UNBREAKABLE:

Designing for Trustworthiness in Private Messaging

October 2022

Dalberg

SUPPORTED BY

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

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**

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 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**

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:

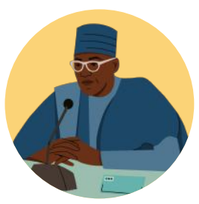
Nigeria

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.

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.

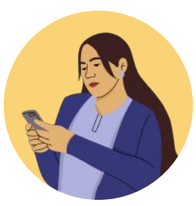
United States

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

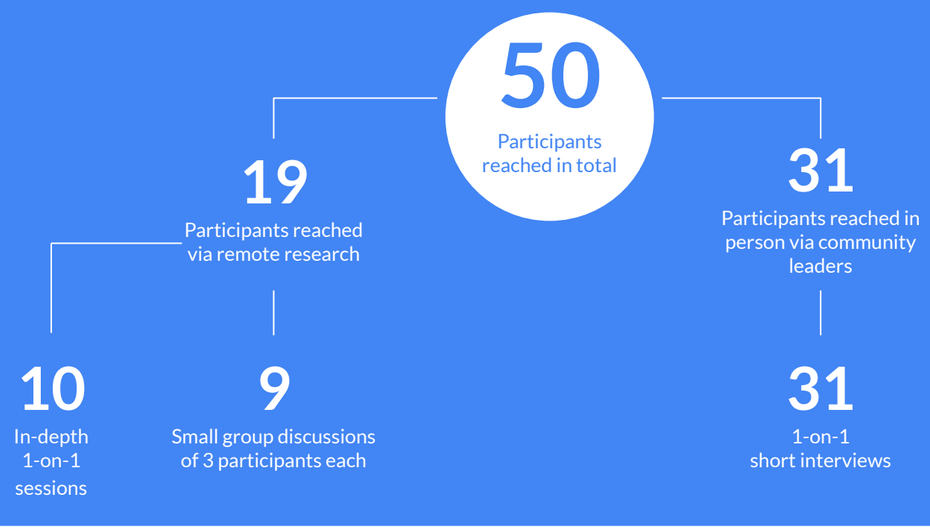
This archetype comprises individuals who conduct frequent international communications across multiple private messaging platforms (e.g., frequent travelers, international students).



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



The Colombian Context

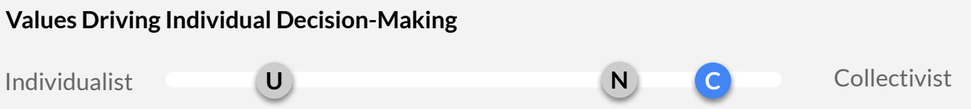
Colombia has a population of about 51 million people, with 66% internet penetration as of 2022.[1] It has a strong collectivist culture relative to the other countries we studied. Belonging and aligning yourself with a group's values and opinions is very important at many different levels in Colombian society, as reported by our research participants. This often shapes structures in social and professional circles and reflects how power is concentrated[2] 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 2019[3]**.** 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.

RELATIVE CHARACTERISTICS

Private Messaging App Market

Values Driving Individual Decision-Making



Decision-Making in Groups

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 prefered, but do not offer comprehensive privacy/protection of individuals and their information.

Related Global Harms

- **Vulnerability to hacking, scamming, blackmailing, extortion, fraud, and harassment**
- **Vulnerability to encryption and data breaches via modified and third-party supporting platforms** *]*
- **Vulnerability to digital surveillance and monitoring**

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*)*
- **Providing accessible & tailored security & privacy controls** *(e.g., concealing & locking chats in user inbox)*
- **Improving verification & permission mechanisms** *(e.g., unknown contact verification)*
- **Improving administrative & management tools** *(e.g., enhanced user* controls for screenshots and forwarding messages*)*

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**
- **Vulnerability to targeted harassment for youth and young adults**
- **Vulnerability to encryption and data breaches via modified and third-party supporting platforms**
- **Vulnerability to adverse mental health impacts**

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*)*
- **Providing accessible & tailored security & privacy controls** *(e.g., concealing & locking chats in user inbox)*
- **Improving verification & permission mechanisms** *(e.g., unknown contact verification)*

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

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*)*
- **Improving verification & permission mechanisms** *(e.g., content verification and blocking, new contact & group verification)*
- **Providing accessible & tailored security & privacy controls** *(e.g.,custom group privacy settings*

Thank you

Dalberg

SUPPORTED BY

OMIDYAR NETWORK™