you have so many apps telling you to look at me. I don't even have time to eat, let alone look at all of this. Most of the notifications are with those apps that have many members. So I need to look at the settings of these.

33-year-old Nigerian man

Vulnerability to adverse mental health impacts - illustrative process



Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

A Easy access to personal identifying data

Personal information on most messaging platforms is easily accessible, while the use of phone numbers as account identifiers makes it easy to connect with any contact.

B Limited verification and consent-focused features for contacts and groups

There is a lack of mechanisms for verifying contacts or groups, while permissions for new contacts and groups are either not set by default or are non-existent.

C Generalized and hidden privacy and security controls for contacts and groups

Security and privacy controls are presented as generic settings applied equally to all contacts and groups while also remaining hidden behind multiple steps within little-used menu structures.

D Infringement by modified (MOD) and third-party supporting apps ecosystem

There are multiple modified (MOD) and third-party supporting private messaging platform apps that offer individuals additional features that they can use in combination with or in replacement of their private messaging platform app without others knowing.

E Limited support and lack of adequate reporting mechanisms

From tech literacy and customer support to emergency and reporting tools, there are limited to no support mechanisms available. Those that exist are not perceived as being useful or adequately functional.

F Limited content management tools

There are very few features that help individuals better manage and organize the content they receive.

G Lack of transparency regarding access to personal data

There are gaps around who can access, use, and potentially misuse personal data (e.g., how and if companies and governments can access personal data). At the same time, messaging platforms don't communicate transparently and in a user-friendly way how they manage and protect personal data.

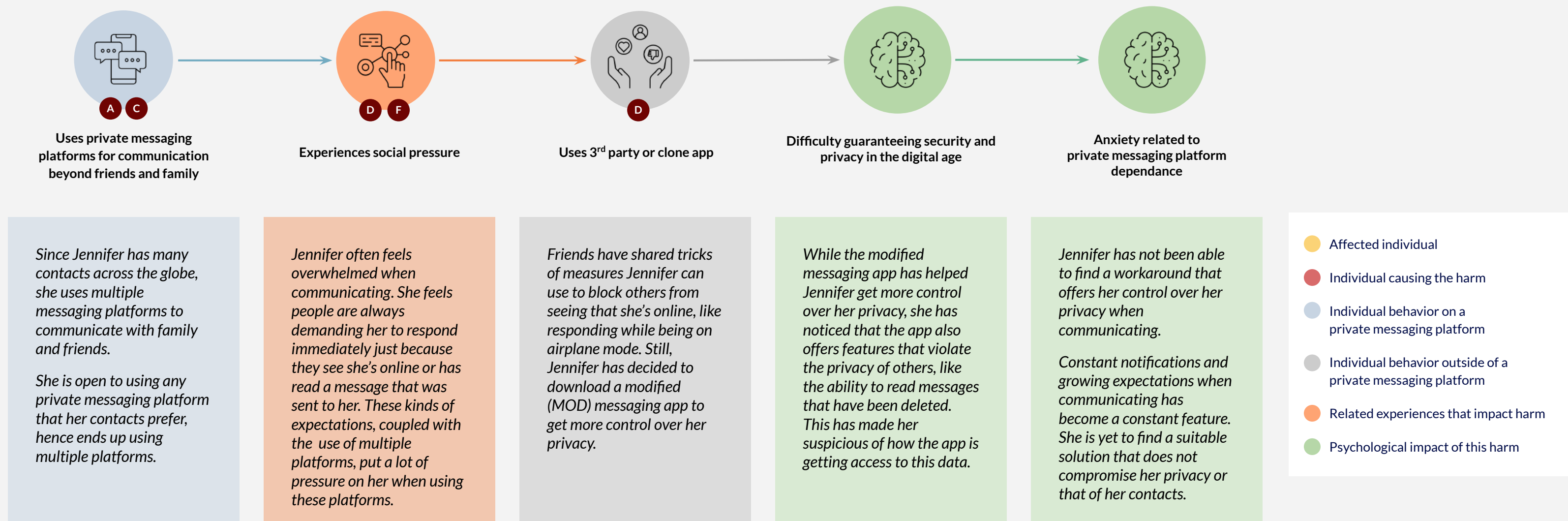
Vulnerability to adverse mental health impacts - illustrative journey



Jennifer - Globe Trotter

Jennifer is an interior designer and loves to travel the world. She has friends across continents whom she keeps in touch with often. She also manages many groups on private messaging apps that stretch across different time zones and continents. She uses several platforms in order to stay in touch with all of her contacts. She often uses WhatsApp because many of her contacts are on it, but she prefers to use Signal because it's simple and has fewer distractions.

“ When I was in Bali I connected with some people on WhatsApp there, and when I got back to Sweden, Facebook tried to connect me to those people. Then I realized okay this is how it is connected together. This was not a coincidence.



Explore the relevant experiences related to this harm

- Globe Trotter
- At Risk Adolescent

Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

- A Easy access to personal identifying data**

Personal information on most messaging platforms is easily accessible, while the use of phone numbers as account identifiers makes it easy to connect with any contact.
- C Generalized and hidden privacy and security controls for contacts and groups**

Security and privacy controls are presented as generic settings applied equally to all contacts and groups while also remaining hidden behind multiple steps within little-used menu structures.
- D Infringement by modified (MOD) and third-party supporting apps ecosystem**

There are multiple modified (MOD) and third-party supporting private messaging platform apps that offer individuals additional features that they can use in combination with or in replacement of their private messaging platform app without others knowing.
- F Limited content management tools**

There are very few features that help individuals better manage and organize the content they receive.

Product opportunities

We identified seven primary product opportunities to address the design gaps that contribute to the proliferation of this harm.

Design Opportunity 1

Securing and/or modifying account information



Product design gaps addressed

A Easy access to personal identifying data

Design Opportunity 2

Improving verification & permission mechanisms



Product design gaps addressed

B Limited verification and consent-focused features for contacts and groups

Design Opportunity 3

Providing accessible & tailored security & privacy controls



Product design gaps addressed

C Generalized and hidden privacy & security controls for contacts & groups

Design Opportunity 4

Managing access to modified & third-party supporting platforms



Product design gaps addressed

D Infringement by modified (MOD) & third-party supporting apps ecosystem

Design Opportunity 5

Providing support mechanisms & emergency controls



Product design gaps addressed

E Limited support and lack of adequate reporting mechanisms

Design Opportunity 6

Improving administrative & management tools



Product design gaps addressed

F Limited content management tools

Design Opportunity 7

Providing data use transparency & the ability to manage data



Product design gaps addressed

G Lack of transparency regarding access to personal data

Click below to learn more about all design opportunities:

Design opportunities

2.

Vulnerability to targeted harassment for youth and young adults

This harm covers the use of private messaging platforms to exploit the vulnerability of youth and minors which our users saw as a distinct concern from more general misuses. This includes physical, sexual, and psychological abuses that are conducted or aided via messaging platforms such as, phishing, circulation of child sexual abuse material, hacking, exposure to online predators, and cyberbullying.



Individual’s experience of this harm

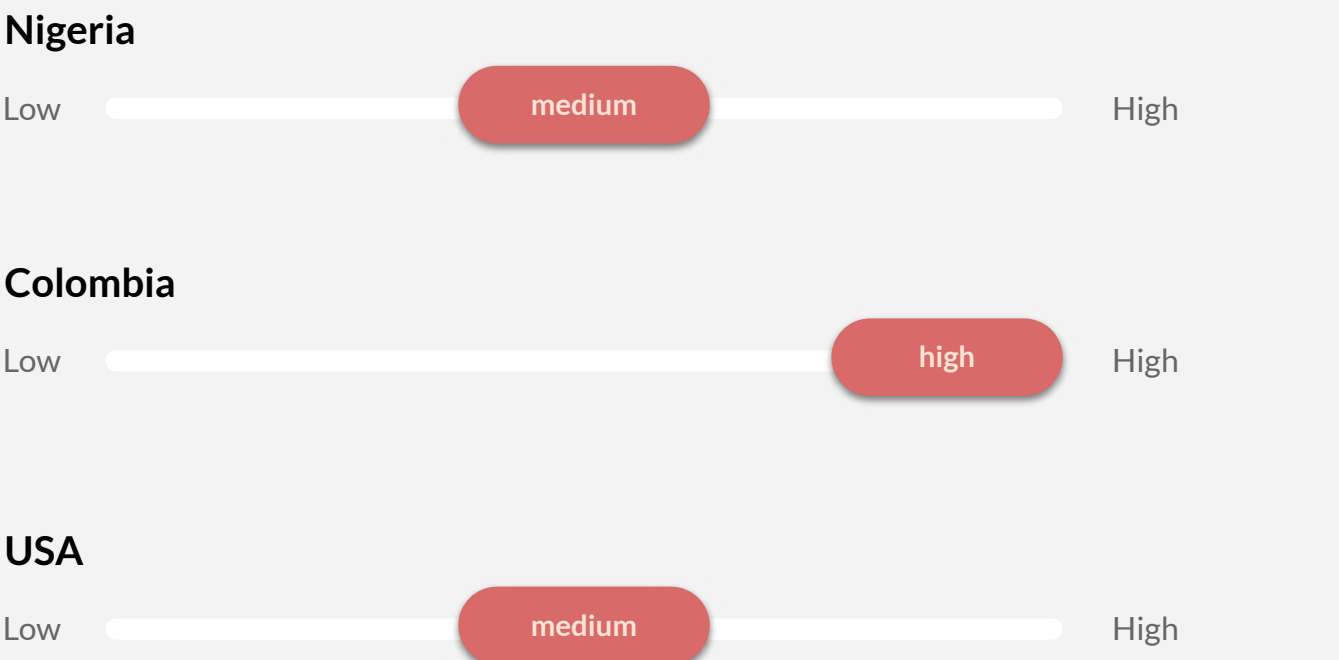
The use of private messaging platforms to exploit the vulnerability of youth and minors was expressed as being of medium concern for participants in Nigeria and the US and of extremely high concern for participants in Colombia. While all Colombian participants worried about this harm, Colombian parents expressed the most severe anguish over this risk. As such, in an effort to gain greater visibility of what could be affecting their children, they often turned to the use of third-party apps to clone the account of their children on their phones. This, however created additional stress as they tried to manage the right level of parental monitoring as their children grow up across multiple app environments.

While our research points to the need for protecting the vulnerability of minors and youth against criminal and abusive usage of private messaging platforms, we did not gather perspectives from minors (18 and under) directly as part of this study. Additional research would be needed to further understand the specific needs and use cases from the perspective of minors. The youth we spoke to (ages 18-20) expressed unique uses for private messaging platforms, including the use of WhatsApp and Telegram as dating apps, study groups, and places to meet new friends outside their circle.

The map on the next page presents a cross-country perspective on the use of private messaging platforms to exploit the vulnerability of youth and minors from the participants in Colombia, Nigeria, and the United States. Particular attention is paid to the design gaps that contribute to the widespread experience of this harm by the participants we spoke with.

Level of concern expressed by participants

The scales below reflect the relative range of concern that participants we spoke with expressed for this harm across different countries.



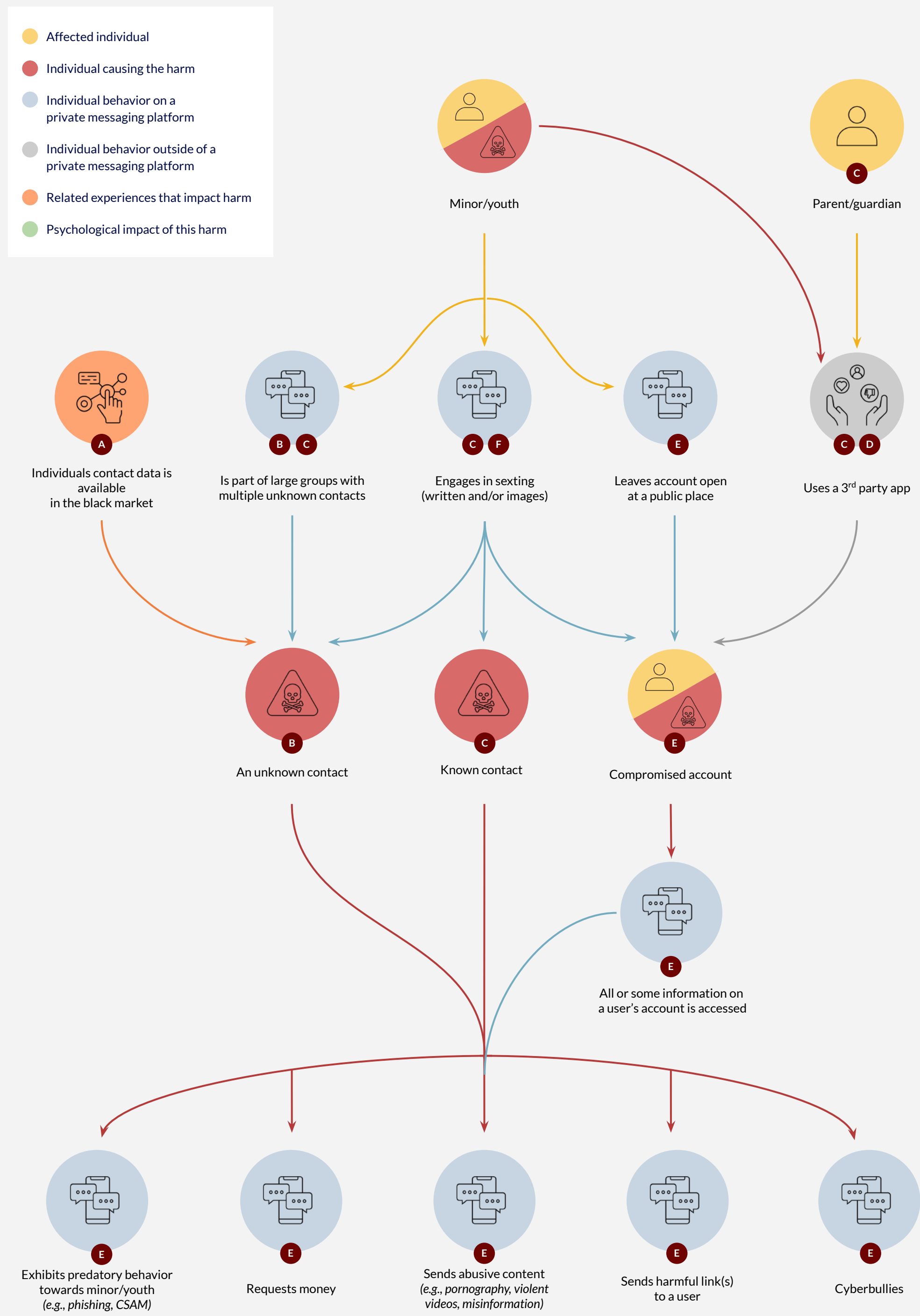
“At the beginning of the pandemic we started to use WhatsApp like a dating app. Posting on each others WhatsApp stories the link to our account so other people could see if they liked it or not.”

18-year-old Colombian boy, using WhatsApp, Telegram and FB Messenger

“When you download an app you never check what instructions or terms and conditions agreement it has, you just install it and that's it because you need it.”

18-year-old Colombian boy

Vulnerability to targeted harassment for youth and young adults - illustrative process



Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

A Easy access to personal identifying data

Personal information on most messaging platforms is easily accessible, while the use of phone numbers as account identifiers makes it easy to connect with any contact.

B Limited verification and consent focused features for contacts and groups

There is a lack of mechanisms for verifying contacts or groups, while permissions for new contacts and groups are either not set by default or are non-existent.

C Generalized and hidden privacy and security controls for contacts and groups

Security and privacy controls are presented as generic settings applied equally to all contacts and groups while also remaining hidden behind multiple steps within the menu.

D Infringement by modified (MOD) and third-party supporting apps ecosystem

There are multiple modified (MOD) and third-party supporting private messaging platform apps that offer individuals additional features that they can use in combination with or in replacement of their private messaging platform app.

E Limited support and lack of adequate reporting mechanisms

From tech literacy and customer support to emergency and reporting tools, there are limited to no support mechanisms available. Those that exist are not perceived as being useful or adequately functional.

F Limited content management tools

There are very few features that help individuals better manage and organize the content they receive.

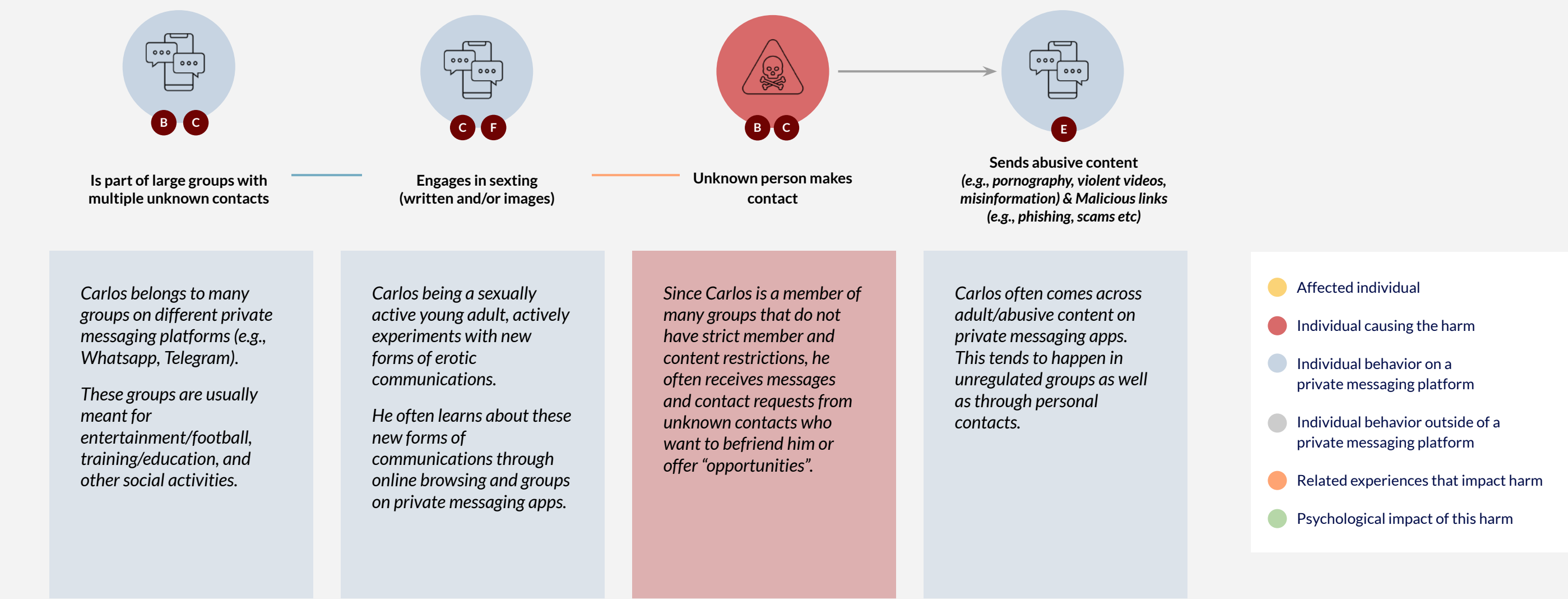
Vulnerability to targeted harassment for youth and young adults - illustrative journey



Carlos - At Risk Adolescent

Carlos, who just turned 18, has been actively using WhatsApp since he was a 14-year-old. He was introduced to WhatsApp by his parents so that they could communicate with one another. He remembers that it was fairly easy to set up an account and start using WhatsApp. Over time, it has become his primary means of communicating not just with his parents but also friends, school administrators and others. Because of his love for technology, Carlos currently uses several platforms, including WhatsApp, Telegram and Discord, alongside other social media platforms for communication and socializing/learning.

“When you download an app you never check what instructions or terms and conditions agreement it has, you just install it and that's it because you need it.”



Explore the relevant experiences related to this harm

- At Risk Adolescent
- Citizen Journalist

Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

- B Limited verification and consent focused features for contacts and groups**

There is a lack of mechanisms for verifying contacts or groups, while permissions for new contacts and groups are either not set by default or are non-existent.
- C Generalized and hidden privacy and security controls for contacts and groups**

Security and privacy controls are presented as generic settings applied equally to all contacts and groups while also remaining hidden behind multiple steps within little-used menu structures.
- E Limited support and lack of adequate reporting mechanisms**

From tech literacy and customer support to emergency and reporting tools, there are limited to no support mechanisms available. Those that exist are not perceived as being useful or adequately functional.
- F Limited content management tools**

There are very few features that help individuals better manage and organize the content they receive.

Design opportunities

We identified six opportunities to address the design gaps that contribute to the proliferation of this harm.

Design Opportunity 1

Securing and/or modifying account information



Product design gaps addressed

A Easy access to personal identifying data

Design Opportunity 2

Improving verification & permission mechanisms



Product design gaps addressed

B Limited verification and consent-focused features for contacts and groups

Design Opportunity 3

Providing accessible & tailored security & privacy controls



Product design gaps addressed

C Generalized and hidden privacy & security controls for contacts & groups

Design Opportunity 4

Managing access to modified & third-party supporting platforms



Product design gaps addressed

D Infringement by modified (MOD) & third-party supporting apps ecosystem

Design Opportunity 5

Providing support mechanisms & emergency controls



Product design gaps addressed

E Limited support and lack of adequate reporting mechanisms

Design Opportunity 6

Improving administrative & management tools



Product design gaps addressed

F Limited content management tools

Click below to learn more about all design opportunities

Design opportunities

3.

Vulnerability to **manipulation** (misleading content, mis/disinformation) **or exposure to offensive content**



This harm covers the use of private messaging platforms to knowingly and unknowingly spread content that can be perceived as being hateful, offensive and/or misleading such as pornography, violent images and videos, and misinformation.

Individual's experience of this harm

The circulation of offensive or misleading content on platforms was of high concern for the participants we spoke to in Nigeria and of medium to high concern for the participants we spoke to in Colombia. However, participants in the US largely opposed interventions geared at addressing this harm. This exposed two contradicting perspectives on ways to address this harm:

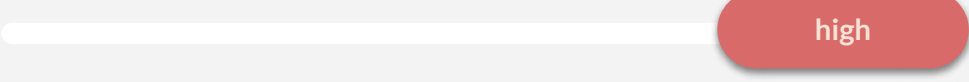
- **The Colombian & Nigerian perspective** - For most participants in Colombia and Nigeria, tackling this harm was important, particularly regarding the circulation of pornography. Tackling misinformation was also perceived as important, and participants in both countries placed great trust in the existence of a potential third-party organization that could be tasked with addressing the harm. Still, participants in both countries expressed some skepticism related to the specific ways that an intervention could effectively address this harm.
- **The US perspective** - Most participants we spoke to in the US were very vocal in expressing their concern that any efforts to address this harm by private messaging platform providers would likely have a negative impact on freedom of speech. Instead, American participants believed that the onus was on individuals themselves, not only to discern if something was misleading or correct but also to know how they could protect themselves, if they wanted to, from different forms of offensive content. This belief was particularly heightened for any intervention geared at the circulation of misinformation. Here, participants expressed overwhelming distrust in the involvement of any third-party organization that might be given the authority to address this harm. Political division, among other factors, would make the role of such an organization extremely polarizing.

The map on the next page presents a cross-country perspective on the circulation of offensive or misleading content on platforms from the participants in Colombia, Nigeria, and the United States. Particular attention is paid to the design gaps that contribute to the widespread experience of this harm by the participants we spoke with.

Level of concern expressed by participants

The scales below reflect the relative range of concern that participants we spoke with expressed for this harm across different countries.


Nigeria

Low  High

Colombia

Low  High

USA

Low  High

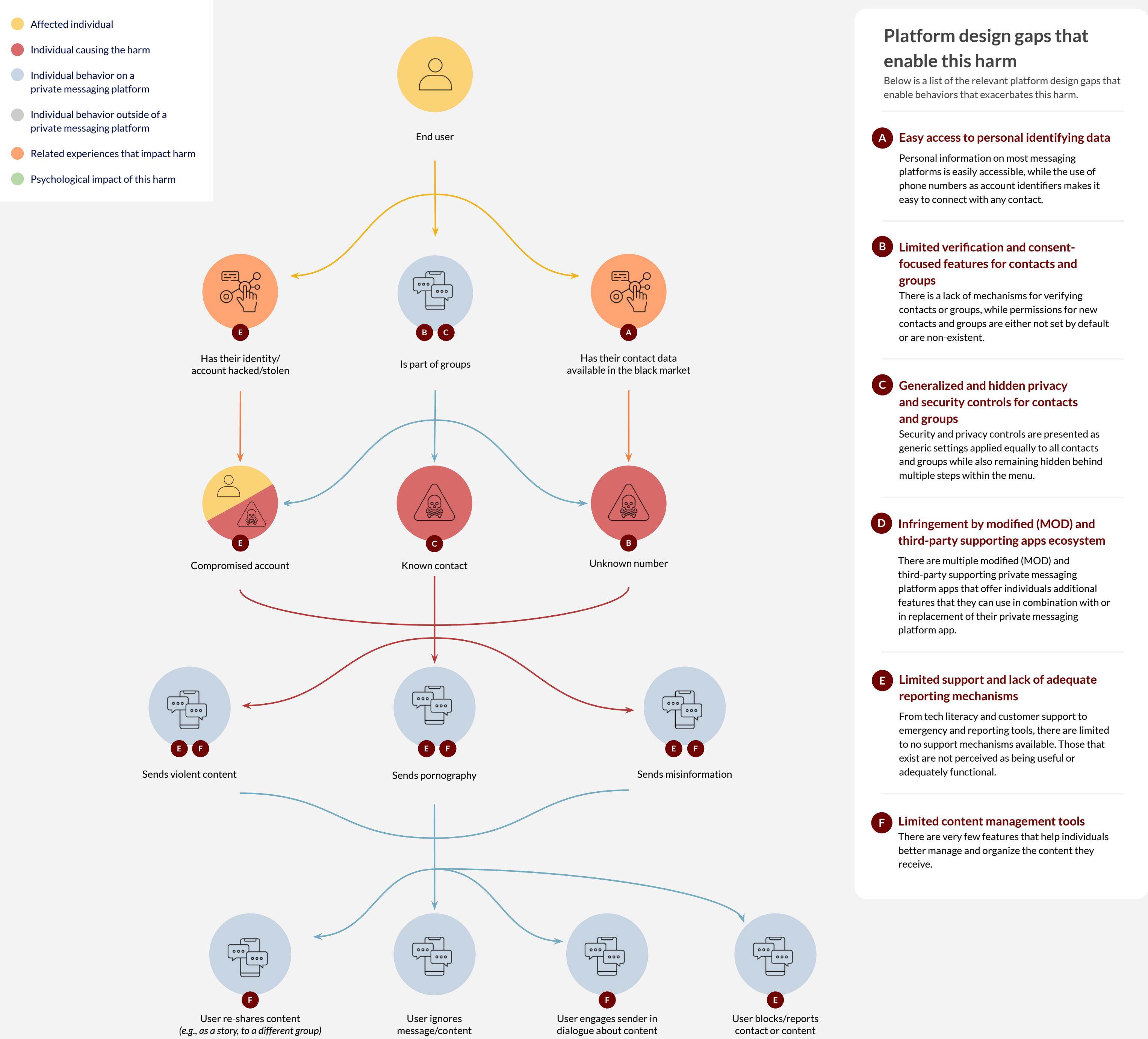
“Misinformation is just a part of the internet and it is people's responsibility to know that and look out for themselves. Tech band-aids feel like they are not enough.”

24-year-old man in the US, using Signal, and Telegram

“I follow up with a phone conversation and see how true it is or go online to verify that story before I choose to re-broadcast it. But in some cases, many people don't verify, they just repost and repost, and it causes panic, and in less than 1 to 3 hours, they find out it's fake.”

38-year-old Nigerian man

Understanding the vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content - illustrative process



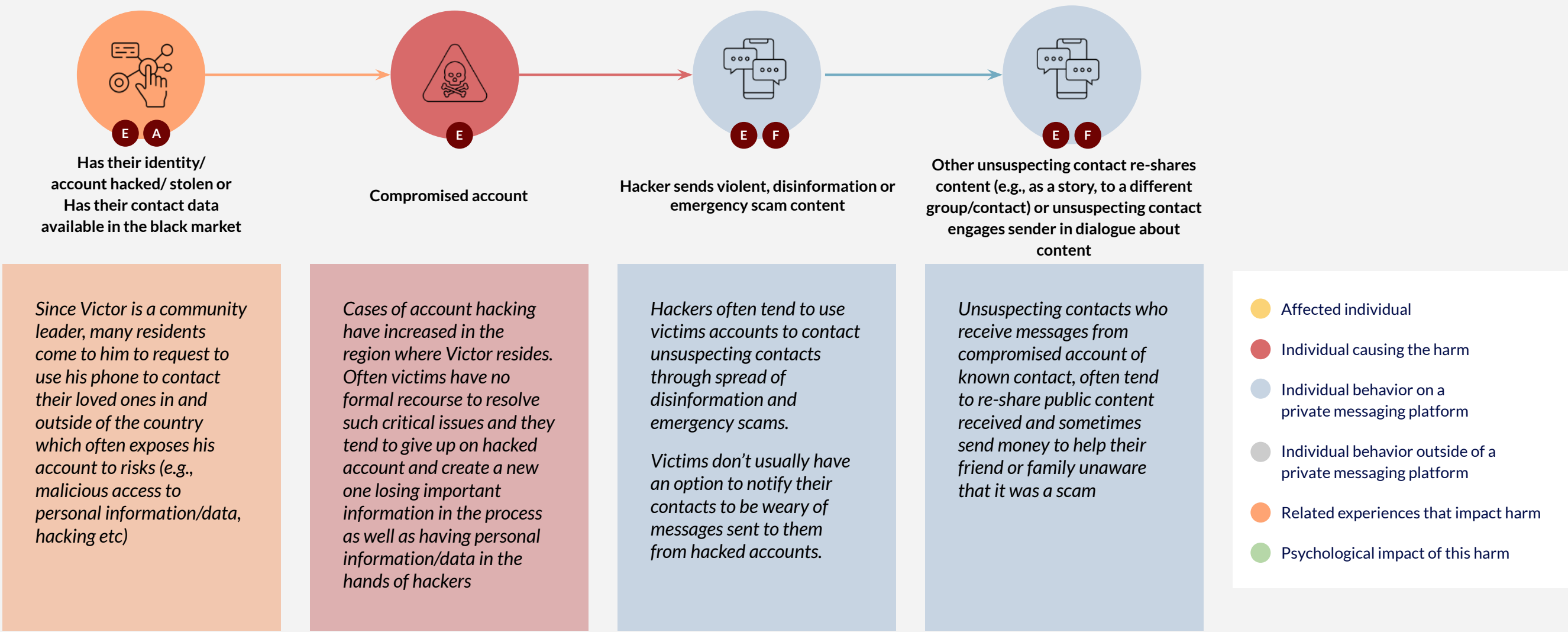
Understanding the vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content - illustrative journey



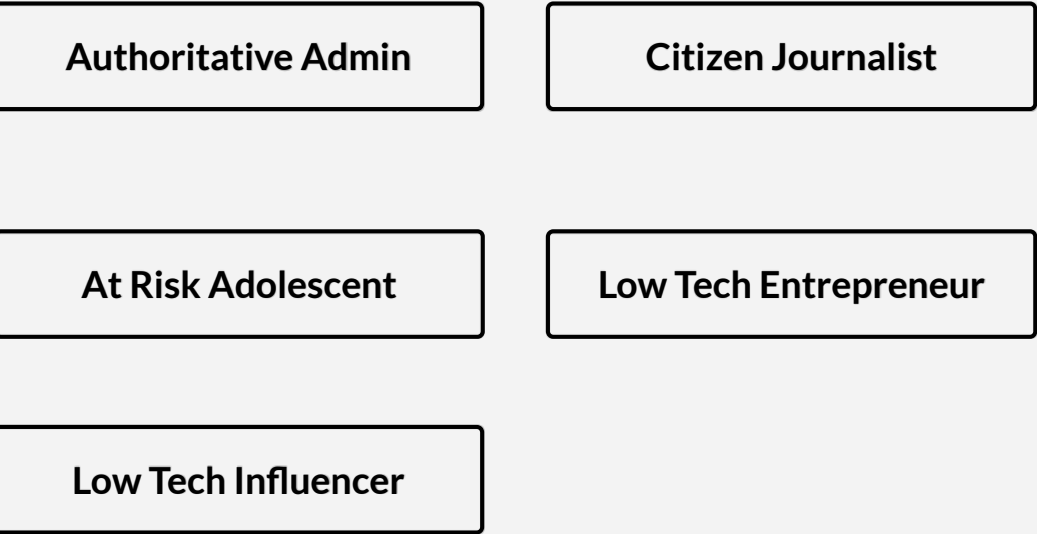
Victor - Citizen Journalist

Victor is a 38-year-old development manager and community leader. He resides in northern Nigeria where he works with community organizations in assisting locals in empowerment initiatives and emergency support interventions. He primarily uses WhatsApp alongside Facebook Messenger and sometimes Telegram to communicate and organize community activities.

“I follow up with a phone conversation and see how true it is or go online to verify that story before I choose to re-broadcast it. But in some cases many people don't verify, they just repost and repost and it causes panic and in less than 1 to 3 hours they find out it's fake.”



Explore the relevant experiences related to this harm



Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

- A Easy access to personal identifying data**
Personal information on most messaging platforms is easily accessible, while the use of phone numbers as account identifiers makes it easy to connect with any contact.
- E Limited support and lack of adequate reporting mechanisms**
From tech literacy and customer support to emergency and reporting tools, there are limited to no support mechanisms available. Those that exist are not perceived as being useful or adequately functional.
- F Limited content management tools**
There are very few features that help individuals better manage and organize the content they receive.

Design opportunities

We identified six opportunities to address the design gaps that contribute to the proliferation of this harm.

Design Opportunity 1

Securing and/or modifying account information



Product design gaps addressed

A Easy access to personal identifying data

Design Opportunity 2

Improving verification & permission mechanisms




Product design gaps addressed

B Limited verification and consent-focused features for contacts and groups

Design Opportunity 3

Providing accessible & tailored security & privacy controls



Product design gaps addressed

C Generalized and hidden privacy & security controls for contacts & groups

Design Opportunity 4

Managing access to modified & third-party supporting platforms



Product design gaps addressed

D Infringement by modified (MOD) & third-party supporting apps ecosystem

Design Opportunity 5

Providing support mechanisms & emergency controls



Product design gaps addressed

E Limited support and lack of adequate reporting mechanisms

Design Opportunity 6

Improving administrative & management tools



Product design gaps addressed

F Limited content management tools

Click below to learn more about all design opportunities:

Design opportunities

4.

Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment

This harm covers the direct misuse of private messaging platforms by adults as distinct from those affecting youth and children.

This includes common digital misuses such as the use of the platforms for scamming, conducting fraud schemes, hacking, or causing deliberate harassment.



Individual's experience of this harm

While the misuse of private messaging platforms was of extremely high concern to the participants we spoke to in Nigeria and Colombia, participants in the US did not mention commonly experiencing or being as concerned about this harm. Colombian and Nigerian participants shared similar concerns regarding platform misuse, yet Colombian participants experienced these misuse more frequently in connection with physical assault or other associated crimes. These crossover digital-to-physical crimes were often linked by individuals to the illegal sale of leaked contact databases that contain phone numbers and other personal information. For Nigerian participants, potential exposure to fraud or other scams was a primary risk associated with WhatsApp and other private messaging apps. The American participants we spoke with were instead more worried about the potential use of the platforms for aiding in organized crime, such as terrorism or media manipulation. That said, it is possible that this concern would have shown up much more prominently if our research had targeted specific groups with different vulnerabilities, such as the elderly.

The list below presents the most common forms of misuse concerns we heard from the participants we spoke with:

- **Hacking** (e.g., cloning of private messaging app account)
- **Scamming**
- **Blackmailing and extortion**
- **Fraud**
- **Harassment and/or stalking**
- **Robbery**

In the efforts to protect themselves against the harms listed above, participants in Nigeria and Colombia used distinct mechanisms. Below is a snapshot of differing behaviors across the two countries:

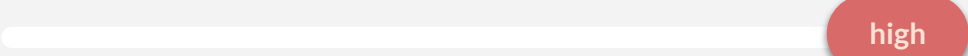
- In Nigeria the primary mechanism used by most participants was to turn on two-step verification. Individuals who are more technologically comfortable also relied on the use of third-party apps to verify links or for caller identification. Only a select few of those who were the most technologically comfortable knew that they could change their privacy settings so only contacts could add them to groups.
- In Colombia two-step verification was not mentioned by any of the participants we spoke with, instead participants spoke of having a general degree of 'vigilance' when communicating on the platforms. Like Nigeria, some technologically comfortable individuals also turned to third-party apps to verify links or for caller identification.

The map on the next page presents a cross-country perspective on the misuse of private messaging platforms from participants in Colombia, Nigeria and the United States. Particular attention is paid to the design gaps that contribute to the widespread experience of this harm by the participants we spoke with.

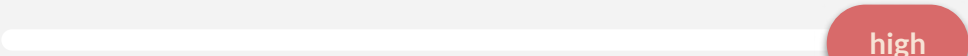
Level of concern expressed by participants

The scales below reflect the relative range of concern that participants we spoke with expressed for this harm across different countries.

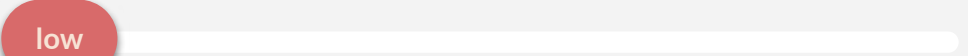
Nigeria

Low  High

Colombia

Low  High

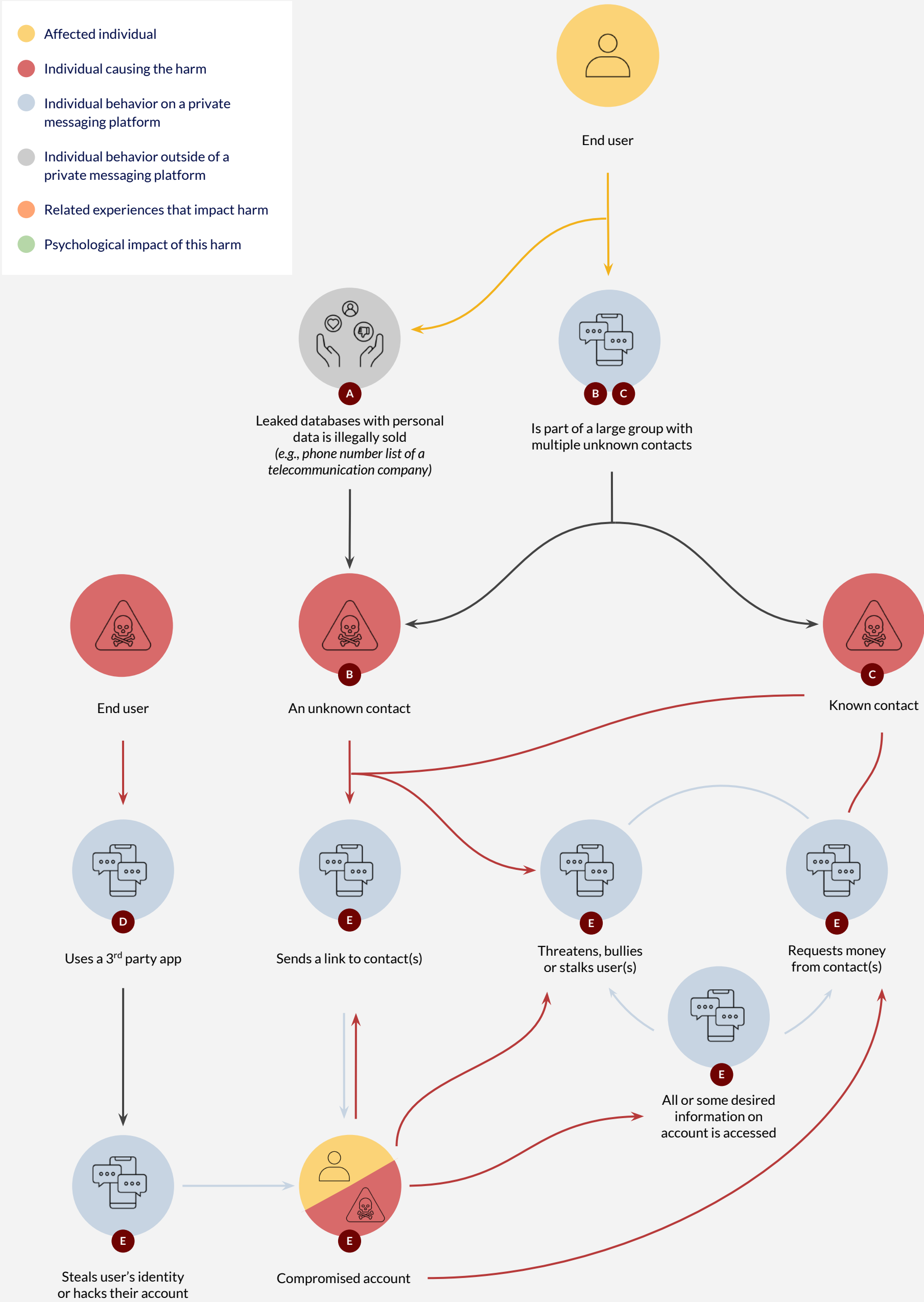
USA

Low  High

“I set up two-step verification because anyone can takeover a WhatsApp account and mess with people. People get access through by dropping links on groups.”

49-year-old Nigerian man

Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment - illustrative process



Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

- A Easy access to personal identifying data**
Personal information on most messaging platforms is easily accessible, while the use of phone numbers as account identifiers makes it easy to connect with any contact.
- B Limited verification and consent-focused features for contacts and groups**
There is a lack of mechanisms for verifying contacts or groups, while permissions for new contacts and groups are either not set by default or are non-existent.
- C Generalized and hidden privacy and security controls for contacts and groups**
Security and privacy controls are presented as generic settings applied equally to all contacts and groups while also remaining hidden behind multiple steps within the menu.
- D Infringement by modified (MOD) and third-party supporting apps ecosystem**
There are multiple modified (MOD) and third-party supporting private messaging platform apps that offer individuals additional features that they can use in combination with or in replacement of their private messaging platform app.
- E Limited support and lack of adequate reporting mechanisms**
From tech literacy and customer support to emergency and reporting tools, there are limited to no support mechanisms available. Those that exist are not perceived as being useful or adequately functional.

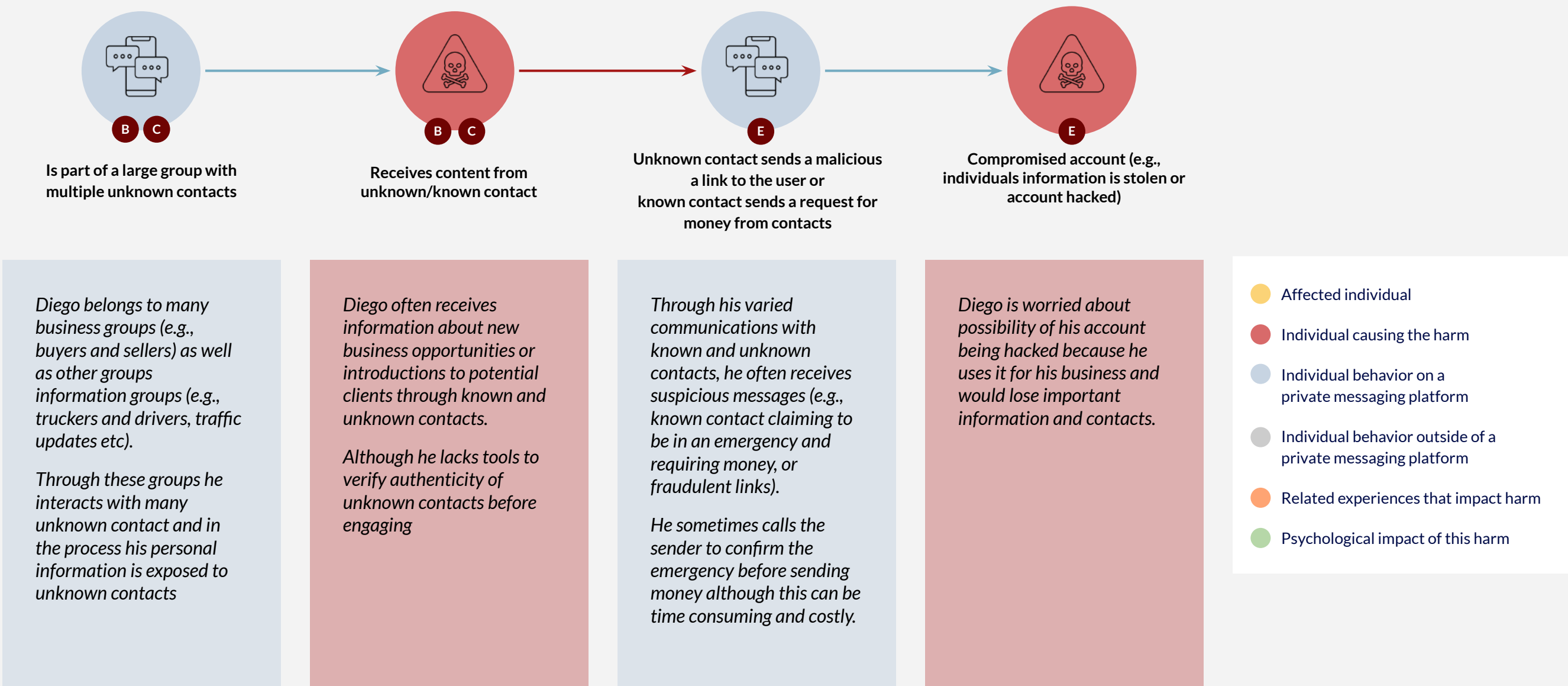
Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment - illustrative journey



Diego - Low Tech Entrepreneur

Diego is 44 years old and runs a small transport company in Villeta. Due to the nature of his job, he is constantly multi-tasking, chasing payments to coordinating and resolving transportation issues. He heavily relies on WhatsApp and Telegram for the day-to-day operations of his business. He belongs to many groups on WhatsApp, and he finds these groups to be very valuable to him in marketing his business. He also uses private messaging apps to receive and share important traffic/emergency information with other drivers in his region.

“ I use an app called Troller, I don't have a good memory.... and with this can identify if a call that comes to my cell phone is reliable. It only works with calls, and there I can see if it is reliable or a scam or robbery.”



Explore the relevant experiences related to this harm

- At Risk Adolescent
- Citizen Journalist
- Low Tech Influencer
- Low Tech Entrepreneur

Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

- B Limited verification and consent focused features for contacts and groups**

There is a lack of mechanisms for verifying contacts or groups, while permissions for new contacts and groups are either not set by default or are non-existent.
- C Generalized and hidden privacy and security controls for contacts and groups**

Security and privacy controls are presented as generic settings applied equally to all contacts and groups while also remaining hidden behind multiple steps within little-used menu structures.
- E Limited support and lack of adequate reporting mechanisms**


From tech literacy and customer support to emergency and reporting tools, there are limited to no support mechanisms available. Those that exist are not perceived as being useful or adequately functional.

Design opportunities

We identified five opportunities to address the design gaps that contribute to the proliferation of this harm.

Design Opportunity 1

Securing and/or modifying account information




Product design gaps addressed

A Easy access to personal identifying data

Design Opportunity 2

Improving verification & permission mechanisms




Product design gaps addressed

B Limited verification and consent-focused features for contacts and groups

Design Opportunity 3

Providing accessible & tailored security & privacy controls

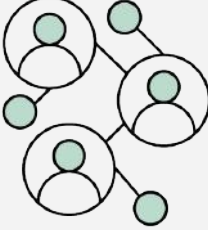


Product design gaps addressed

C Generalized and hidden privacy & security controls for contacts & groups

Design Opportunity 4

Managing access to modified & third-party supporting platforms




Product design gaps addressed

D Infringement by modified (MOD) & third-party supporting apps ecosystem

Design Opportunity 5

Providing support mechanisms & emergency controls



Product design gaps addressed

E Limited support and lack of adequate reporting mechanisms

Click below to learn more about all design opportunities:

Design opportunities

5.

Vulnerability to encryption and data breaches via modified and third-party supporting platforms

This harm covers the different ways that private messaging platforms security, privacy and encryption features are bypassed by users through the use of modified and third-party supporting private messaging platform apps; and the detrimental impact their adoption has on other individuals.



Individual's experience of this harm

This harm was expressed as being of medium to high concern for some of the participants we spoke to in Nigeria and Colombia but was not mentioned by any user we spoke to in the US. In both Nigeria and Colombia, participants rely heavily on WhatsApp as a standard and ubiquitous form of communication. participants in both countries reported expansive use of the app which goes beyond communication between friends and family (e.g., work, news, networking, dating, emergency reporting, communication with businesses and services). In their pursuit of additional features to give them more control, some participants have taken to using modified (MOD) versions of private messaging platforms or third-party supporting apps. Some of these participants seem to not be aware that they are using a MOD private messaging platform app. Those that are, or participants who know someone that uses them, are concerned about the privacy and security risks they pose to others. But these concerns are not always sufficient to get them to stop using MODs entirely.

While reasons for using MOD and third-party supporting apps vary, below are some of the most common reasons we heard from participants:

Modified private messaging platforms

- **Individuals seeking greater privacy while communicating.** These individuals seek additional privacy controls that help them avoid social pressures. MODs allow them the ability to toggle on and off the communication of their own actions on WhatsApp (e.g., user is online, read receipts, user is writing, last seen, private mode for chatting)
- **Individuals seeking greater security while communicating** (e.g., app lock, password lock for particular chats, ability to hide chats)
- **Individuals seeking better content management** (e.g., separate folders for DMs and group chats, configuration of automatic reply messages, ability to share large media files, recall and scheduling of WhatsApp messages, disabling of app notifications)
- **Individuals seeking greater customization of the apps user interface design** (e.g., changing fonts, features, and colors)
- **Individuals seeking to preserve access to deleted messages** (e.g., anti-delete features)

Third-party supporting apps

- Parents seeking to monitor their children's account
- Partners seeking to monitor their corresponding partners
- Individuals seeking private message reading
- Individuals seeking to preserve access to deleted messages
- Individuals seeking to download/ copy the stories of other contacts
- Individuals seeking to get easier contact adding features (e.g., tapping a phone to get the WhatsApp account of another user)

The map on the next page presents a cross-country perspective on the use of modified (MOD) & third-party supporting platforms from participants in Colombia, Nigeria, and the United States. Particular attention is paid to the design gaps that contribute to the widespread experience of this harm by the participants we spoke with.

Level of concern expressed by participants

The scales below reflect the relative range of concern that participants we spoke with expressed for this harm across different countries.

Nigeria

Low medium to high High

Colombia

Low medium to high High

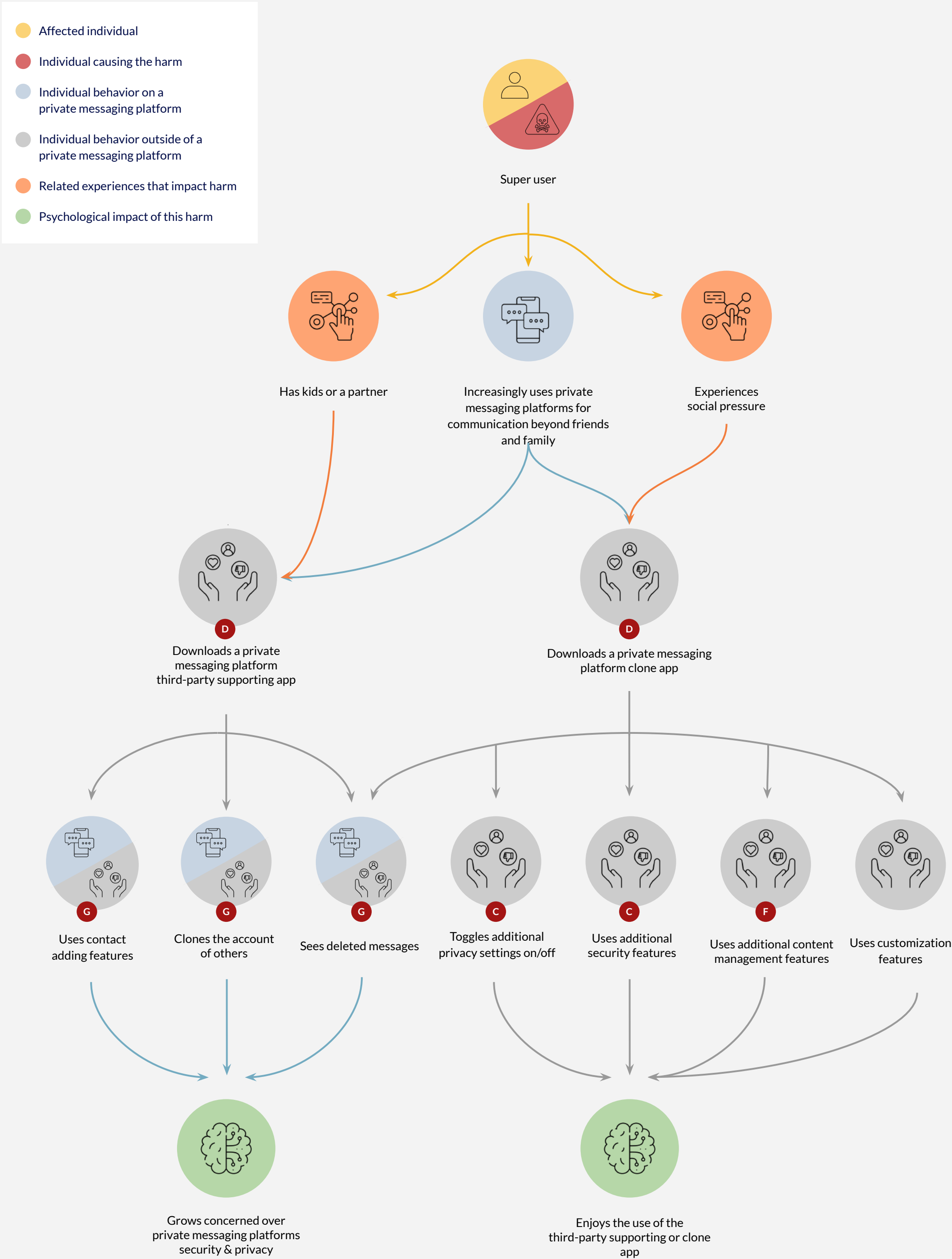
USA

Low none High

“There is an app that duplicates WhatsApp accounts. I used to use it with my daughter so I could have more control over who she talks to, what she posts, the conversations she has, and until what time she uses the cell phone. After some time we stopped using it because she understood and educated herself about the use and management of these platforms.”

28 -year-old Colombian woman

Vulnerability to encryption and data breaches via modified and third-party supporting platforms - illustrative process

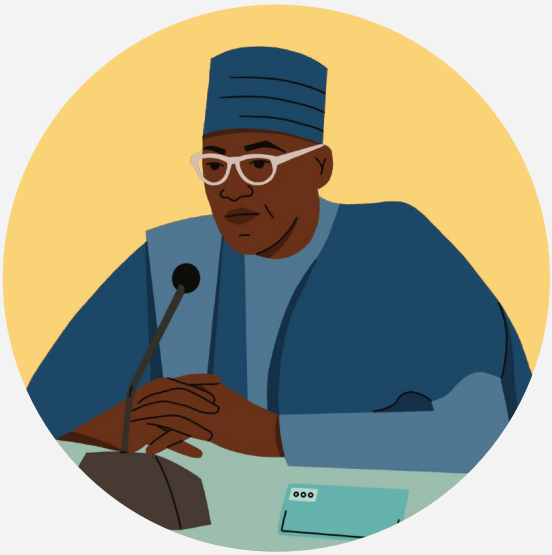


Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

- C Generalized and hidden privacy and security controls for contacts and groups**
Security and privacy controls are presented as generic settings applied equally to all contacts and groups while also remaining hidden behind multiple steps within little-used menu structures.
- D Infringement by modified (MOD) and third-party supporting apps ecosystem**
There are multiple modified (MOD) and third-party supporting private messaging platform apps that offer individuals additional features that they can use in combination with or in replacement of their private messaging platform app without others knowing.
- F Limited content management tools**
There are very few features that help individuals better manage and organize the content they receive.
- G Lack of transparency regarding access to personal data**
There are gaps around who can access, use, and potentially misuse user data (e.g., how and if companies and governments can access user data). At the same time, messaging platforms don't communicate transparently and in an user-friendly way how they manage and protect personal data.

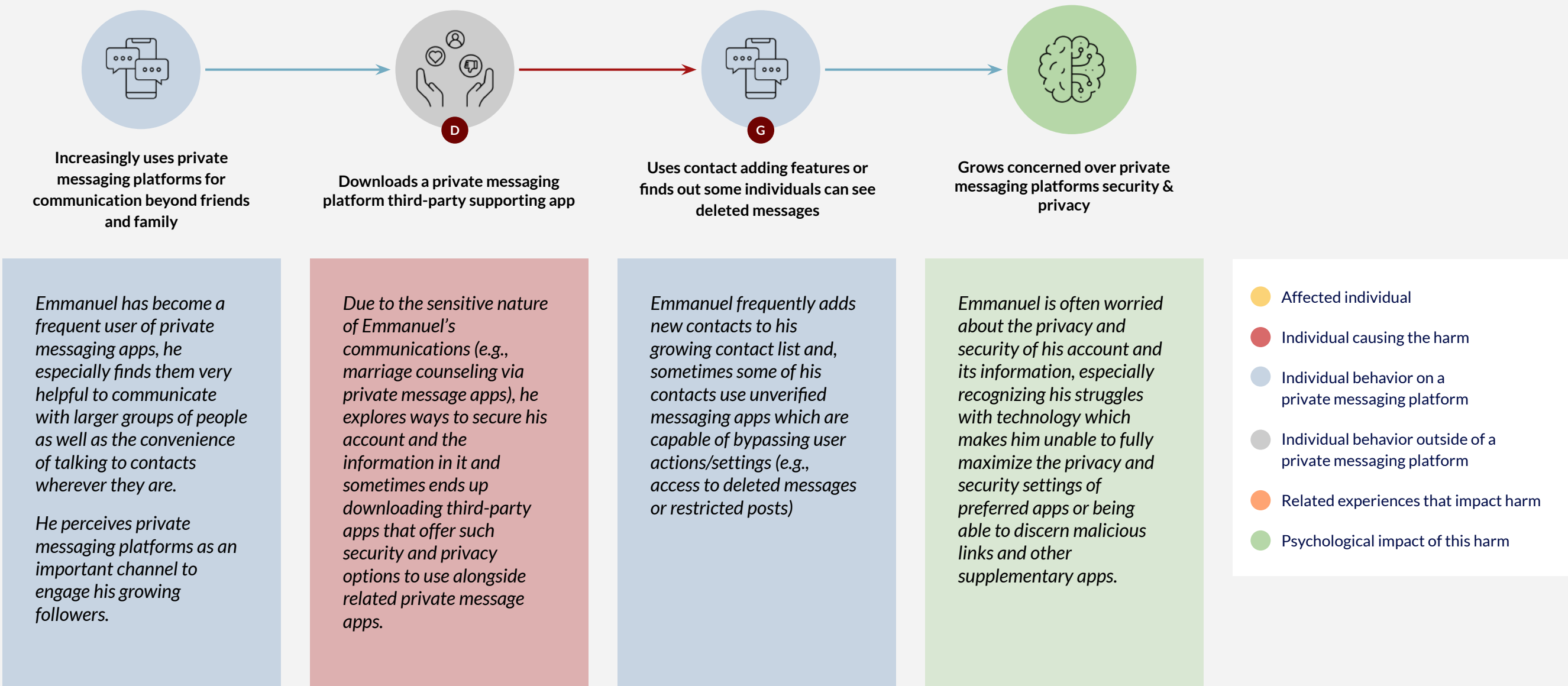
Vulnerability to encryption and data breaches via modified and third-party supporting platforms - illustrative journey



Emmanuel - Low Tech Influencer

Emmanuel is a 48- year-old church leader who lives in Lagos, Nigeria. He runs a local church and is also an inspirational speaker and life coach to his followers. He often meets his followers through scheduled public gatherings, however after he started using a private messaging app, he quickly realized the convenience it offered through individual and group communications, so he now heavily uses private messaging apps to engage his followers. He primarily uses WhatsApp to communicate, but he also connects on other platforms like Telegram in order to reach as many followers as possible, wherever they are most comfortable.

“Sometimes, especially when counseling, the information shared is very sensitive. For instance, if you are doing counseling and you should separate from your husband, this is sensitive and you need security.”



Explore the relevant experiences related to this harm

- Authoritative Admin
- Citizen Journalist
- At Risk Adolescent
- Globe Trotter

Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

- D** **Infringement by modified (MOD) and third-party supporting apps ecosystem**

There are multiple modified (MOD) and third-party supporting private messaging platform apps that offer individuals additional features that they can use in combination with or in replacement of their private messaging platform app without others knowing.
- G** **Lack of transparency regarding access to personal data**


There are gaps around who can access, use, and potentially misuse user data (e.g., how and if companies and governments can access user data). At the same time, messaging platforms don't communicate transparently and in an user-friendly way, how they manage and protect personal data.

Design opportunities

We identified four opportunities to address the design gaps that contribute to the proliferation of this harm.

Design Opportunity 3

Providing accessible & tailored security & privacy controls

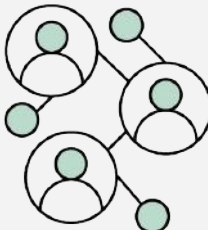


Product design gaps addressed

C Generalized and hidden privacy & security controls for contacts & groups

Design Opportunity 4

Managing access to modified & third-party supporting platforms

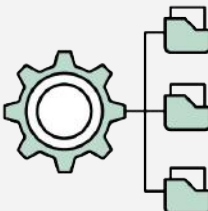


Product design gaps addressed

D Infringement by modified (MOD) & third-party supporting apps ecosystem

Design Opportunity 6

Improving administrative & management tools




Product design gaps addressed

F Limited content management tools

Design Opportunity 7

Providing data use transparency & the ability to manage data



Product design gaps addressed

G Lack of transparency regarding access to personal data

Click below to learn more about all design opportunities:

Design opportunities

6.

Vulnerability to digital surveillance and monitoring

This harm covers the different ways users on private messaging platforms experience and perceive infringement of their privacy. It speaks to concerns of surveillance and monitoring of conversations by those in power, be it for business reasons (targeted advertising) or political reasons (surveillance of critics and activists).



Individual's experience of this harm

This harm was of low to medium concern for participants we spoke to in Nigeria and Colombia. For participants in the US, this was of much higher concern. Apart from activists and journalists, Colombian and Nigerian participants reported that they are not worried about government surveillance since they don't believe that they have anything to hide. Some participants even advocated for government surveillance to curb criminal activities on digital platforms. These individuals were more concerned about access and/or monitoring of private conversations by other entities/contacts.

By contrast, many users in the US are highly concerned about the infringement of their privacy on private messaging platforms. The US is comprised of a variety of users who all agreed on the need for stronger measures to protect users' privacy and security online. Activists in the US reported the use of sophisticated tools for surveillance by government agencies and other tech organizations. Many privacy-sensitive users have resorted to using other forms of communications outside of private messaging apps (e.g., emails, in-person) to pass sensitive information.

Tracking of movements using geolocation was reported as the main concern among activists/journalists in both Colombia and the US. These location services are relied on by activists to rally support or help during demonstrations, especially in Colombia. But they are also used by authorities to track the gathering of demonstrators which can lead to violent confrontations. Activists in the US are even warier of location data and often leave their phones behind for sensitive meetings. Methods of surveillance/monitoring of concerns to users in Nigeria, Colombia and the US include:

- Monitoring of conversations for targeted ads (e.g., through digital assistants Siri/Alexa)
- Monitoring and tracking of movements
- Using devices to eavesdrop
- Spying (e.g., in private messaging groups by law enforcement)
- Remote screen and audio recording

The map on the next page presents a cross-country perspective on surveillance and monitoring based on feedback from users in Colombia, Nigeria and the United States. Particular attention is paid to the design gaps that contribute to the widespread concerns about this harm among some of the users we spoke with.

Level of concern expressed by participants

The scales below reflect the relative range of concern that participants we spoke with expressed for this harm across different countries.

Nigeria

Low low to medium High

Colombia

Low low to medium High

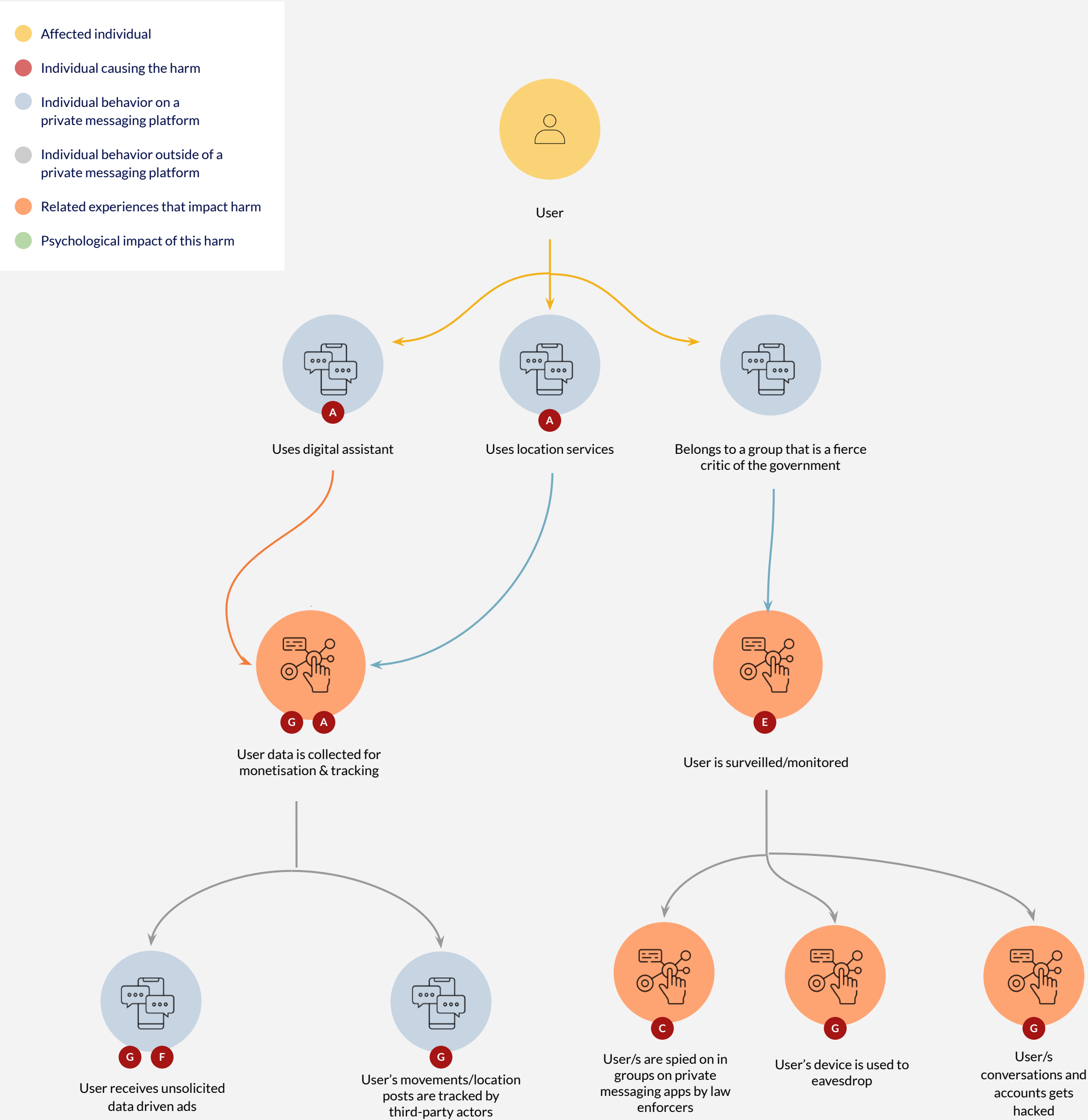
USA

Low high High

“During the protests WhatsApp helped a lot because people who were lost in the streets could easily locate us because Facebook would get blocked and the networks were blocked as well.”

24 -year-old Colombian activist

Vulnerability to digital surveillance and monitoring - illustrative process



Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

- A Easy access to personal identifying data**

Personal information on most messaging platforms is easily accessible, while the use of phone numbers as account identifiers makes it easy to connect with any contact.
- C Generalized and hidden privacy and security controls for contacts and groups**

Security and privacy controls are presented as generic settings applied equally to all contacts and groups while also remaining hidden behind multiple steps within complex menu structures.
- E Limited support and lack of adequate reporting mechanisms**

From tech literacy and customer support to emergency and reporting tools, there are limited to no support mechanisms available. Those that exist are not perceived as being useful or adequately functional.
- G Lack of transparency regarding access to personal data**

There are gaps around who can access, use, and potentially misuse user data (e.g., how and if companies and governments can access user data). And messaging platforms don't communicate transparently and in an user-friendly way how they manage and protect individual's data.

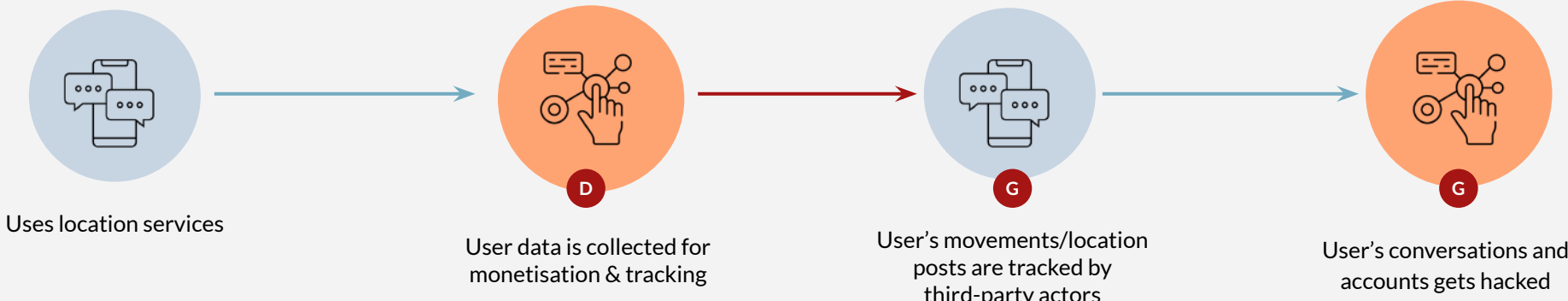
Vulnerability to digital surveillance and monitoring - illustrative journey



Barbara - Concerned Activist

Barbara is a 24-year-old Colombian who is self-employed and lives in Bogota. She is passionate about human rights and actively involved in protests and championing the rights of others. She is very concerned and protective of her privacy when using private messaging which deeply influences her adoption and usage of different platforms. Also, due to her activism, Barbara has become a target of government surveillance from time-to-time, so her safety is also becoming a cause for concern. She used to use WhatsApp as her primary private messaging app but switched to Telegram when WhatsApp updated its privacy policies, which made her distrustful of the platform.

“A password in this day and age feels rudimentary, because if someone really wants to, they can still access your account.”



Barbara uses location services frequently to share her location with friends and loved ones, especially during trips and geo-tagging posts on social media.

Besides social use, Barbara and her activist friends often use location services to find each other and rally support and help during street demonstrations.

Government agencies, including law enforcement, frequently collect/monitor location data of targeted groups or individuals for monitoring of movements and coordinated crackdowns against gatherings and demonstrations.

Other unauthorized contacts (e.g., law enforcement agents or stalkers) can track Barbara's location information to monitor her movements and activities due to the lack of better location privacy tools.

Barbara often receives strange links and contact invites from unknown contacts which leads her to believe that either someone is actively trying to get access to her account or she is being monitored. But due to a lack of sufficient verification and safety tools, she often struggles to discern the authenticity of a new contact or ways to better secure her account.

- Affected individual
- Individual causing the harm
- Individual behavior on a private messaging platform
- Individual behavior outside of a private messaging platform
- Related experiences that impact harm
- Psychological impact of this harm

Explore the relevant experiences related to this harm

- Globe Trotter

At Risk Adolescent
- Advantaged Activist

Concerned Activist

Platform design gaps that enable this harm

Below is a list of the relevant platform design gaps that enable behaviors that exacerbates this harm.

- D** **Infringement by modified (MOD) and third-party supporting apps ecosystem**

There are multiple modified (MOD) and third-party supporting private messaging platform apps that offer individuals additional features that they can use in combination with or in replacement of their private messaging platform app without others knowing.
- G** **Lack of transparency regarding access to personal data**


There are gaps around who can access, use, and potentially misuse user data (e.g., how and if companies and governments can access user data). At the same time, messaging platforms don't communicate transparently and in an user-friendly way how they manage and protect personal data.

Design opportunities

We identified seven opportunities to address the design gaps that contribute to the proliferation of this harm.

Design Opportunity 1

Securing and/or modifying account information




Product design gaps addressed

A Easy access to personal identifying data

Design Opportunity 2

Improving verification & permission mechanisms




Product design gaps addressed

B Limited verification and consent-focused features for contacts and groups

Design Opportunity 3

Providing accessible & tailored security & privacy controls

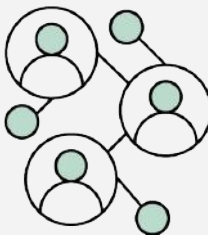


Product design gaps addressed

C Generalized and hidden privacy & security controls for contacts & groups

Design Opportunity 4

Managing access to modified & third-party supporting platforms




Product design gaps addressed

D Infringement by modified (MOD) & third-party supporting apps ecosystem

Design Opportunity 5

Providing support mechanisms & emergency controls




Product design gaps addressed

E Limited support and lack of adequate reporting mechanisms

Design Opportunity 7

Providing data use transparency & the ability to manage data



Product design gaps addressed

G Lack of transparency regarding access to personal data

Click below to learn more about all design opportunities:

Design opportunities



04 Design Opportunities

Design opportunities



Participants helped us uncover a range of design opportunities that private messaging platforms should consider to improve trustworthiness.

These design opportunities are presented as areas where platform providers can increase user trustworthiness while reducing exposure to the harms. We feature **seven** design opportunities that emerged from our research along with representative ideas for how these changes might be implemented. They are meant to be illustrative and likely come with other tradeoffs in practice that only private messaging platforms will be able to solve for. These ideas were lightly tested with participants in most cases.

While individuals are looking for progress on many fronts, addressing the design opportunities here can be an important step for platform providers to signal their willingness to commit to positive change.

We should also note that these design opportunities are probably not sufficient to truly change the dynamics around trustworthiness. Research participants called out a number of fundamental opportunities—greater awareness regarding privacy and security, improved processes for updating and sharing policy changes, and changes in business models related to how user data is mined – as equally important steps they would like platform providers to take to earn and maintain their trust.

Each design opportunity includes information on:

- The specific product **design gap** the opportunity addresses
- The **harms** the opportunity could potentially have impact on
- The relevant messaging platform **pain points** that individuals experience and is addressed by the relevant design opportunity
- Cross-cutting **design principles** that will be important for messaging platforms to keep in mind when developing platform design changes geared at this opportunity
- A set of **platform design ideas** that illustrate design directions private messaging platforms could take

As you explore the design opportunities, it will be important to keep in mind that

1. Every platform design idea has upsides as well as potential downsides (e.g., unintended consequences) for building trustworthiness. We have tried to raise these where possible.
2. All platform design ideas were either lightly tested, discussed or raised by participants and will require additional rounds of testing and refinement with a variety of participants to understand how perceptions differ across countries and user types.
3. The design opportunities and platform ideas we have included are agnostic to any one type of private messaging platform. However, our research was primarily focused on understanding the use and needs of WhatsApp, FB Messenger, Telegram, and Signal users.

Design principles

Across the design opportunities we identified a common set of principles to guide the design of features to improve the trustworthiness, privacy, and security of private messaging platforms.

While these design principles are cross-cutting they address specific pain points within each opportunity. As you explore the design opportunities you will see what design principles apply to each opportunity and the specific pain points they address.

DESIGN PRINCIPLE 1

Surface information related to trust, privacy and security so that it is accessible to users in the places and moments that it is most relevant and actionable to them

DESIGN PRINCIPLE 2

Extend user control over privacy and security into all aspects of the platform experience where they feel at risk

DESIGN PRINCIPLE 3

Default to a high/the highest level of security whenever possible while providing easy and timely access for users to adjust their preferences to suit specific situations

DESIGN PRINCIPLE 4

Offer flexibility so that users can tailor their trust, privacy and security preferences to specific relationships at the level of granularity that is most meaningful to them

DESIGN PRINCIPLE 5

Instill a common mental model for how trust and security should work to cement safer practices in communications

DESIGN PRINCIPLE 6

Communicate issues related to privacy and security in simple, user-friendly language so users always understand what is at stake, and can make informed decisions


DESIGN PRINCIPLE 7

Make redressal paths simple and clear so users know who to turn to and what to expect when concerns arise

Design opportunities at a glance

Design Opportunity 1

Ability to secure and/or modify account information




Platform design gap addressed

A Easy access to personal identifying data

Design Opportunity 2

Improving verification & permission mechanisms




Platform design gap addressed

B Limited verification and consent-focused features for contacts and groups

Design Opportunity 3

Providing accessible & tailored security & privacy controls

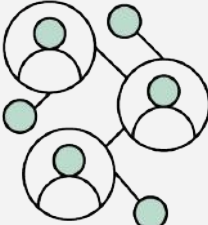


Platform design gap addressed

C Generalized and hidden privacy & security controls for contacts & groups

Design Opportunity 4

Ability to manage access to modified & third-party supporting platforms




Platform design gap addressed

D Existence of modified (MOD) & third-party supporting apps ecosystem

Design Opportunity 5

Providing user support mechanisms & emergency controls

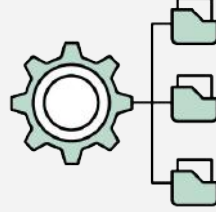


Platform design gap addressed

E Limited user support and lack of adequate reporting mechanisms

Design Opportunity 6

Improving administrative & management tools




Platform design gap addressed

F Limited content management tools

Design Opportunity 7

Providing data use transparency & the ability to manage data



Platform design gap addressed

G Lack of transparency regarding access to user data

How are harms to user trustworthiness addressed through these design opportunities?

While not all design opportunities will have an impact on all harms, some design opportunities can impact multiple harms. The chart below presents a summary view of the specific design opportunities that would impact each harm.

<div>HARMS IMPACTING USAGE & TRUSTWORTHINESS</div> <div>DESIGN OPPORTUNITIES</div>	1. Vulnerability to adverse mental health impacts	2. Vulnerability to targeted harassment for youth and young adults	3. Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content	4. Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment	5. Vulnerability to encryption and data breaches via modified and third-party supporting platforms	6. Vulnerability to digital surveillance and monitoring
1. Securing and/ or modifying account information	✓	✓	✓	✓	✓	✓
2 Improving verification & permission mechanisms	✓	✓	✓	✓		
3. Providing accessible & tailored security & privacy controls	✓	✓	✓	✓	✓	✓
4. Managing access to modified & third-party supporting platforms	✓	✓	✓	✓	✓	
5. Providing support mechanisms & emergency controls	✓	✓	✓	✓		✓
6. Improving administrative & management tools	✓	✓	✓		✓	
7. Providing data use transparency & managing data access loop holes	✓				✓	✓

Securing personal data & account information

This design opportunity addresses the platform design gap ‘A. Easy access to personal identifying data.’ It covers the different ways that private messaging platforms could help users better protect their personal identifying data from harm.

Platform design gap addressed

A. Easy access to personal identifying data

Personal information on most messaging platforms is easily accessible, while the use of phone numbers as account identifiers makes it easy to connect with any user.

Understanding the opportunity

Easy access to personal identifying data affects individuals in many ways. Using phone numbers for the account identifier, for example, increases the likelihood that a harmful or non-desired person can contact the user, or that the phone number and other relevant personal identifying data (e.g., name) become available on a black market via illegally acquired databases. This, in turn increases the vulnerability to platform misuses that the participants that we spoke with are most afraid of (e.g., hacking, scamming, blackmailing, fraud, harassment) and digital surveillance and monitoring.

In this section, we cover the harms that design improvements related to this opportunity could mitigate as well as the principles that will be important to keep in mind when making design changes geared at this opportunity area.

HARMS IT COULD IMPACT

1. Vulnerability to adverse mental health impacts

2. Vulnerability to targeted harassment for youth and young adults

3. Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content

4. Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment

6. Vulnerability to digital surveillance and monitoring

PAIN POINT 1

Inability to hide or limit access to personal data

Individuals need to be able to control how much personal data is accessible by others in different situations and social spaces (e.g., overarching privacy and security settings, in group invites, in contact invites).

PAIN POINT 2

Minimal controls for protecting personal data

In some messaging platforms, individuals are not able to have control over who sees their personal identifying data and how it becomes visible to others (e.g., inability to hide phone numbers, names, or about information on profile).

PAIN POINT 3

Low-security default settings

Most settings/controls on private messaging platforms are typically set to the lowest security and privacy options. This makes changing to higher settings more difficult for individuals to discover. It also invites social pressures that may keep individuals from changing them in situations where they feel at risk.

RELEVANT DESIGN PRINCIPLE #1

Surface information related to trust, privacy and security so that it is accessible to users in the places and moments that it is most relevant and actionable to them

RELEVANT DESIGN PRINCIPLE #2

Extend user control over privacy and security into all aspects of the platform experience where they feel at risk

RELEVANT DESIGN PRINCIPLE #3

Default to a high/the highest level of security whenever possible while providing easy and timely access for users to adjust their preferences to suit specific situations

Securing personal data & account information

Platform design ideas

The following are the preferred design ideas generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to inspire new features and design improvements for private messaging platforms providers.

Key

Applicability of idea

- Cross-cutting** - idea was welcomed by most users we spoke to across all three countries and identified archetypes
- Segmented** - idea was welcomed by some archetypes and/ or countries.

Type of idea

- New** - new idea that's not based on an adaptation of existing features
- Incremental** - idea is an adaptation or an addition to an existing feature

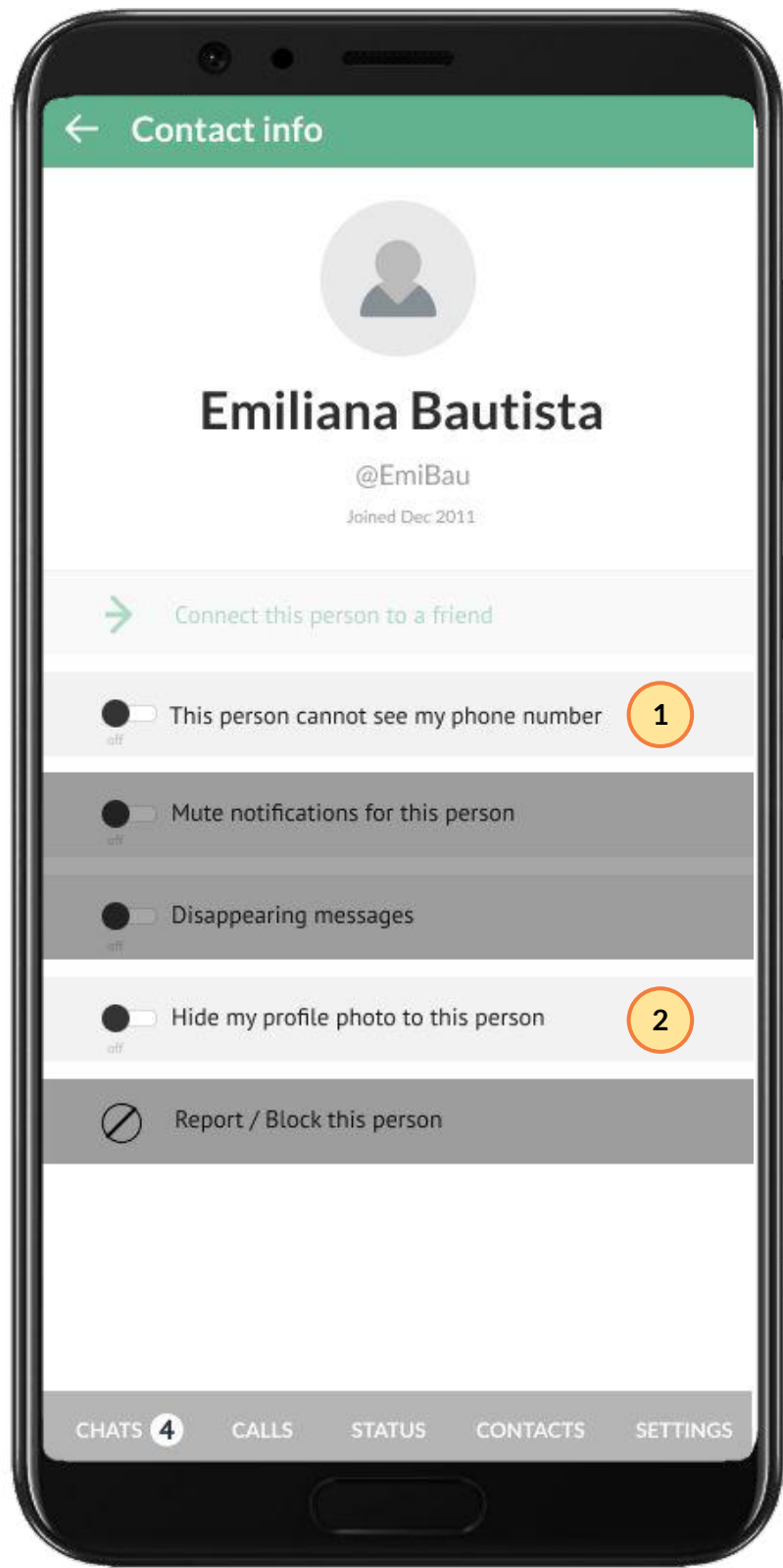
PROTECTION OF PERSONAL IDENTIFICATION DATA

Examples of relevant design ideas:

1A. Custom privacy for personal data

Users can completely hide and/ or selectively limit access to their data which is identified as personal. Options to hide personal data could be available via the main platform privacy and security settings, while limiting access could be done via contact or group invites.

- Cross-cutting idea**
- Incremental change**



Considerations

- User testing:** This idea was **prototyped** with users in all three countries
- Novelty:** This idea derives from the existing features (e.g., [Telegram's find by phone number](#) function)
- Popularity:** This idea, as presented within the group invite and contact and group settings, was highly popular across all three countries and showed potential for being useful across other ideas we tested
- Notable trade-offs:** The level of depth of controls could add some complexity and friction to the user experience, particularly for newer users

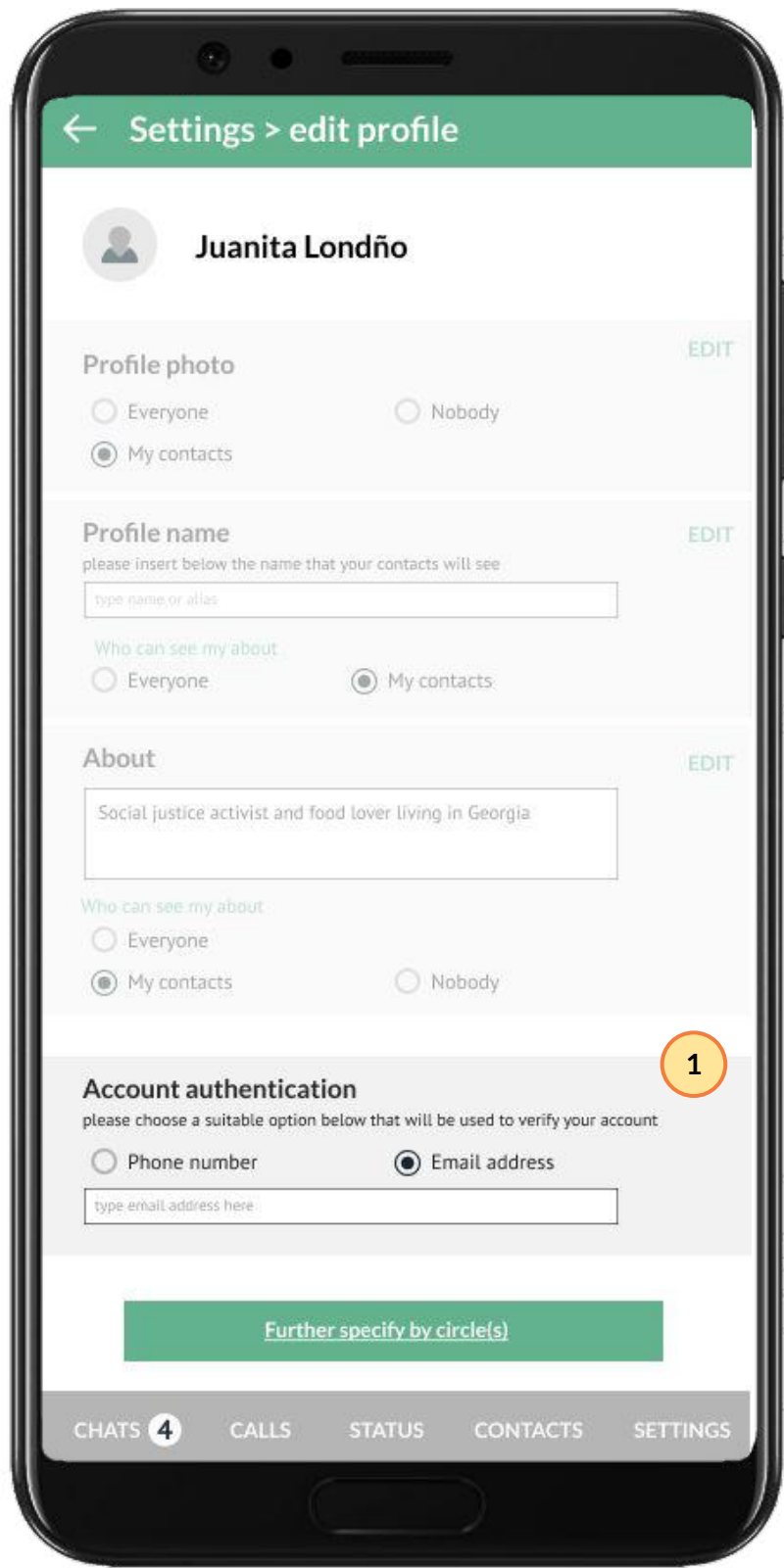
Key feature/s

- Enables users to adjust the accessibility of their phone number** - users can determine who is able to see their phone number allowing them to increase privacy and security for individual contacts and / or groups
- Enables users to adjust visibility of profile photo** - users can determine who is able to see their profile photo for individual contacts and / or groups

1B. User account identifier

User accounts on private messaging platforms are not identified by a phone number but by a user account name. If desired, users can choose to add their phone numbers.

- Cross-cutting idea**
- Incremental change**



Considerations

- User testing:** This idea was **discussed** with users in all three countries but **not prototyped/tested**
- Novelty:** This idea **derives** from the existing features (e.g., [Telegram's find by phone number](#) function)
- Popularity:** Given the idea was discussed but not tested, we were not able to state its popularity. However, when discussing it, users were highly interested in the ability to move away from a phone number as the main identification mechanism for their account.
- Notable trade-offs:** Shifting from a phone number to a user name may create a barrier to access, particularly for users with lower technological comfort. Also, illegally sold databases could contain user names too.

Key feature/s

- Enables users to choose a unique identifier that can be also be used to verify their account** - Has the potential to enhance user privacy and increase access/usage of private messaging platforms especially by users who may not have access to a sim card (e.g., undocumented persons, IDPs)

* features/options that lightly obscured are covered in other sections, the others that are darkened are already implemented by existing private messaging platforms

Improving verification & permission mechanisms

This design opportunity addresses platform design gap ‘B. Limited verification and consent-focused features for contacts and groups’. It covers the different ways that private messaging platforms could improve or create new mechanisms that help users verify the trustworthiness of contacts and groups.

Platform design gap addressed

B. Limited verification and consent-focused features for contacts and groups

There is a lack of mechanisms for verifying contacts or groups, while permissions for new contacts and groups are either not set by default or are non-existent.

Understanding the opportunity

User and group verification is a subject that is highly top-of mind for most users we spoke to in Nigeria and Colombia due to the tendency of users to extensively use messaging platforms as well as the commonality of platform misuse. However, In the US, verification via a messaging platform was highly controversial as it clashed with a desire and belief in digital anonymity. Most users we spoke to in the US tended to instead, opt for sharing as little information as possible on the platform and turn to physical interaction or vetting by trusted members of their circle for verification.

In this section we cover the harms that design improvements related to this opportunity could mitigate as well as the principles that will be important to keep in mind when making design changes geared at this opportunity area.

HARMS IT COULD IMPACT

1. Vulnerability to adverse mental health impacts

2. Vulnerability to targeted harassment for youth and young adults

3. Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content

4. Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment

PAIN POINT 1

Missing verification tools when it matters most

Assessing contact and group trustworthiness is most crucial at the moment when users choose to accept or ignore an invite. While most messaging platforms give users control over individual and group invites, they do not provide the basic profile information that users most need to inform these decisions before making them.

RELEVANT DESIGN PRINCIPLE #1

Surface information related to trust, privacy and security so that it is accessible to users in the places and moments that it is most relevant and actionable to them

PAIN POINT 2

Minimal verification and permission controls

While group and contact invites exist on many messaging platforms they provide minimal verification information or permission controls (e.g., no control over who sees their phone number, no control over who can message them directly, little information on group size and focus/ aim of a group). This limited information doesn’t help users to make informed decisions about the trustworthiness of the person or group and undermines their sense of confidence in these platforms more generally.

RELEVANT DESIGN PRINCIPLE #2

Extend user control over privacy and security into all aspects of the platform experience where they feel at risk

PAIN POINT 3

Problematic default permission settings

On many private messaging platforms more secure permission settings are typically turned off by default for new group or contact invites. While these default settings can be changed, it requires motivation, knowledge, and effort on the user’s part, which is a challenge, particularly for those with lower comfort with technology.

RELEVANT DESIGN PRINCIPLE #3

Default to a high/the highest level of security whenever possible while providing easy and timely access for users to adjust their preferences to suit specific situations

PAIN POINT 4

Generic and unadaptable controls

Most control options are designed to function like a blanket, affecting most/ all contacts or groups, however permissions and verification needs vary depending the type of interaction. For example, individuals don’t need extensive verification and permissions for a close family/ friend group but they do for a large group or when interacting with strangers, businesses, or services.

RELEVANT DESIGN PRINCIPLE #4

Offer flexibility so that users can tailor their trust, privacy and security preferences to specific relationships at the level of granularity that is most meaningful to them

Improving verification & permission mechanisms

Platform design ideas

The following are the preferred design ideas that were generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to serve as inspiration for new features and design improvements for private messaging platforms providers.

Key

Applicability of idea

- Cross-cutting** - idea was welcomed by most users we spoke to across all three countries and identified archetypes
- Segmented** - idea was welcomed by some archetypes and/or countries.

Type of idea

- New** - new idea that's not based on an adaptation of existing features
- Incremental** - idea is an adaptation or an addition to an existing feature

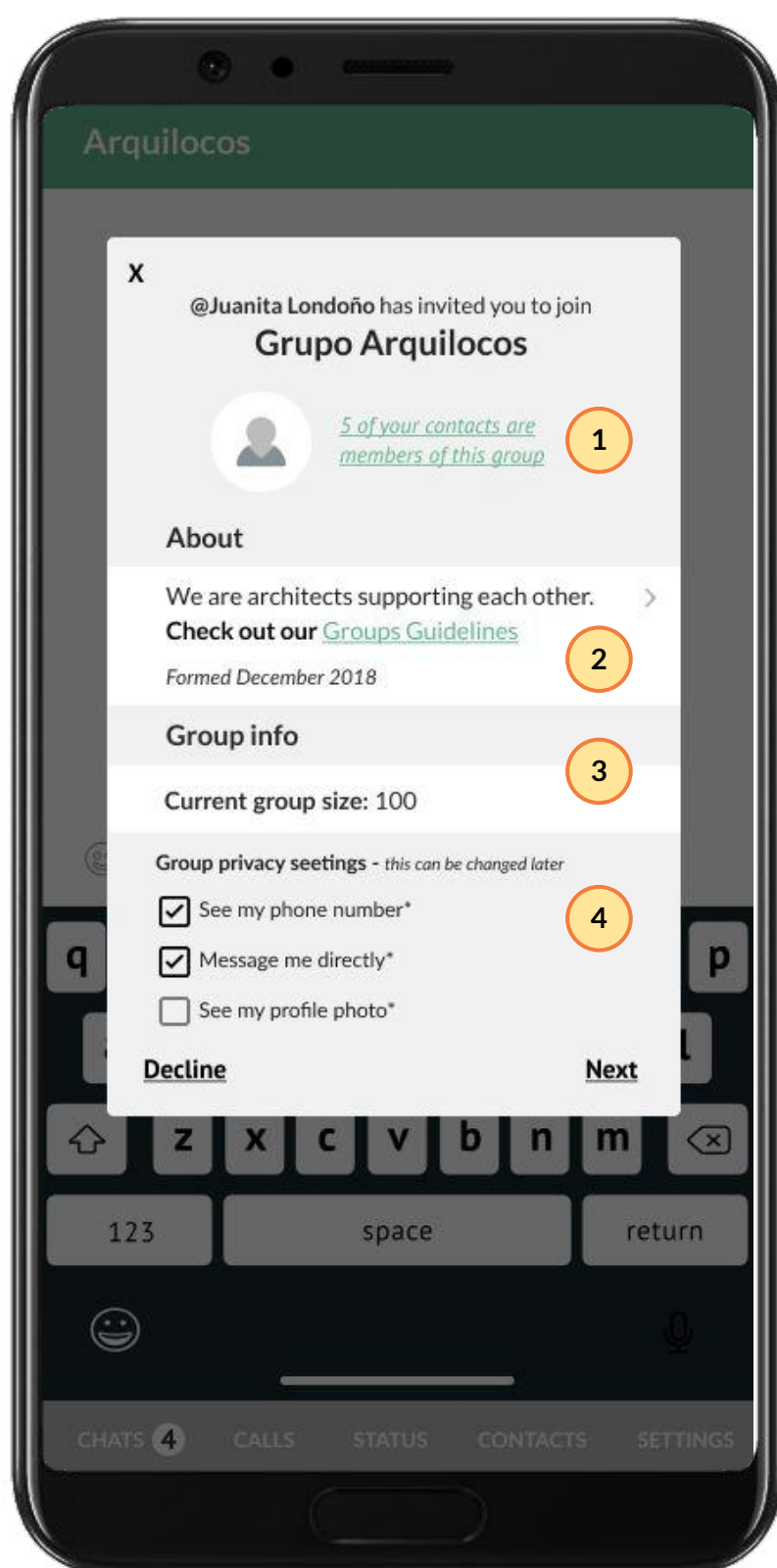
VERIFICATIONS & PERMISSIONS

Examples of relevant design ideas:

2A. Group invite

By default, allowing users to consent to join a group through a detailed group invite request. Users in all three countries acknowledged the need for certain group data (e.g., total group members, date of formation) to evaluate whether to join a group or not.

● Cross-cutting idea ● Incremental change



Considerations

- User testing:** This idea was **prototyped/tested** in all three countries.
- Novelty:** This idea **derives** from an existing feature (e.g., [WhatsApp group invite](#))
- Popularity:** The idea was highly popular across all three countries. However users differed in the type and granularity of the information and controls they would want on the invite.
- Notable trade-offs:** (1) Level of granularity would add complexity and friction to the user experience. (2) The decision to include mutual contacts on the invite is highly useful as a verification tool for some users. But it can also expose users to greater risk that their social graph can be mapped without their consent.
- Other relevant factors:** Including the number of reported messages and users on the invite was desired by many participants in Nigeria and Colombia but highly controversial in the US. Furthermore, the level of granularity of the data included in this invite would likely need to vary depending on the type of group that was created (e.g., close family group vs. large thematic group).

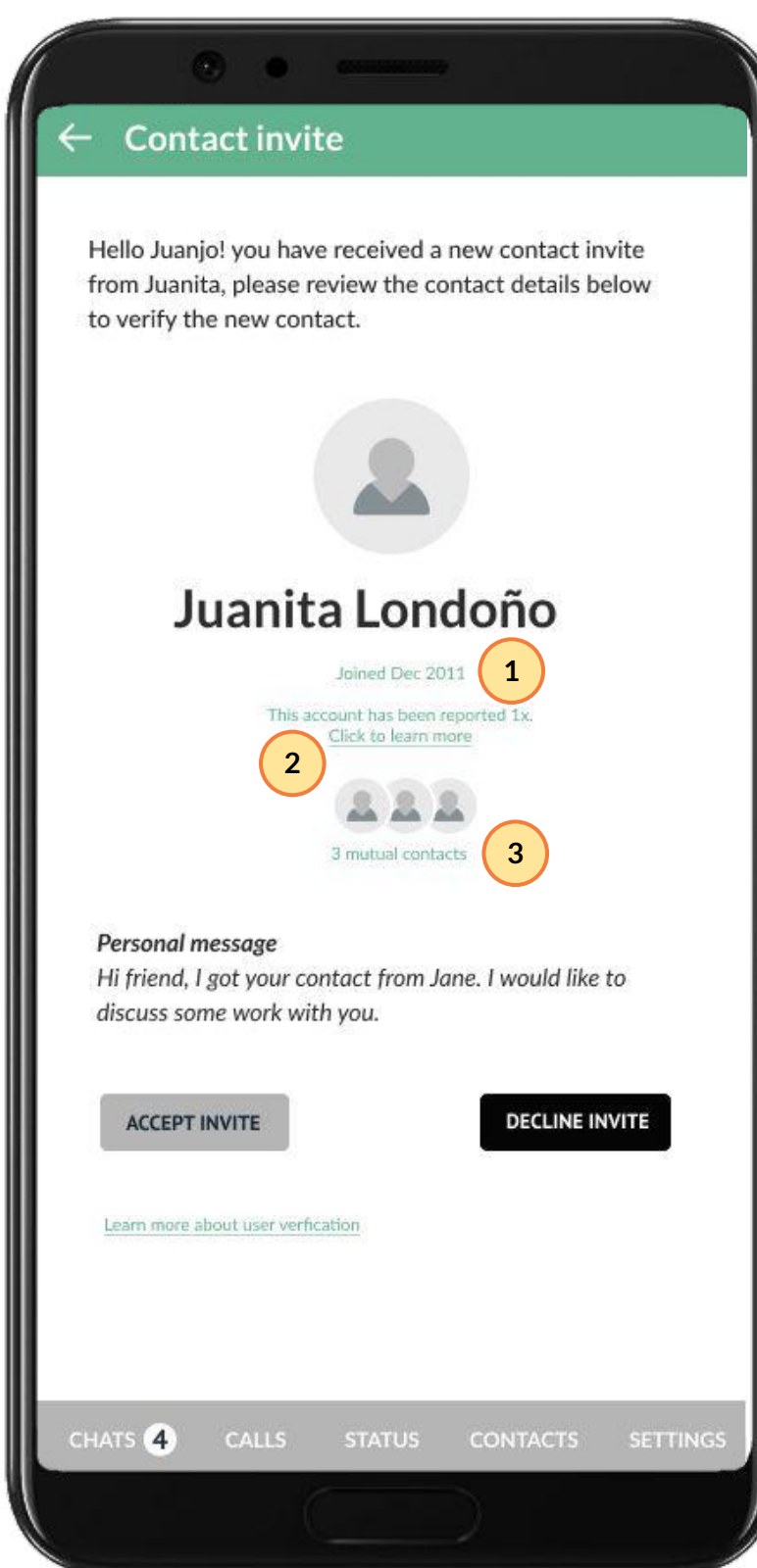
Key feature/s

- Enables users to see saved contacts who are existing members of the group** - Individuals can determine whether they can trust the group or not partly based on who they already know. This feature was especially popular in Nigeria and Colombia. Participants in the US raised concerns about this idea due to the potential for exposure of their graph.
- Enables users to see defined metadata related to the group, including date of formation, group size (#3)** - to aid individuals in evaluating the suitability/authenticity of a group.
- Enables individuals to see the number of group members** - to allow individuals to gauge suitability. Some of the participants we spoke with had set upper limits on the size of the group they were comfortable participating in.
- Enables users to set group privacy settings** - users can set custom privacy settings for new groups.

2B. Contact invite

Users would like to see critical information to vet the trustworthiness of new contact invites. The added information and controls available on the contact invite screen would allow users to make more informed decisions when new people reach out to them.

● Segmented idea ● Incremental change



Considerations

- User testing:** This idea was **discussed** with participants in all three countries but has **not been prototyped/tested**
- Novelty:** This idea **derives** from an existing feature (e.g., [Signals contact identity verification](#))
- Popularity:** The idea was raised at the end of our research. However, we were unable to assess its popularity. Users had a strong cross-country preference for consent related to group invites, which may be an indication of their support for this idea.
- Notable trade-offs:** The level of granularity might introduce some complexity and friction into the user experience.
- Other relevant factors:** Users expressed that verification information could be problematic if always present on the contact's profile but useful if a new contact reaches out.

Key feature/s

- Date joined** - This feature would be useful to some participants in Nigeria and Colombia to identify “propaganda” accounts that are newly created to influence an upcoming event (e.g., country general election).
- Reported accounts** - This feature would enable individuals to identify accounts that have been reported before for misuse etc. Although participants, especially in the US, had some concerns about the negative impact this feature may have on accounts.
- Mutual contact** - Participants, especially in Nigeria, agreed that having mutual contacts is a very useful factor when authenticating a strange contact. This way, they can quickly ascertain if they can trust the contact. However, some participants in the US were concerned about the potential misuse of this feature (e.g., social mapping).

Providing accessible & tailored security & privacy settings

This design opportunity addresses platform design gap ‘C. Generalized & hidden privacy & security controls for contacts & groups’. It covers the different ways that private messaging platforms could provide a range of security and privacy settings that adapt to user circumstances and are accessible in the places users need them most to be.

Platform design gap addressed

C. Generalized & hidden privacy & security controls for contacts & groups

Security and privacy controls are presented as generic settings applied equally to all contacts and groups while also remaining hidden behind multiple steps within little-used menu structures.

Understanding the opportunity

Security and privacy are not usually at the top of mind for users until they have been exposed to a higher perceived risk. But the design choices that platform providers make in how they structure privacy and security settings can play a significant role in mitigating users’ exposure to potentially harmful behavior. These design choices are also felt more generally in the visibility of a user’s status or the persistence of identifying information like their phone number. Users’ lack of control over these choices contributes to an overwhelming feeling that they are being tracked and watched all the time. This contributes to a sense of social pressure and anxiety associated with platform use/overuse as indicated by many of the users we interviewed.

In this section we cover the harms that design improvements related to this opportunity could mitigate as well as the principles that will be important to keep in mind when making design changes geared at this opportunity area.

HARMS IT COULD IMPACT

1. Vulnerability to adverse mental health impacts
2. Vulnerability to targeted harassment for youth and young adults
3. Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content
4. Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment
5. Vulnerability to encryption and data breaches via modified and third-party supporting platforms

PAIN POINT 1

Hidden & isolated privacy & security settings

The majority of private messaging platforms only provide one multi-step path for editing privacy and security settings. While this is less of a barrier for users with high-tech comfort and/or high perceived exposure to risk, it is a major problem for most users who won’t proactively search for these settings.

RELEVANT DESIGN PRINCIPLE #1

Surface information related to trust, privacy and security so that it is accessible to users in the places and moments that it is most relevant and actionable to them

PAIN POINT 2

Minimal security & privacy settings

Users are not able to have control over all the key features that impact their security and privacy on private messaging platforms (e.g., inability to adjust the visibility of when a user is online or when they are writing, inability to lock/ hide chats).

RELEVANT DESIGN PRINCIPLE #2

Extend user control over privacy and security into all aspects of the platform experience where they feel at risk

PAIN POINT 3

Problematic default security & privacy settings

Most settings/controls on private messaging platforms are typically set to the lowest security and privacy options. This makes changing to higher settings more difficult for users to discover. It also invites social pressures that may keep users from changing them in situations where they feel at risk.

RELEVANT DESIGN PRINCIPLE #3

Default to a high/the highest level of security whenever possible while providing easy and timely access for users to adjust their preferences to suit specific situations

PAIN POINT 4

Generic and unadaptable controls

Most control options are designed to function like a blanket, affecting most/ all contacts or groups. However, permissions and verification needs vary depending on the type of interaction. For example, users don’t need extensive verification and permissions for a close family/ friend group, but they do for a large group or when interacting with strangers, businesses, or services.

RELEVANT DESIGN PRINCIPLE #4

Offer flexibility so that users can tailor their trust, privacy and security preferences to specific relationships at the level of granularity that is most meaningful to them

PAIN POINT 5

Lack of promoting a culture that values security and privacy

Besides the need of UX/ UI design improvements, many participants we spoke to mentioned a need to couple those improvements with a campaign that promotes a cultural shift that nudges individuals to value caring about their security and privacy.

RELEVANT DESIGN PRINCIPLE #5

Instill a common mental model for how trust and security should work to cement safer practices in communications

Providing accessible & tailored security & privacy settings

Platform design ideas

The following are the preferred design ideas that were generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to serve as inspiration for new features and design improvements for private messaging platforms providers.

Key	
Applicability of idea	
● Cross-cutting - idea was welcomed by most users we spoke to across all three countries and identified archetypes	● Segmented - idea was welcomed by some archetypes and/ or countries.
Type of idea	
● New - new idea that's not based on an adaptation of existing features	● Incremental - idea is an adaptation or an addition to an existing feature

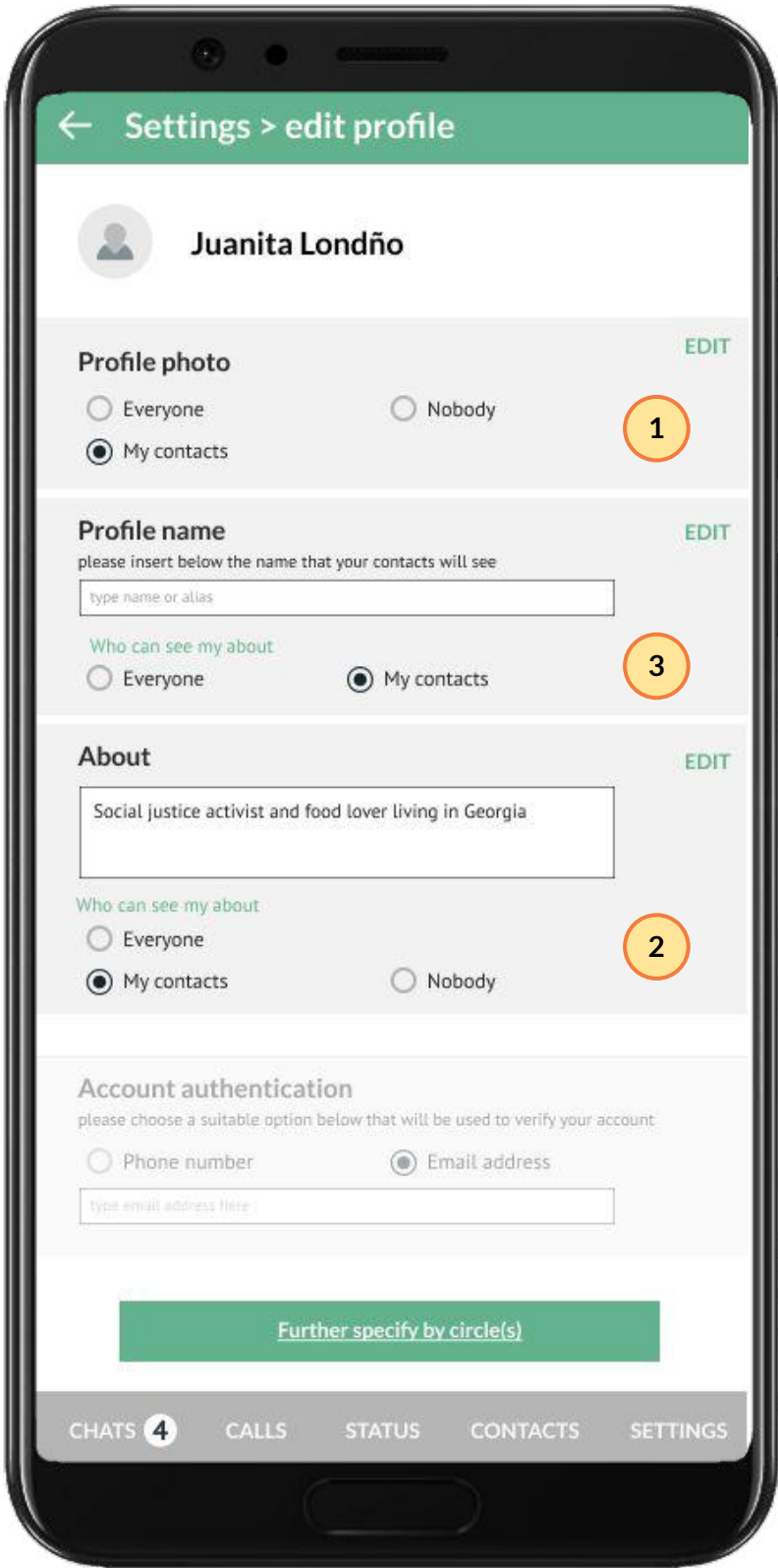
ACCESSIBILITY & DISCOVERABILITY 1/2

Examples of relevant design ideas:

3A. Integrated settings

Enabling users to quickly access important privacy settings in other relevant screens (e.g., account privacy settings accessible through edit profile screen) This involves surfacing such settings in the places that users visit frequently instead of in a separate section of the platform. This would make the settings more relevant and easier to discover.

● Segmented idea ● New idea



Considerations

- User testing:** This idea was discussed with users in Nigeria, and **prototyped/tested** with users in the US and Colombia.
- Novelty:** This idea **does not derive** from any existing feature on private messaging apps
- Popularity:** Popular in Nigeria and Colombia but users in the US were less inclined to support this idea as they felt this feature would make the private messaging platform seem like social media.
- Notable trade-offs:** There could be a loss of trustworthiness with medium and high-technological comfort users who disliked the “social media” feel of this idea as these platforms tend to offer more robust profile creation and management features than private messaging platforms.
- Other relevant factors:** This idea would likely need to be accompanied with a campaign focused on promoting a security and privacy culture to drive engagement. **This idea could work well in combination with the ‘user profiles’ idea on the next page.**

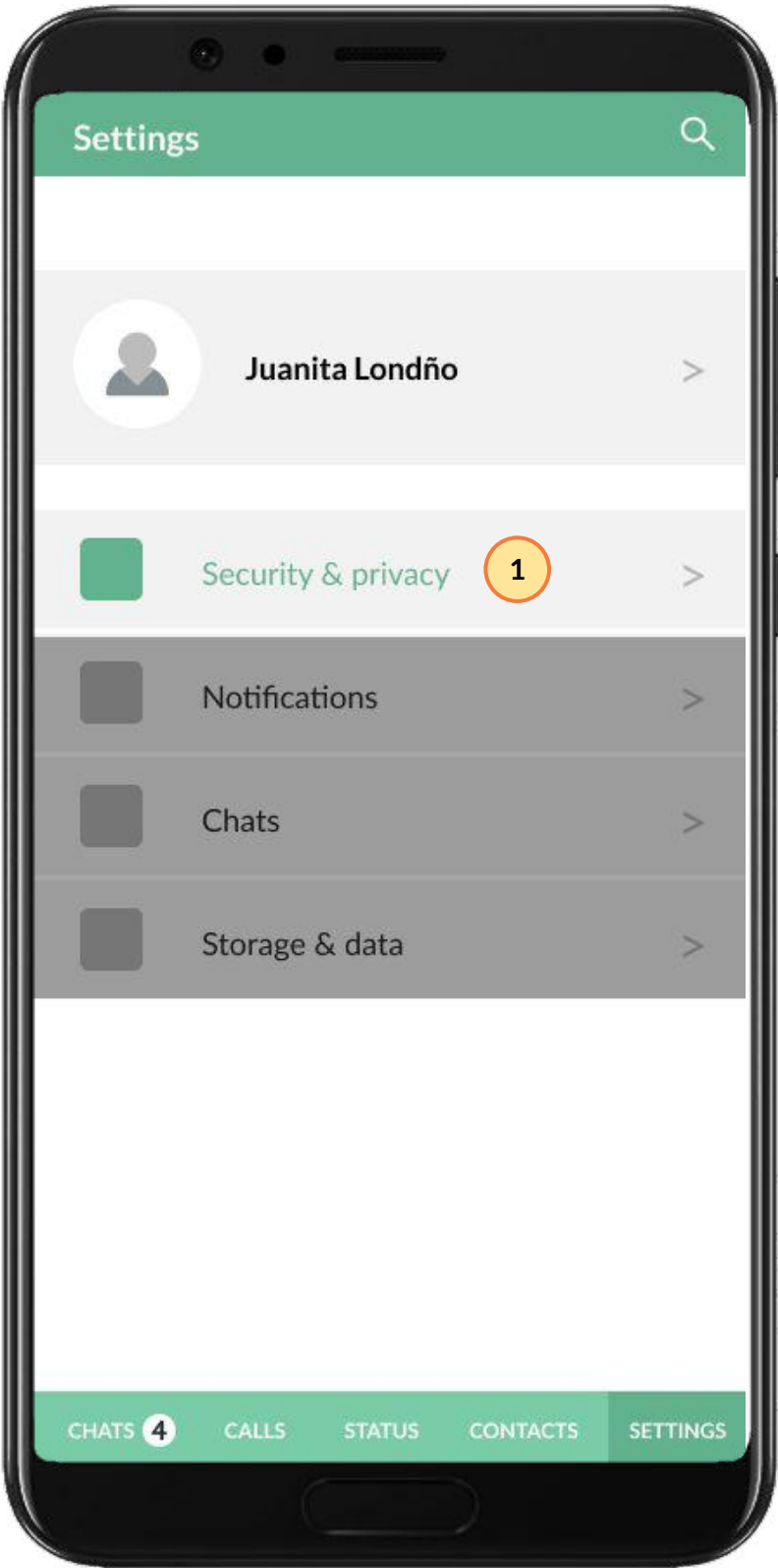
Key feature/s

- 1 Enables individuals to quickly change the permissions associated with their profile photo in the same interface where they add or update the image
- 2 Enables individuals to choose a public-facing profile/user name and also define who can see that information
- 3 Enables individuals to update and adjust access to their “about” information - to allow for quick selection of who can see this personal information

3B. Accessible settings

Users have easier access to a wider range of privacy and security settings. Making the settings easier to discover by having less steps between the main menu and the settings. The change would help a variety of users have improved access to changing their privacy and security settings.

● Cross-cutting idea ● Incremental change



Considerations

- User testing:** This idea was discussed with users in Nigeria, and **prototyped/tested** with participants in the US and Colombia
- Novelty:** This idea **derives** from existing private messaging platform feature (e.g., [Signal navigational steps to access settings](#))
- Popularity:** Popular in all three countries and for a variety of participants.
- Notable trade-offs:** This idea would likely have less impact on individuals with lower-technological comfort in comparison to the ‘integrated settings’ idea as it still requires added steps for discovery
- Other relevant factors:** The idea would likely need to be accompanied with a campaign focused on promoting a security and privacy culture to drive user engagement.

Key feature/s

- 1 Reduces number of steps to access privacy and security settings - to increase the ease of discoverability and usage

* features/options that lightly obscured are covered in other sections, the others that are darkened are already implemented by existing private messaging platforms

Providing accessible & tailored security & privacy settings

Platform design ideas

The following are the preferred design ideas that were generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to serve as inspiration for new features and design improvements for private messaging platforms providers.

Key	
Applicability of idea	
● Cross-cutting - idea was welcomed by most users we spoke to across all three countries and identified archetypes	● Segmented - idea was welcomed by some archetypes and/ or countries.
Type of idea	
● New - new idea that's not based on an adaptation of existing features	● Incremental - idea is an adaptation or an addition to an existing feature

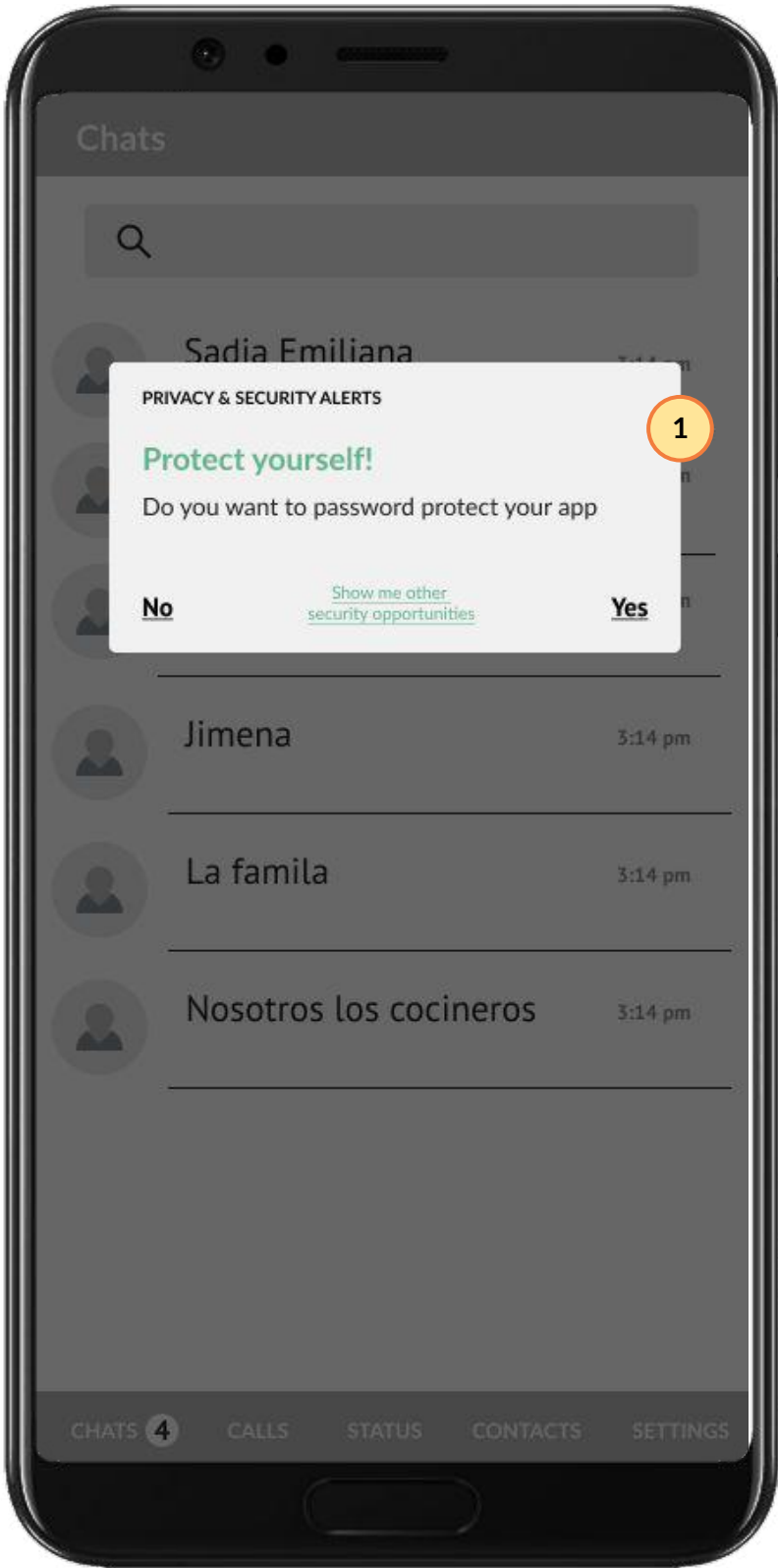
ACCESSIBILITY & DISCOVERABILITY 2/2

Examples of relevant design ideas:

3C. Security & privacy tips

Users are able to receive tips about settings they can use to improve their security and privacy. The notifications would help make settings easier to discover by bringing them in front to the users. The idea would help users who rarely change privacy and security settings due to lack of awareness or know-how.

● Segmented idea ● Incremental change



Considerations

- User testing:** This idea was **prototyped / tested** with participants in the US and Colombia
- Novelty:** This idea **derives** from existing feature on private messaging platform (e.g., [Telegram Tips](#))
- Popularity:** This idea was desired by participants with low-technological comfort, however all other participants were concerned that it might be a potential nuisance.
- Notable trade-offs:** Repeated exposure to these messages could become a nuisance for many users over time, depending on the variety, frequency, and ease of opting out. Tech-savvy users would prefer for these notifications to be sent infrequently so that they don't become a nuisance.
- Other relevant factors:** This idea could work better if accompanied with a campaign focused on promoting a security and privacy culture to increase user comfort and engagement.

Key feature/s

- 1 Push popup notification** - to remind individuals of unutilised important security settings

* features/options that lightly obscured are covered in other sections, the others that are darkened are already implemented by existing private messaging platforms

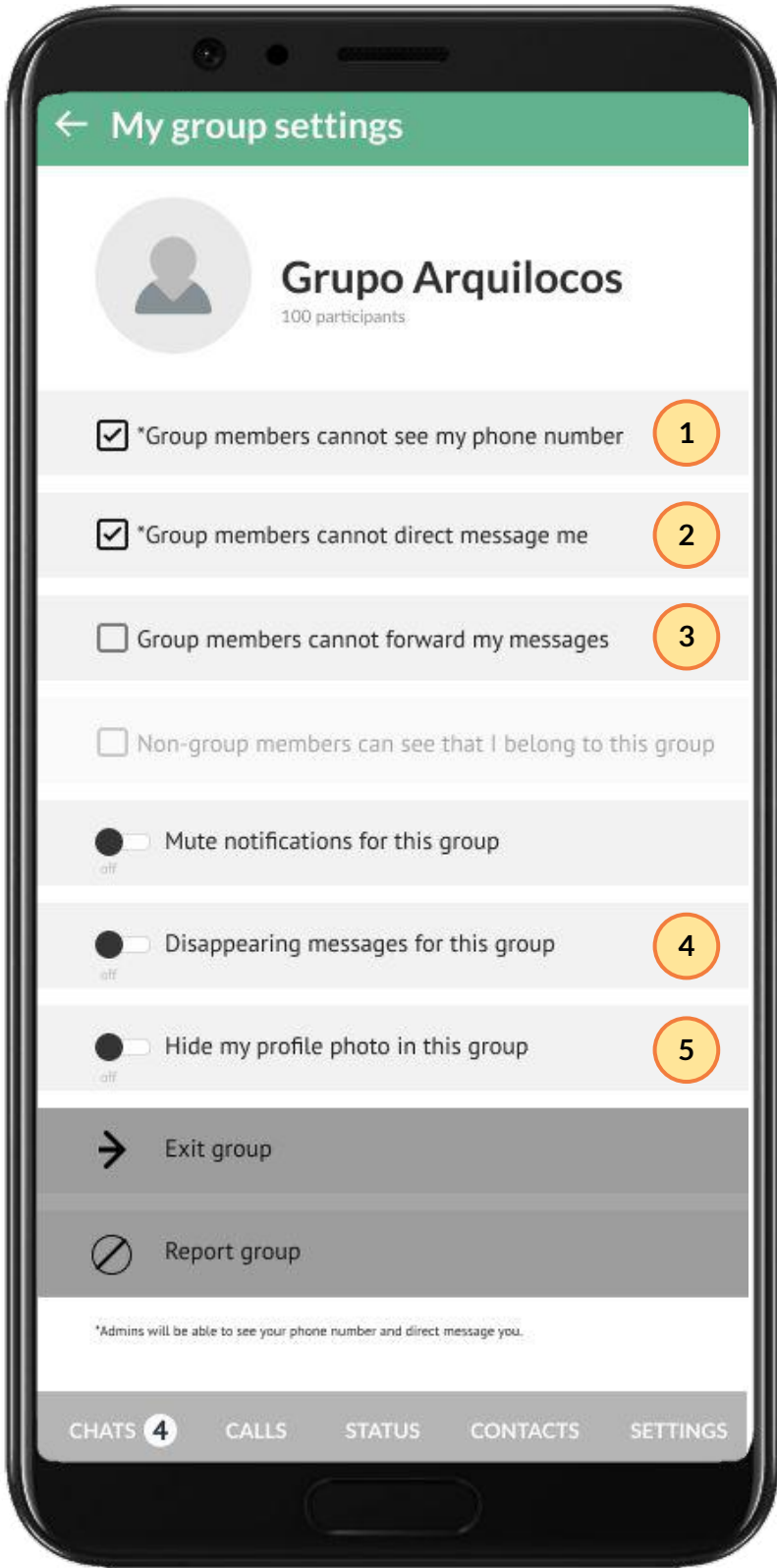
TAILORED CONTROLS 1/2

Examples of relevant design ideas:

3D. Custom Group & contact settings

Users are able to set privacy and security settings at a group and/ or contact level, not just at a cross-platform level. This level of granularity would enable users to set higher or lower privacy and security settings depending on the level of trust they have with who they are chatting with.

● Segmented idea ● New idea



Considerations

- User testing:** This idea was **prototyped/ tested** with participants in the US and Colombia
- Novelty:** This idea **does not derive** from any existing feature on private messaging platform/s
- User testing:** Tested in Colombia and the US.
- Popularity:** Popular in Colombia and Nigeria. However, in the US, many users did not express seeking granularity but rather higher privacy and security as their default settings.
- Notable trade-offs:** This level of granularity could add complexity to the user experience, which would have a bigger impact on individuals with lower technological comfort.
- Other relevant factors:** This idea could work well with preset settings that can help reduce the burden of the task.

Key feature/s

- 1 Ability to hide user phone number in groups** - to increase individual's safety in untrusted groups
- 2 Restricting sending of direct messages to users by group members** - to increase individual's privacy in group spaces
- 3 Restricting forwarding of user messages in groups** - to increase content protection in groups.
- 4 Adjusting disappearing messages in groups** - to increase content protection
- 5 Restricting access to user profile photo** - to increase privacy in untrusted groups

Providing accessible & tailored security & privacy settings

Platform design ideas

The following are the preferred design ideas that were generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to serve as inspiration for new features and design improvements for private messaging platforms providers.

Key	
Applicability of idea	
● Cross-cutting - idea was welcomed by most users we spoke to across all three countries and identified archetypes	● Segmented - idea was welcomed by some archetypes and/ or countries.
Type of idea	
● New - new idea that's not based on an adaptation of existing features	● Incremental - idea is an adaptation or an addition to an existing feature

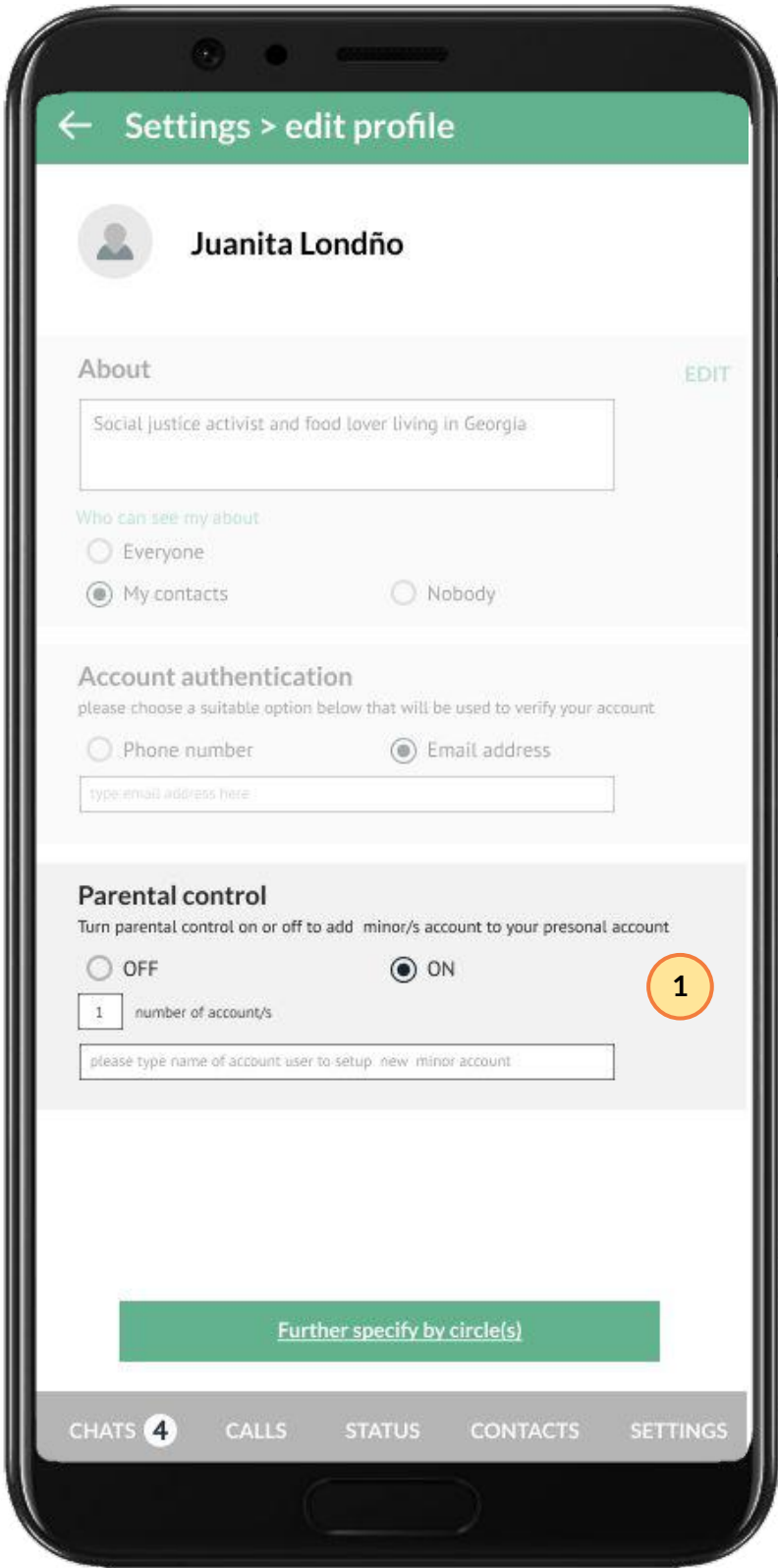
TAILORED CONTROLS 2/2

Examples of relevant design ideas:

3E. Parental controls

Parents are able to create special accounts for minors that come with pre-determined parental controls. The account of the minor is linked to the parent account, giving the parent visibility over certain aspects of the child's account without violating their privacy. The level of control and visibility the parent has could then vary depending the age of the minor.

● Segmented idea ● New idea



Considerations

- User testing:** This idea was discussed with users in Colombia only
- Novelty:** This idea does not derive from any existing feature on private messaging platform
- Popularity:** Given idea was raised at the end of our research, we are unable to assess its popularity. However, the Colombian users who suggested this idea, which included both parents and non-parents, felt strongly about its value.
- Notable trade-offs:** Minors and children could potentially feel the controls infringe on their privacy. This idea has the potential to be misused (e.g., to monitor the activities of another user over whom they wield a certain amount of power).
- Other relevant factors:** Age brackets will be critical for defining the types of controls available to parents.

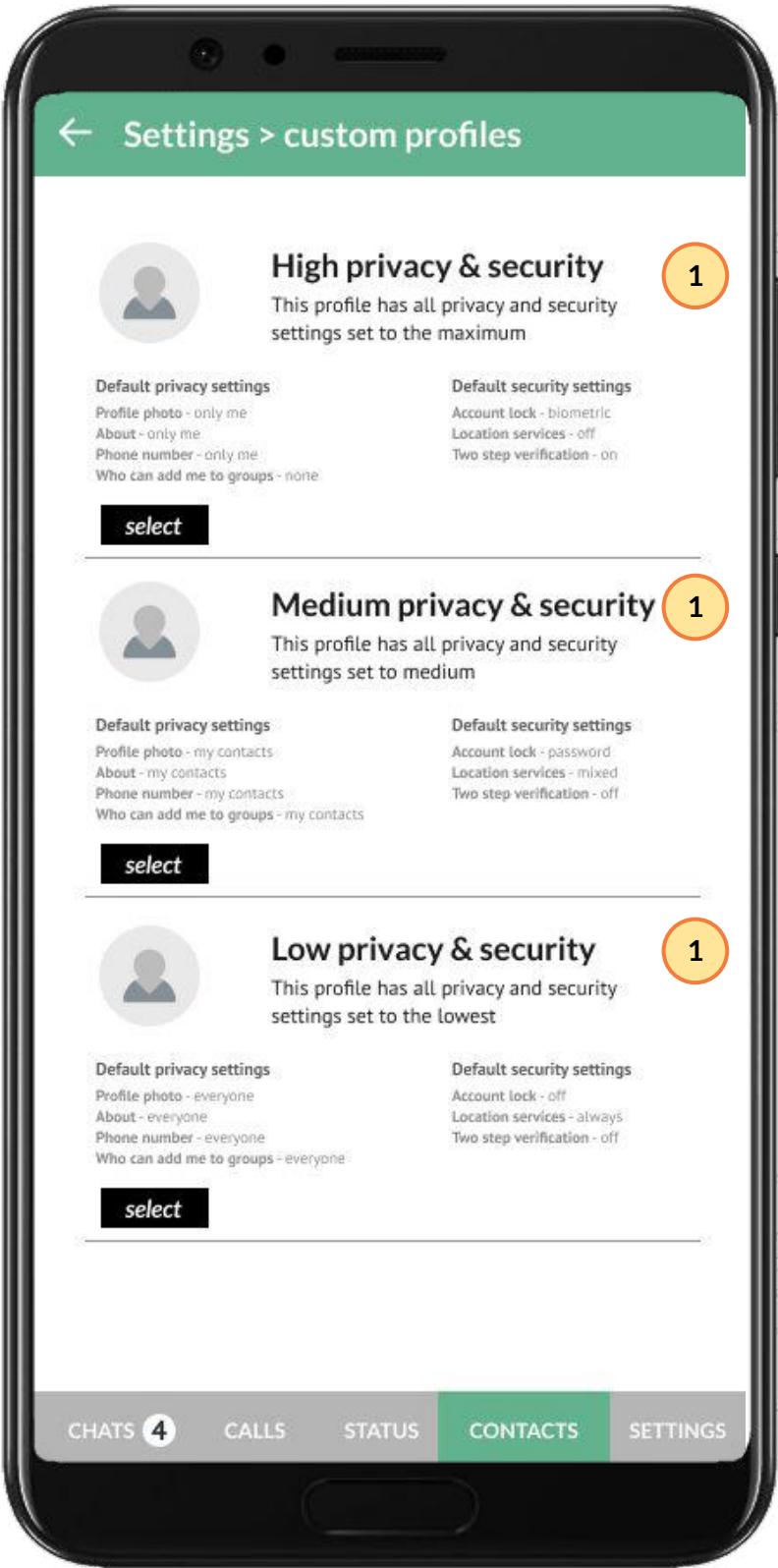
Key feature/s

- Parental control options** - to enable parents/guardians to create a minor's account that has specific restrictions and can be monitored for safety.

3F. Pre-configured user profiles

Users are able to choose from a set of pre-configured profiles linked to different feature packages. The unique combination of features would be tailored to a certain type of user, disabling any other unnecessary features. Profile types that we have seen during our research include: parents, minors, super users, typical users, and users who need tech-support.

● N/A ● New idea



Considerations

- User testing:** This idea was discussed with users in Colombia only
- Novelty:** This idea does not derive from any existing feature on private messaging platform
- Popularity:** Given idea was raised at the end of our research, we are unable to assess its popularity.
- Notable trade-offs:** These preset configurations need to match the user's mental model, which can vary quite a bit by the level of experience or market. They would need to include tools to easily tune/modify the configuration, which could get complex if not designed well.
- Other relevant factors:** The use of profiles could be a significant change for messaging platforms to implement. It would require some sort of algorithm for matching settings with a generalized set of preferences and updating those settings as new options become available.

Key feature/s

- Enabling users to quickly select and modify a tailored profile that best fits their needs** - Users, especially those with low-tech familiarity, can easily secure their account and privacy at the level that suits them without having to dive deeply into all the different options.

* features/options that lightly obscured are covered in other sections, the others that are darkened are already implemented by existing private messaging platforms

Providing accessible & tailored security & privacy settings

Platform design ideas

The following are the preferred design ideas that were generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to serve as inspiration for new features and design improvements for private messaging platforms providers.

Key

Applicability of idea

- Cross-cutting** - idea was welcomed by most users we spoke to across all three countries and identified archetypes
- Segmented** - idea was welcomed by some archetypes and/ or countries.

Type of idea

- New** - new idea that's not based on an adaptation of existing features
- Incremental** - idea is an adaptation or an addition to an existing feature

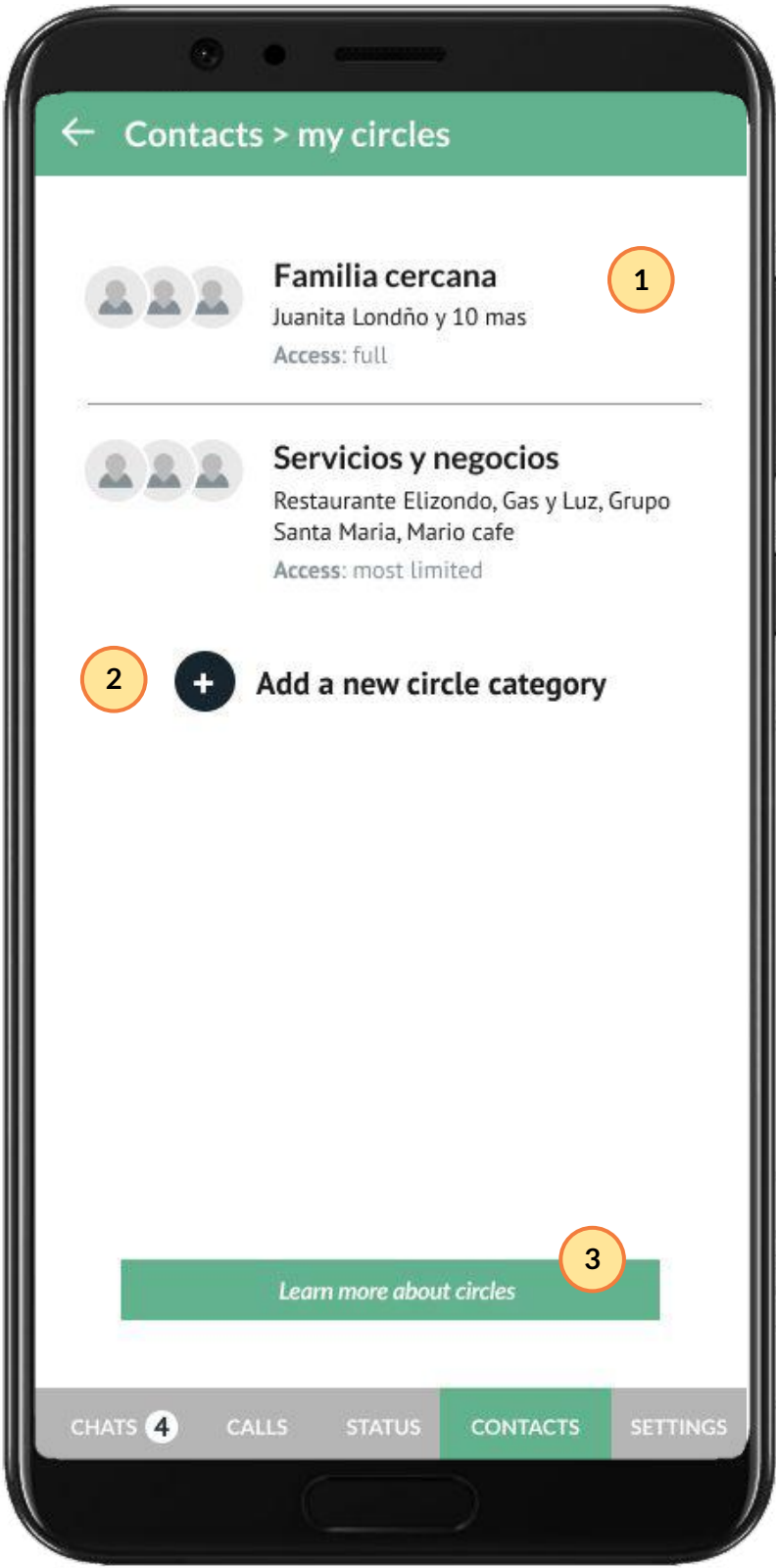
CONTACT AND GROUP MANAGEMENT

Examples of relevant design ideas:

3G. Contact circles

Users can form contact circles that can be used to organize select contacts based on their level of access to their accounts. Users could use this to differentiate who can see their personal information (e.g., phone number, photo, name, status), but also for selectively sharing things like stories or designating certain contacts to reach them anytime.

Segmented ideas New idea



Considerations

- User testing:** This idea was **prototyped / tested** with users in all three countries
- Novelty:** This idea **does not derive** from any existing feature on private messaging platform
- Popularity:** This idea was highly popular in Nigeria and Colombia where users tend to make more extensive use of messaging platforms throughout their day-to-day lives. Users in the US did not see this feature as necessary.
- Notable trade-offs:** Users with low familiarity with messaging platforms would not welcome the added complexity, while users with extensive usage could gain relief.
- Other relevant factors:** This idea could be a way to avoid the burden of adjusting contact and group settings on a case-by-case basis (as described in the 'group and contact settings' idea).

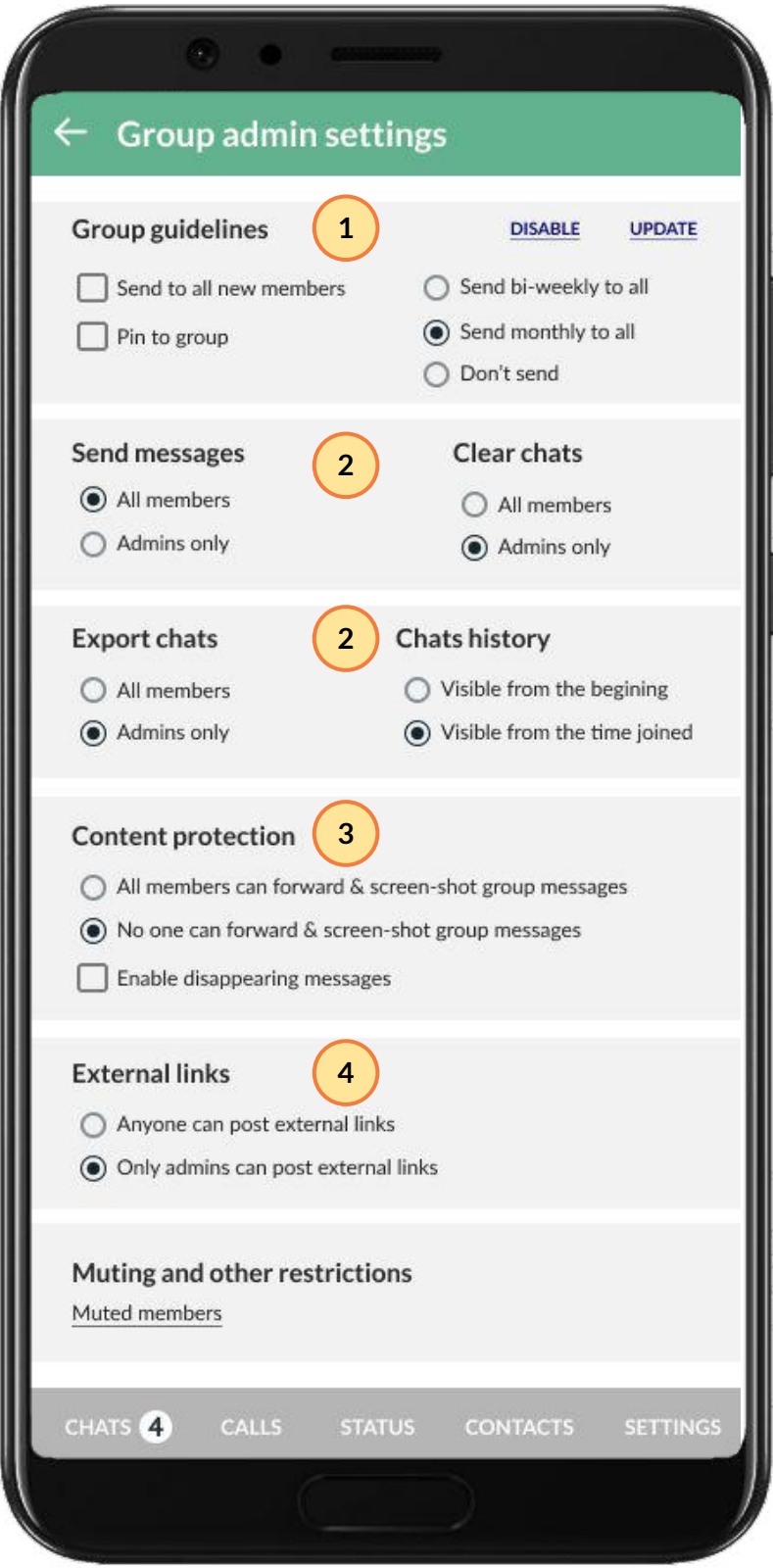
Key feature/s

- Customised groups based on user preferences:** Users have full control over the composition of these circles and the permissions associated with them.
- Ability for users to add more custom contact groups:** To reflect their changing needs over time and help support users who run both their personal and professional lives on private messaging platforms

3H. Custom admin group tools

Admins are able to access custom settings that help them act on group misuse. These settings can include things like the ability to set group guidelines, the ability to silence select members, and the ability to block re-sharing or screen-grabbing of content, among others.

Segmented idea Incremental change



Considerations

- User testing:** Tested in Nigeria, Colombia and the US.
- Novelty:** This idea **derives** from existing feature on private messaging platform (e.g., [Signal](#) & [WhatsApp](#) group settings)
- Popularity:** This idea was highly popular with most users in Nigeria and Colombia but more controversial with the US participants due to differing perceptions towards the admin role and the level of control they could/should exert over a group.
- Notable trade-offs:** Users who do not want admins to have such a high level of control could migrate to other messaging platforms that offer flatter hierarchies.
- Other relevant factors:** The extensiveness of the settings available to the admin could depend on the type of group created. For example, minimal settings would be needed for small social/family groups but extensive settings would be useful for large themed groups.

Key feature/s

- Ability to create and share group guidelines** - to allow group members to agree on shared rules of dos and don'ts in group spaces as well as reinforce those norms for new members
- Increased group content protection** - by restricting exporting of chats, visibility of chat history, screenshots, forwarding of messages, and clearing chats from groups.
- Restricting export chats and visibility of chats history** - to give admins more custom flexibility to adjust member's ability to export chats or view chat history especially for new members
- Restricting who can post external links in group chats** - to avoid unauthorised and malicious links

Managing access to modified & third-party supporting platforms

This design opportunity addresses platform design gap ‘D. Infringement by modified (MOD) & third-party supporting apps ecosystem’. It covers the different ways that private messaging platforms could improve the design of their platforms so as to not lose users to MOD or third-party apps, as well as, other actions the platforms should be taking to protect their users from them.

Platform design gap addressed

D. Existence of modified (MOD) & third-party supporting apps ecosystem

There are multiple modified (MOD) and third-party supporting private messaging platform apps that offer users additional features that they can use in combination with or in replacement of their private messaging platform app.

Understanding the opportunity

Modified and third-party supporting apps are an interesting problem for private messaging platform providers. They did not come up in all of our research discussions, but they seem to be a growing concern for users in markets where they are becoming more prevalent such as Nigeria and Colombia. On the one hand, these MODs provide a window into the kinds of features that super users seek that is not offered by private messaging platforms. These features have enough of a pull that users have chosen to download a new unverified app that enhances their existing features, which might pose additional risks. These apps also raise questions with users about how the encryption of private messaging platforms is being breached. Research participants were concerned that the use of these MODs will create unknown security risks for the user as well as the people they connect with due to their fundamental asymmetry.

In this section we cover the harms that design improvements related to this opportunity could mitigate as well as the principles that will be important to keep in mind when making design changes geared at this opportunity area.

HARMS IT COULD IMPACT

1. Vulnerability to adverse mental health impacts

2. Vulnerability to targeted harassment for youth and young adults

3. Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content

4. Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment

5. Vulnerability to encryption and data breaches via modified and third-party supporting platforms

PAIN POINT 1

Lack of visibility into platform end-to-end experience

Users of verified private messaging platforms (e.g., WhatsApp) are unaware when they communicate with a contact who uses an unverified private message platform (e.g., GB WhatsApp).

RELEVANT DESIGN PRINCIPLE #1

Surface information related to trust, privacy and security so that it is accessible to users in the places and moments that it is most relevant and actionable to them

PAIN POINT 2

Bypassing user’s privacy settings

Users who adopt unverified platforms (e.g., GB WhatsApp) are able to bypass the privacy settings of users of verified/standard platforms (e.g., WhatsApp). Examples of affected privacy settings include bypassing restrictions on user status, viewing users deleted status posts, etc.

RELEVANT DESIGN PRINCIPLE #2

Extend user control over privacy and security into all aspects of the platform experience where they feel at risk

Managing access to modified & third-party supporting platforms

Platform design ideas

The following are the preferred design ideas that were generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to serve as inspiration for new features and design improvements for private messaging platforms providers.

Key

Applicability of idea

- **Cross-cutting** - idea was welcomed by most users we spoke to across all three countries and identified archetypes
- **Segmented** - idea was welcomed by some archetypes and/ or countries.

Type of idea

- **New** - new idea that's not based on an adaptation of existing features
- **Incremental** - idea is an adaptation or an addition to an existing feature

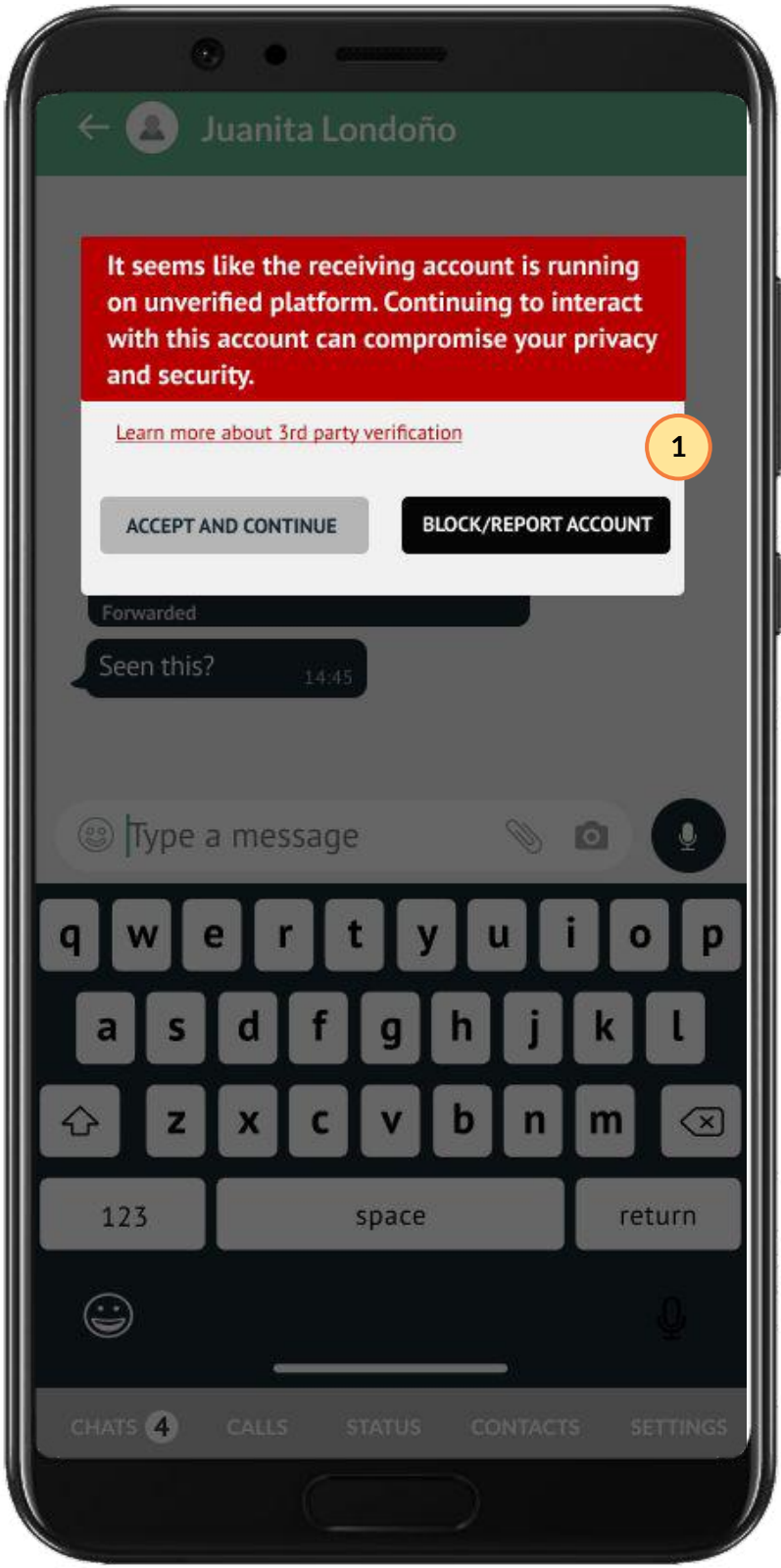
3rd PARTY PLATFORM VERIFICATION AND USER NOTIFICATION

Examples of relevant design ideas:

4A. Platform end-to-end verification and user notification

Verify end-to-end authenticity of private messaging platform used and notify user of unverified platform use **within a chat**. This would enable users to identify third-party apps (e.g., GB WhatsApp) that compromise user's privacy and security so that they can determine how to proceed with such exchanges.

● Segmented idea ● New idea



Considerations

- **User testing** - This idea was **prototyped/ tested** with users in all three countries
- **Novelty**: This idea **does not derive** from any existing feature on private messaging platforms
- **Popularity** - users especially in Colombia were excited about this added layer of visibility.
- **Notable trade-offs** - Users may be confused why they are being notified of interactions with other users on unverified platforms and it may undercut their overall confidence in the standard private messaging platforms experience. It will be important to educate users on the risks and functions of this type of verification.
- **Other relevant factors** - N/A

Key feature/s

- 1

Push notifications to users when receiving platform is unverified - to enable users to identify users of malicious/unverified 3rd party apps e.g., GB WhatsApp

Providing user support mechanisms & emergency controls

This design opportunity addresses platform design gap ‘E. Limited user support and lack of adequate reporting mechanisms’. It covers the different ways that private messaging platforms could provide a range of support tools that help users with reporting, troubleshooting, verifying typical security risks (e.g., links), and resolving critical issues.

Platform design gap addressed

E. Limited user support and lack of adequate reporting mechanisms

From tech literacy and customer support to emergency and reporting tools, there are limited to no user support mechanisms available. Those that exist are not perceived as being useful or adequately functional.

Understanding the opportunity

Many users of private messaging apps, especially in Colombia and Nigeria, strongly believe that dedicated tools would be very helpful to support first-time use as well as resolve critical account issues (e.g., disabling and recovery of a hacked account etc). Some users who have been victims of hacking reported that, due to lack of proper support, they were forced to abandon their hacked account and open a new account, losing important information in the process.

In this section, we cover the harms that design improvements related to this opportunity could mitigate as well as the principles that will be important to keep in mind when making design changes geared at this opportunity area.

HARMS IT COULD IMPACT

1. Vulnerability to adverse mental health impacts

2. Vulnerability to targeted harassment for youth and young adults

3. Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content

4. Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment

PAIN POINT 1

Limited contact verification options

Due to frequent cases of scams, especially in Nigeria and Colombia, some users have felt a strong need for contact verification options to determine the authenticity of unknown contacts. Currently, users leverage caller ID apps (e.g., Truecaller) to identify unknown contacts.

RELEVANT DESIGN PRINCIPLE #1

Surface information related to trust, privacy and security so that it is accessible to users in the places and moments that it is most relevant and actionable to them

PAIN POINT 2

Lack of alternative tools for users to resolve critical issues.

Many users, especially in Nigeria and Colombia, reported facing crippling challenges when their private messaging app account was compromised (e.g., hacking, theft). Often they end up opening a new account and losing important information/contacts in the process.

RELEVANT DESIGN PRINCIPLE #2

Extend user control over privacy and security into all aspects of the platform experience where they feel at risk

PAIN POINT 3

Sharing of unverified hyperlinks in chats

Many users felt the need for a hyperlink verification option to identify phishing and fraudulent links, especially in group chats on private messaging apps.

RELEVANT DESIGN PRINCIPLE #3

Default to a high/the highest level of security whenever possible while providing easy and timely access for users to adjust their preferences to suit specific situations

PAIN POINT 4

Limited or inconsistent user feedback when reporting, querying etc.

Users reported frustration when finding answers to questions regarding app functionalities/features. They are also discouraged by the lack of feedback from private messaging platforms when they reported serious misuse and infringements

RELEVANT DESIGN PRINCIPLE #7

Make redressal paths simple and clear so users know who to turn to and what to expect when concerns arise

Providing user support mechanisms & emergency controls

Platform design ideas 1/2

The following are the preferred design ideas that were generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to serve as inspiration for new features and design improvements for private messaging platforms providers.

Key

Applicability of idea

Cross-cutting - idea was welcomed by most users we spoke to across all three countries and identified archetypes

Segmented - idea was welcomed by some archetypes and/ or countries.

Type of idea

New - new idea that's not based on an adaptation of existing features

Incremental - idea is an adaptation or an addition to an existing feature

USER SUPPORT TOOLS

Examples of relevant design ideas:

5A. Official chat channel

An official chat channel that users can use to send direct queries to a respective private messaging app. This would allow users to make important queries related to customer support issues (e.g., privacy and security tools, reporting, data privacy) to enable users to fully maximize the functionalities of the respective private messaging app.

● Cross-cutting idea ● Incremental change

Considerations

- User testing** - This idea was discussed with users in Nigeria and Colombia
- Novelty**: This idea derives from existing feature on private messaging platform/s (e.g., [Telegram Tips](#))
- Popularity** - popular with low-tech comfort users in Nigeria and Colombia. However, more tech-savvy users would rather find solutions via the web.
- Notable trade-offs** - Some users may see this channel as a nuisance especially if they receive unsolicited messages and communications. General questions (e.g., FAQs) can be automated to increase efficiency. But more serious issues (e.g., loss of data, compromised account) should be augmented with human support.
- Other relevant factors** - Communications for common questions may be automated by a bot. But other unique and more serious issues would require human support.

Key feature/s

- Personalised messages** - to drive increased engagement
- Ability for users to ask and find solutions to common problems in a single chat**: (1) ask questions related to privacy and security, (2) receive redress info related to reporting/ flagging and (3) access general customer tech support.

5B. Alternative emergency access point (e.g., web portal).

An official emergency access point (e.g., web portal) allows users to access important account control tools in an emergency (e.g., theft, hacking). This would help users to resolve or escalate crucial account issues, such as the loss of primary access due to hacking or phone theft.

● Segmented idea ● New idea

Considerations

- User testing** - This idea was prototyped/ tested with users in Colombia and discussed with users in Nigeria and the US
- Novelty**: This idea does not derive from any existing feature on private messaging platform
- Popularity** - popular with low-tech users who feel at risk of theft, hacking, and other types of unauthorised access to their account (e.g., physical access by law enforcement)
- Notable trade-offs** - Unauthorised access to this portal could be crippling to the rightful owner
- Other relevant factors** - Important to perform vigorous verification before user access this portal to avoid malicious unauthorised misuse

Key feature/s

- Report compromised account** - to block account usage and mitigate potential harms caused by hacking, etc
- Erase account information/data** - to protect personal data in case of loss of device through theft, physical access by law enforcement, etc
- Alerting pre-selected close contacts** - to notify them of a user's compromised account and to be wary of messages from the account to avoid scams, etc
- Recover account** - to reclaim a compromised account through hacking. This process should include verification options to the authentic rightful owner
- Escalation path** - to easily connect with customer support if their issue is not easily addressed with automated services
- Ability for users to receive additional support via chat**: to resolve any complications and other support. (see also the previous idea "Official chat channel")

68

Providing user support mechanisms & emergency controls

Platform design ideas 2/2

The following are the preferred design ideas that were generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to serve as inspiration for new features and design improvements for private messaging platforms providers.

Key

Applicability of idea

- **Cross-cutting** - idea was welcomed by most users we spoke to across all three countries and identified archetypes
- **Segmented** - idea was welcomed by some archetypes and/or countries.

Type of idea

- **New** - new idea that's not based on an adaptation of existing features
- **Incremental** - idea is an adaptation or an addition to an existing feature

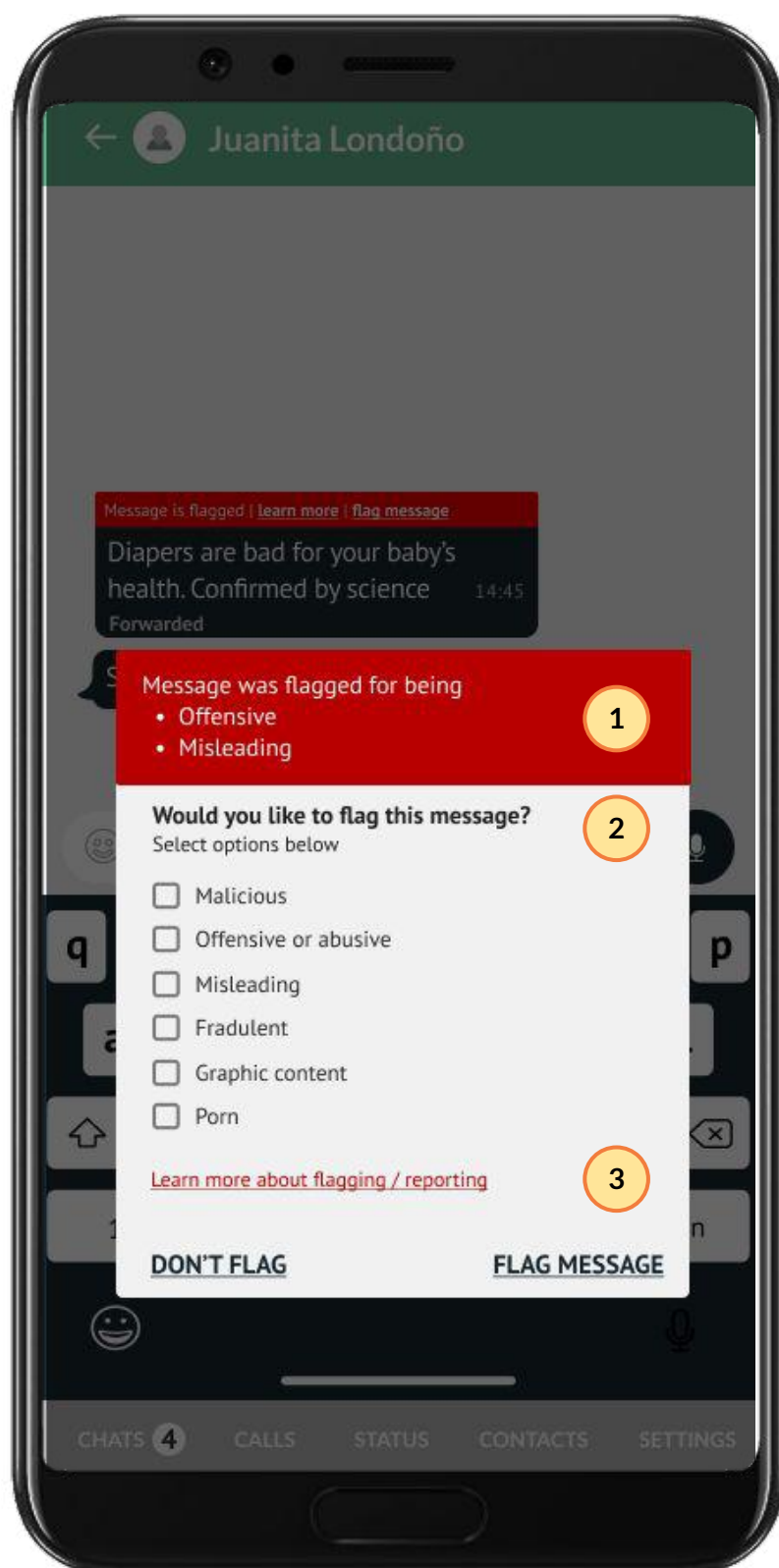
MANAGING MALICIOUS INFORMATION/CONTENT

Examples of relevant design ideas:

5A. Content flagging

Ability for users to flag malicious and non-factual information within context of use (e.g., group and 1:1 chats). This enhancement would allow users to flag problematic content both for themselves and other users who may come across such content. However, verification of user-flagged content is a critical ingredient to increase users' trust, address skepticism and avoid misuse of this feature.

● Segmented idea ● Incremental change



Considerations

- User testing** - This idea was **prototyped/ tested** with users in Nigeria, Colombia and the US.
- Novelty**: This idea **derives** from existing features on private messaging platforms (e.g., [Twitter's misinformation label](#))
- Popularity** - This idea was popular with users in Nigeria and Colombia, however users in the US were deeply concerned about it. Users raised concerns about the potential misuse of this sort of function. Key reasons why they opposed such functionalities included the credibility of verifying flagged messages, the potential use for malicious flagging and the deleterious use as a tool to silence critics.
- Notable trade-offs** - This mechanism might encourage some users to deliberately flag messages as an alternate way of voicing their opinion or discrediting another user. US participants also voiced a strong concern that this feature could infringe on freedom of speech given the subjective nature of what is and isn't classified as "misinformation".
- Other relevant factors** - The process for verifying flagged messages should be transparent and properly communicated to users to remove any doubts regarding credibility.

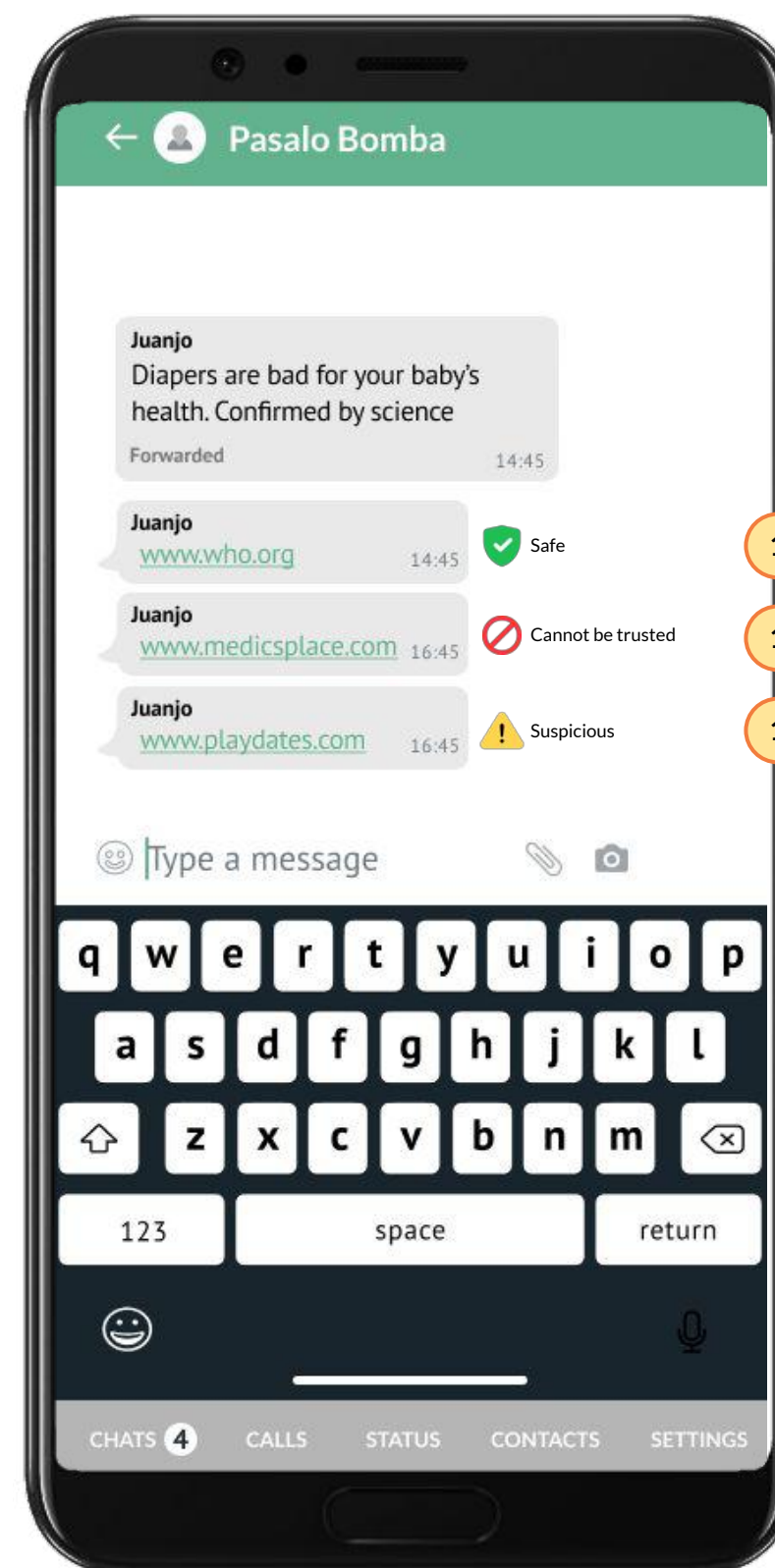
Key feature/s

- 1 Clear communication on infringement type** - to enable users to understand the specific reason this content was flagged by others
- 2 Options for users to choose for reason of flagging** - to allow for precise and accurate flagging
- 3 Option for users to learn more** - to understand process and what happens to content once it is flagged for verification

5B. URL safety checker.

Automated URL scan to check the safety of links, detect malicious links (e.g., includes malware, phishing links), and notify user if the link is unsafe. This would particularly be helpful to minors, low tech-savvy users, the elderly, and other users who are acutely vulnerable to phishing, scamming and hacking.

● Segmented idea ● Incremental change



Considerations

- User testing** - This idea was **discussed** with users in Colombia and Nigeria
- Novelty**: This idea **derives** from existing feature on other messaging platform/s (e.g., [Google safebrowsing](#))
- Popularity** - This idea was popular with low-tech users and other segments who are highly vulnerable to phishing, scamming, and hacking.
- Notable trade-offs** - Users may not fully understand the level of verification that the private messaging platform will be able to provide as it is likely not to address all potential risks. Users should be prompted to confirm their choice if they decide to proceed with an unsafe link (e.g., pop up dialog window)
- Other relevant factors** - It is important to communicate basic information to users on why/how this feature helps them feel more secure in using private messaging platforms.

Key feature/s

- 1 Automated checking of hyperlinks to authenticate safety** - to enable users to quickly identify unsafe links before clicking

Improving administrative & management tools

This design opportunity addresses platform design gap ‘F. Limited content management tools’. This opportunity covers the different ways that private messaging platforms could enable users and administrators to better manage information and interactions on messaging platforms.

Platform design gap addressed

F. Limited content management tools

There are very few features that help users better manage and organize the content they receive.

Understanding the opportunity

Many users of private messaging apps have experienced the misuse of social spaces, especially groups, for spreading malicious/spam information. They expressed the need for better tools to manage conversations and information shared in such social spaces. Other areas of concern include: restricting screen grabs and forwarding of messages, exporting of chats, managing contacts.

In this section we cover the harms that design improvements related to this opportunity could mitigate as well as the principles that will be important to keep in mind when making design changes geared at this opportunity area.

HARMS IT COULD IMPACT

1. Vulnerability to adverse mental health impacts

2. Vulnerability to targeted harassment for youth and young adults

3. Vulnerability to manipulation (misleading content, mis/disinformation) or exposure to offensive content

PAIN POINT 1

Inability to restrict unauthorised access of private messages

Participants, especially in Nigeria and Colombia, expressed the need to restrict the use of sharing screen grabs, forwarding and exporting chats in groups, so as to curb access to private conversations.

RELEVANT DESIGN PRINCIPLE #2

Extend user control over privacy and security into all aspects of the platform experience where they feel at risk

PAIN POINT 2

Inability to tailor privacy settings based on individual contact or group

Participants across the three countries expressed the need to define the level of access to their personal information and content based on their level of trust in individual contacts and or groups to avoid unwanted access to their private information by unapproved contacts.

RELEVANT DESIGN PRINCIPLE #4

Offer flexibility so that users can tailor their trust, privacy and security preferences to specific relationships at the level of granularity that is most meaningful to them

Improving administrative & management tools

Platform design ideas

The following are the preferred design ideas that were generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to serve as inspiration for new features and design improvements for private messaging platforms providers.

Key

Applicability of idea

- Cross-cutting** - idea was welcomed by most users we spoke to across all three countries and identified archetypes
- Segmented** - idea was welcomed by some archetypes and/ or countries.

Type of idea

- New** - new idea that's not based on an adaptation of existing features
- Incremental** - idea is an adaptation or an addition to an existing feature

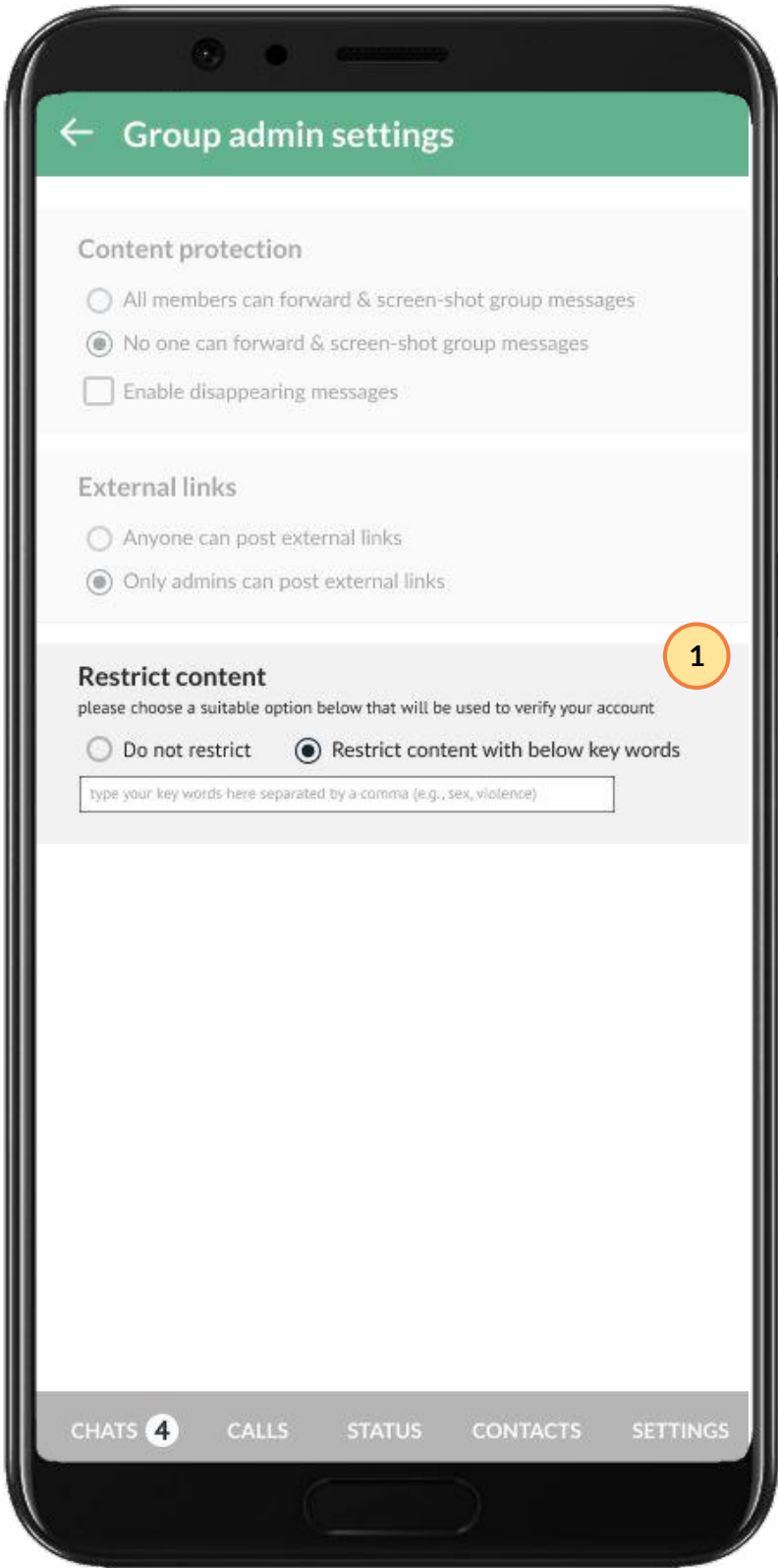
CONTENT MANAGEMENT

Examples of relevant design ideas:

5A. Content restriction in groups

Ability for admins to restrict non-relevant or fraudulent content to avoid misuse of group spaces. Admins can input keywords in the content restriction settings to identify contents/messages for relevant action steps (e.g., review of flagged content before posting or deleting)

● Segmented idea ● New idea



Considerations

- User testing** - This idea was discussed with users in Colombia
- Novelty**: This idea **does not derive** from existing feature on private messaging platform/s
- Popularity** - N/A
- Notable trade-offs** - Some admins may use this feature to block certain content without the knowledge or the support of the other members. This idea has the potential to be misused by admins to censor certain topics of conversation. It also creates a bit of a burden for admins to build out and maintain a user of back-listed terms.
- Other relevant factors** - Identification of restricted key words or content should be inclusive of all members input to ensure transparency and accountability.

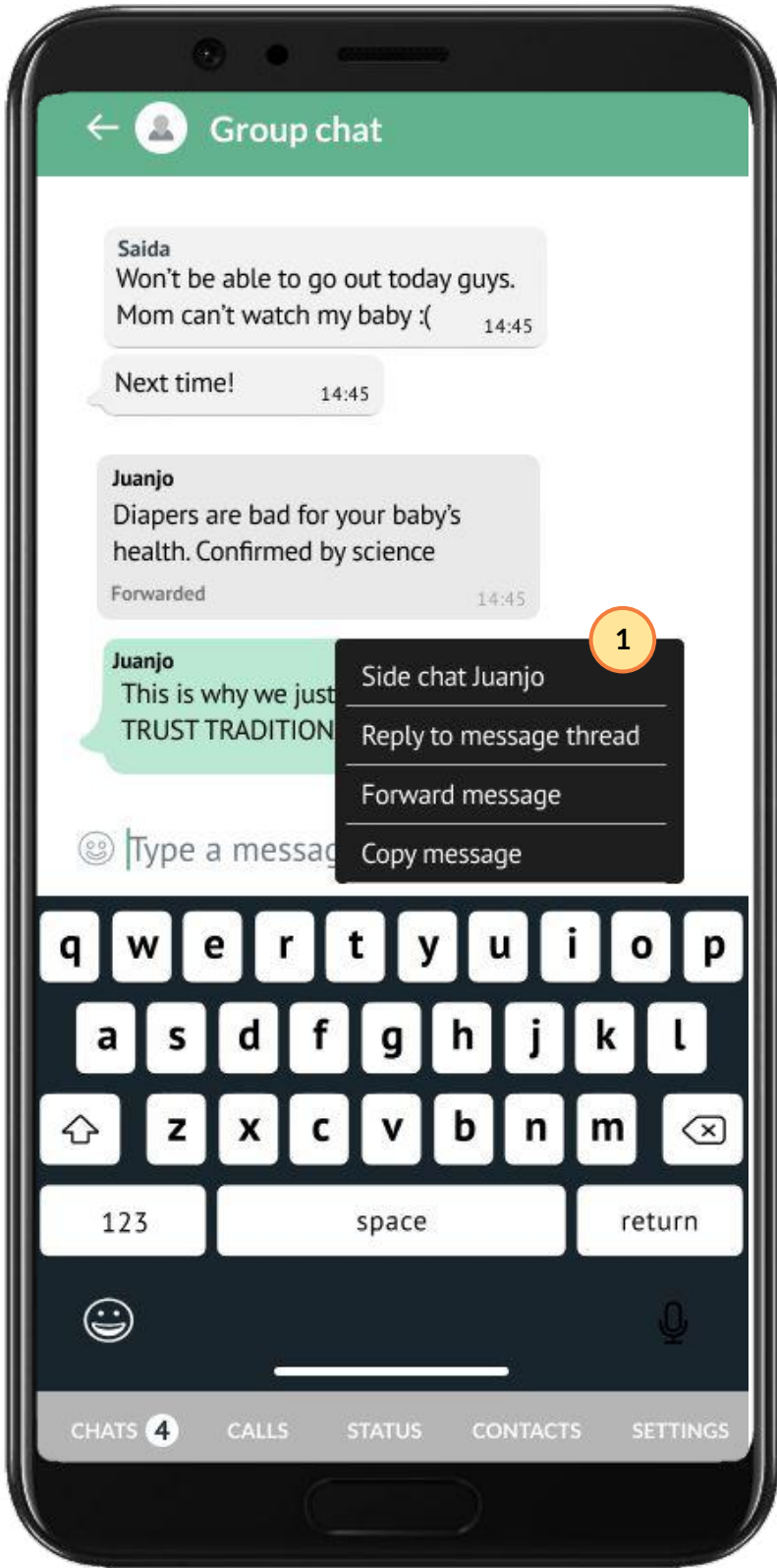
Key feature/s

- 1 **Enabling admins to restrict content in groups** - to filter contents shared in the group to remove unwanted content

5B. Lateral chats in groups spaces and message threads

Enabling users in group chats to start temporary conversations for side topics that are relevant to fewer people and/or individual message threads (e.g., nested replies to a message). While this idea does not directly address a specific privacy or security concern, users generally feel overwhelmed by the volume of notifications they receive and voiced concerns that this undermines their ability to make good decisions to reduce the potential harms they face. So design enhancements that reduce traffic, particularly for less relevant conversations, would be welcomed and could contribute to overall confidence and trustworthiness for many users.

● Segmented idea ● Incremental change



Considerations

- User testing** - This idea was discussed with users in Colombia and the US
- Novelty**: This idea **derives** from existing feature on private messaging platform/s (e.g., [Slack message thread](#))
- User testing** - This idea was discussed with users in Colombia and the US
- Popularity** - This idea was popular with participants in the US
- Notable trade-offs** - Tracking and history of subthreads, especially side chats. Accountability of conversations in side chats to the rest of the group members and group admins
- Other relevant factors** - N/A

Key feature/s

- 1 **Enabling lateral chats and message threads for group interactions** - to reduce traffic in main group threads and intentional communication to users who are interested in topic/message

* features/options that lightly obscured are covered in other sections, the others that are darkened are already implemented by existing private messaging platforms

Providing data use transparency & managing data access

This design opportunity addresses platform design gap ‘G. Lack of transparency regarding access to user data’. This opportunity covers the different ways that private messaging platforms could improve how they communicate about user data management and its implications on users’ sense of privacy and security.

Platform design gap addressed

G. Lack of transparency regarding access to user data

There are gaps around who can access, use, and potentially misuse user data (e.g., how and if companies and governments can access user data). At the same time, messaging platforms don’t communicate transparently and in an user-friendly way how they manage and protect users data.

Understanding the opportunity

Most users we spoke with are worried about how their data is used and managed. But they don’t feel they are able to understand how their preferred messaging platform(s) handles these issues. At the same time, most users reported that they don’t read the data policies even if they feel concerned about their security. This is in part due to the way the information is presented to via long jargon. But users also feel that the policies are aimed primarily at protecting the company rather than genuinely informing them and offering options for how they can get control of their data. This often causes user confusion regarding which security and privacy risks are valid or not (e.g., corporate surveillance for ads) based on rumors and other discussions of these risks in the media or their social circles.

In this section we cover the harms that design improvements related to this opportunity could mitigate as well as the principles that will be important to keep in mind when making design changes geared at this opportunity area.

HARMS IT COULD IMPACT

1. Vulnerability to adverse mental health impacts

2. Vulnerability to targeted harassment for youth and young adults

PAIN POINT 1

Lack of promoting a culture that values security and privacy

Along with improvements in UX/ UI design, many users wanted improvements coupled with a campaign to promote a cultural shift encouraging users to care more about their security and privacy.

RELEVANT DESIGN PRINCIPLE #5

Instill a common mental model for how trust and security should work to cement safer practices in communications

PAIN POINT 2

Use of long jargony and non-relevant information

Information intended to explain how user data is managed and security/privacy implications are presented using jargon that users often don’t understand, and in long formats along with other non-relevant information.

RELEVANT DESIGN PRINCIPLE #6

Communicate issues related to privacy and security in simple, user-friendly language so users always understand what is at stake, and can make informed decisions

Providing data use transparency & managing data access

Platform feature ideas

The following are the preferred design ideas that were generated with the participants from our research in Colombia, Nigeria, and the US. These ideas are intended to serve as inspiration for new features and design improvements for private messaging platforms providers.

Key	
Applicability of idea	
● Cross-cutting - idea was welcomed by most users we spoke to across all three countries and identified archetypes	● Segmented - idea was welcomed by some archetypes and/ or countries.
Type of idea	
● New - new idea that's not based on an adaptation of existing features	● Incremental - idea is an adaptation or an addition to an existing feature

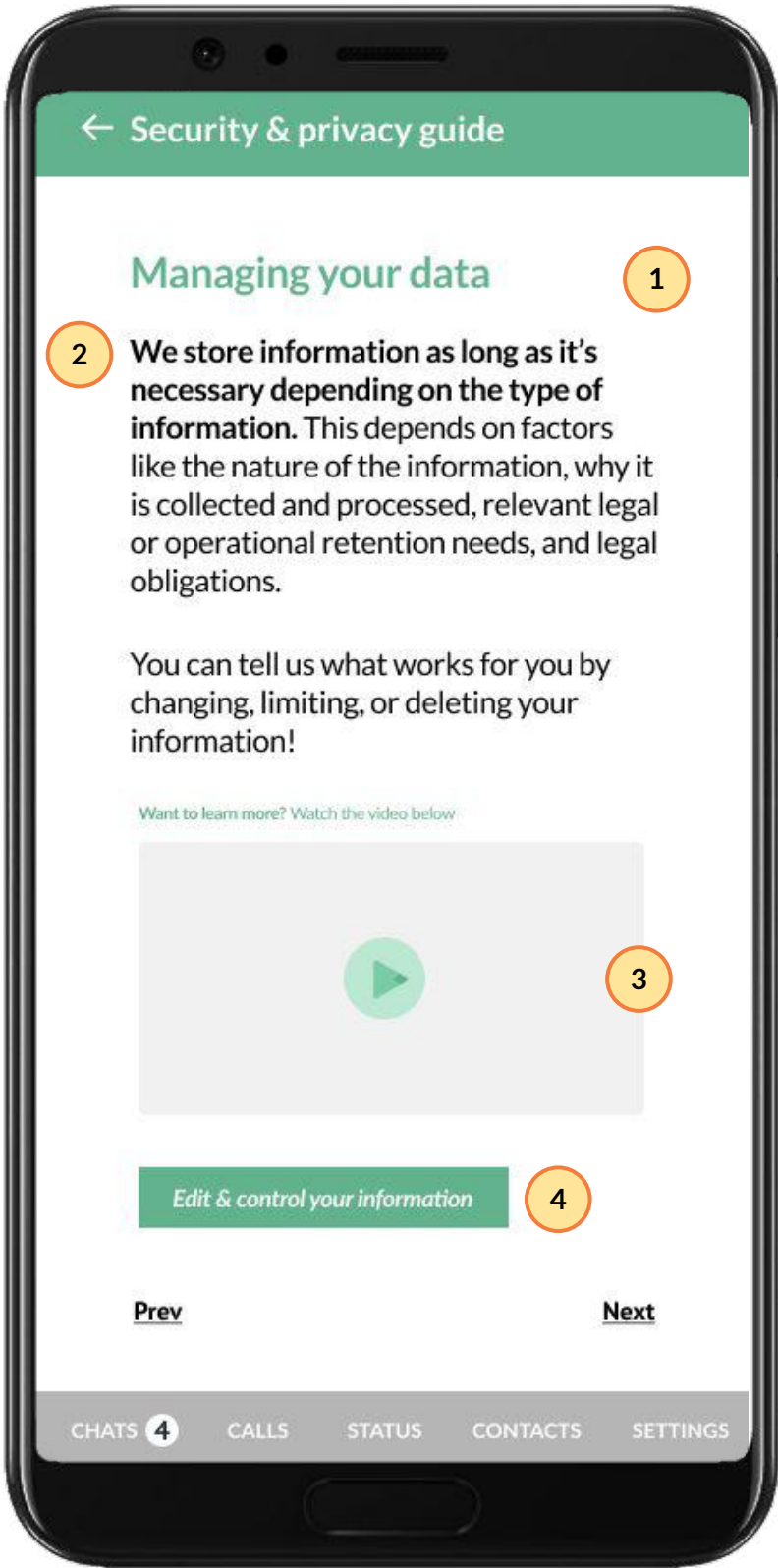
USER FRIENDLY DATA POLICY

Examples of relevant design ideas:

5A. Optimising language, and content on data policies

Optimising user data policy information to increase access and use. This includes but is not limited to the use of more user-friendly language, reducing content to bite-size nuggets, and prioritizing user-centered information that puts the reader at the center of managing their data to increase confidence and trust in data policies

● Segmented idea ● N/A



5A Considerations

- **User testing** - This idea was **discussed and tested** with users in Colombia and the US
- **Novelty**: N/A
- **Popularity** - popular with low-tech comfort users in Colombia
- **Notable trade-offs** - N/A
- **Other relevant factors** - Data policies should be made accessible to users through their private messaging platforms to increase reach. Use of visuals to communicate important information is also highly recommended for low literacy users

Key feature/s

- 1 **Prioritising user-centered information** - to put users at the center of managing their data and increase confidence and trust among users.
- 2 **Optimised/bite-size content** - to enable users to quickly digest information in a more manageable way
- 3 **Use of visuals/video** - to communicate important steps and complex information in a user-friendly format.
- 4 **Clear call to action** - to encourage users to act on relevant user data

5B. User oriented data policy guide

Surfacing data policy information in a manner that encourages user action (e.g., walkthrough guides, use of visuals including videos, communicating clear next steps, etc): This would enable many users to better comprehend data policies and be more proactive in managing their data.

5B Considerations

- **User testing** - This idea was **discussed and prototyped** with users in Colombia and the US
- **Novelty**: This idea **does not derive** from existing feature on private messaging platform/s
- **Popularity** - popular with low tech comfort users in Colombia and low literate users
- **Notable trade-offs** - N/A
- **Other relevant factors** - Users should be able to follow up with private messaging platforms on important questions that emerge following the privacy guide



05 Approach

Approach



This research was carried out using a mixed methods approach that brought diverse perspectives and experiences to the table while prioritizing learning as much as we could from users directly. Each phase of the research process was guided by a common learning agenda that was informed and shaped with expert input from a globally diverse group of perspectives. We selected Colombia, Nigeria, and the USA to represent a diversity of markets where private messaging platforms play a dominant, though somewhat distinct, role in people’s personal and professional lives. To maximize the opportunity to learn from and with our participants, we incorporated a robust, participatory approach (leveraging prototypes and other stimulus) to uncover important insights and surface ideas to address serious harms enabled by private messaging platforms. Key elements of our research approach are summarized below:

UX review

Our design team conducted desk research and an UX review of key features of several popular private messaging platforms. In our UX review, a significant focus was on privacy and security features to build foundational knowledge and to identify initial gaps and opportunities as input to developing and testing prototypes of design enhancements.

Expert workshops

We engaged a diverse group of experts in the private messaging ecosystem (e.g., policy makers, private messaging tech experts, civil society leaders, academics) in a series of workshops to refine the learning agenda and identify key focus areas and recruiting criteria to guide our user research.

1:1 and small group discussions

We recruited a mix of research participants from each country to participate in remote small group discussions where they shared stories and contextualized their issues and concerns within their lived experience as frequent users of these platforms. In selecting participants, we focused on specific criteria and risk factors rather than a demographically representative sample. Our experience suggests that these “edge” cases with higher needs, whether human rights activists or recent immigrants, have the most teach us about where these platforms are falling short.

Building early prototype design ideas

To translate the design considerations into ideas, we tested with users a variety of prototypes and used the feedback from these sessions to refine and build new ideas. Early prototypes focused on visualizing the key features of the design idea and were in the form of a clone of rough messaging app screens.

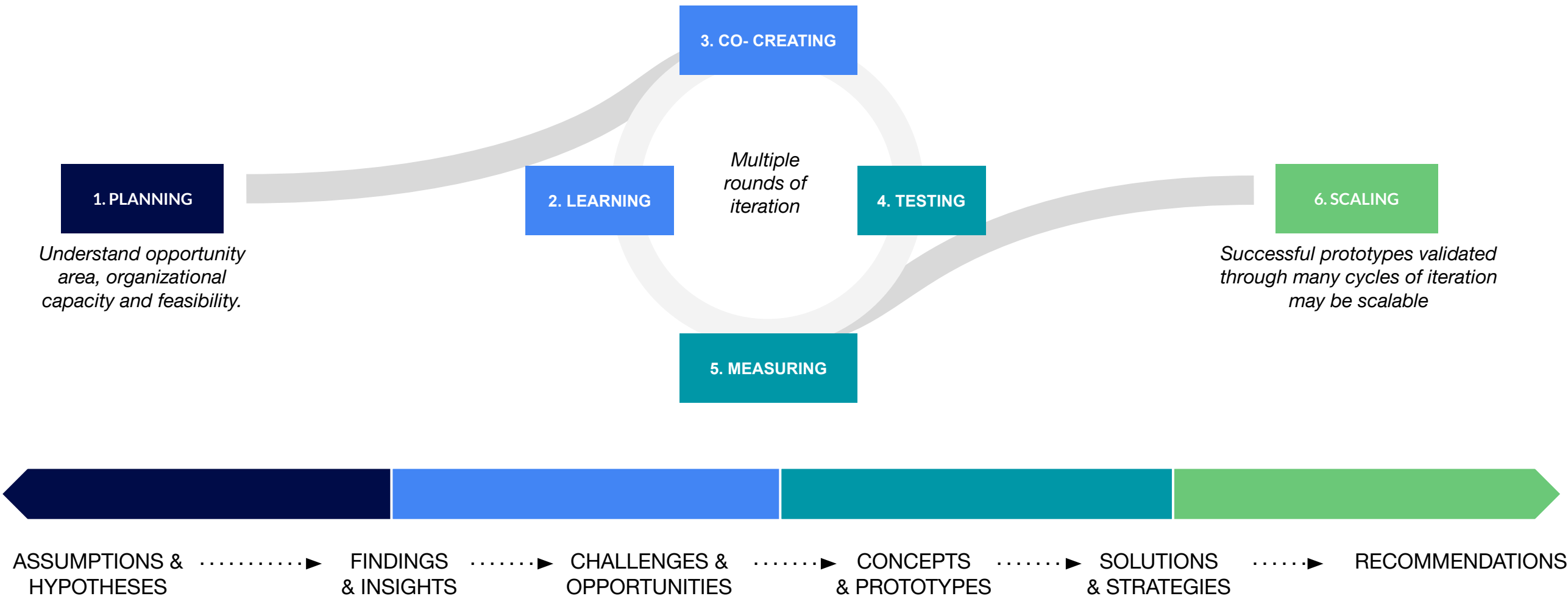
Rapid testing and participatory design

We rapidly and iteratively tested early prototypes through participatory design methods. Each prototype design idea had a clear value proposition and assumptions to test as well as a set of exploratory questions. Using participatory methods, we probed the prototype design ideas in-depth, refining them iteratively across our sessions. We also created space to allow for co-designing with users to generate new ideas that are responsive to their lived experiences. Over the course of the project, the thinking and design ideas evolved, and we validated those changes in subsequent prototyping sessions with new participants. (*Learn more about how Dalberg applies human-centered design by placing people at the center of the design, innovation, and implementation process [here](#).*)

Equity-centered approaches

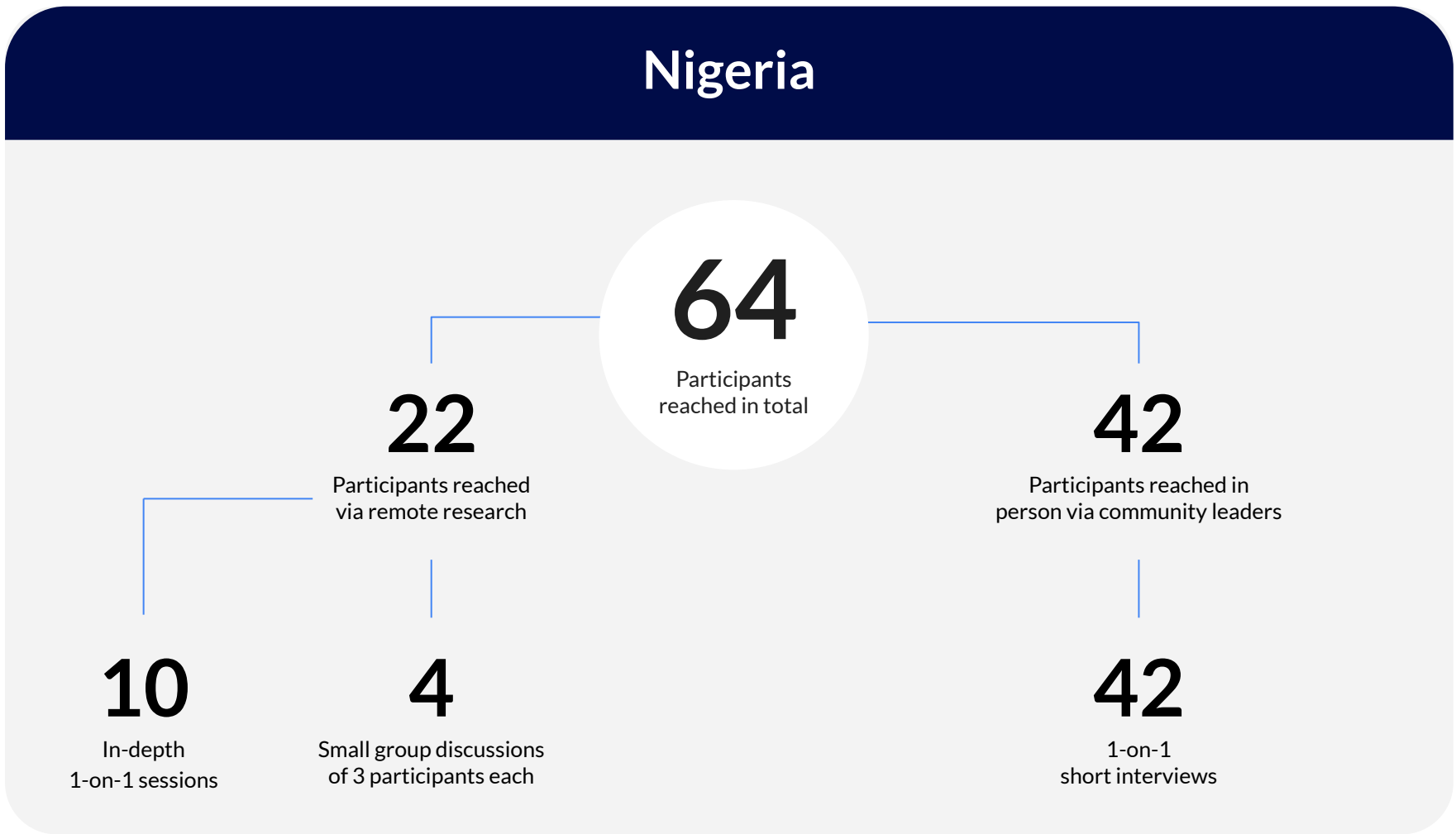
As we grapple with the negative effects of messaging platforms, the conversation often tilts toward the needs of technology companies or policymakers. One primary goal of this research was to bring voices to the forefront that are often marginalized. To that effect, we evolved our research approach to consider issues of equity in how we selected and engaged participants. This involves research models where we partner with community leads in rural areas to conduct in-person prototype testing and research based on remote training by the Dalberg team, for example. These equity-centered models allowed us to leverage the trust that community leads have with their local community and helped to surface cultural and social nuances that impact usage of private messaging applications. (*Learn more about Dalberg’s equity-centered design approach [here](#).*)

OUR PROCESS



Participants & sessions

In the course of ten weeks, we engaged a total of 185 participants, which included ecosystem experts from several countries in rounds of co-creation workshops, community leaders and product users in 1-on-1 and small group discussions in Nigeria, Colombia and the United States. All sessions were conducted remotely except for the community-led sessions. Below is a breakdown of the user research sessions and participants for each country.



Thank you

Dalberg

SUPPORTED BY

