Beyond Encryption: Our Vision for Trustworthy Messaging in a Viral World

OMIDYAR NETWORK™

Beyond Encryption: Our Vision for Trustworthy Messaging in a Viral World

Private messaging platforms like Messenger, Signal, Telegram, WeChat, and WhatsApp are seminal technologies. By assuring private communication on a global scale, these innovations expand and protect democracy as well as our human rights. They have fundamentally reshaped human connection.

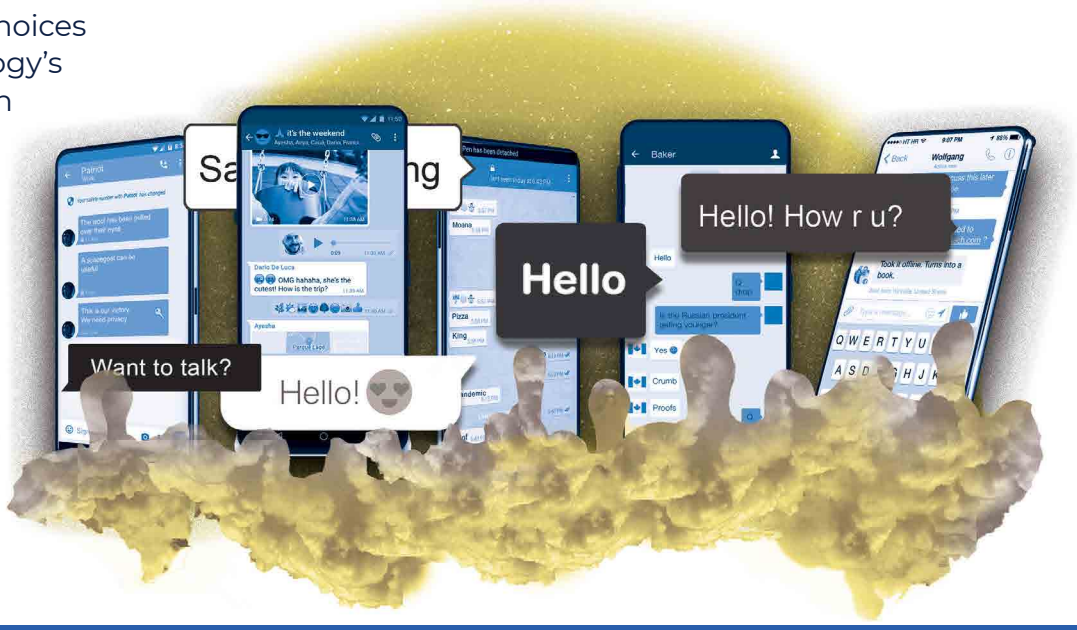
Omidyar Network believes in the promise of this type of technological innovation. We also believe tools with this depth of political, economic, social, and cultural influence must be held to the highest standards of trustworthiness and safety.

For the past three years, we have invested in individuals and organizations that are working to make private messaging platforms more trustworthy (and as a result, safer). We have seen firsthand the pivotal role of private messaging platforms in empowering diverse ideas and social movements. And we have witnessed the inequality, injustice, and trauma that result from risky design choices which preference the technology's scale, virality, and monetization over its users' well-being. To preserve the best qualities of these innovations, all stakeholders must engage in renovating the product designs, policies, and incentives that introduce and increase risk.

We call on technologists, investors, nonprofits, researchers, and governments around the world to join us and play a critical role in ensuring private messaging platforms are trustworthy by:

1. **Upholding encryption that empowers users, communities, and movements; and**
2. **Establishing incentives that promote safer design choices, transparency, and accountability.**

We believe these joint priorities will lead to the breakthroughs that make private messaging platforms safer—less hospitable places for hate, violence, abuse, and lies—and more trustworthy tools that are indispensable for free and open societies everywhere. Our principal belief in the power of innovation means we don't have to choose between privacy and safety.



Groundbreaking, global, and growing

In just over a decade, private messaging platforms like Messenger, Signal, Telegram, WeChat, and WhatsApp have become a critical and central component of our digital existence. Ubiquitous in nearly every country around the globe, their scale is staggering.

Since it launched in 2014, Telegram's user base has increased tenfold, jumping from 50 million active users in 2014 to 500 million in 2021. WhatsApp, the most popular private messaging service in the world, reports its two billion users send more than 100 billion messages each day; that's 1.1 million messages per second. In the US alone, Meta's (formerly Facebook's) Messenger is on track to add 2.2 million more users (or 6,000 per day) in 2022. And WeChat boasts nearly as many active users as the population of China: 1.25 billion. In 2022, market research companies estimate that two people in every household (or roughly 40% of the global population) will be actively using the mobile version of at least one private messaging platform.

This mass digital migration is a relatively new phenomenon. Prior to 2009-2010, when WhatsApp and an early version of Signal entered the market, most private messaging took place via SMS or email. Users who wanted more convenience and real-time connection often opted to communicate via open chatrooms, message boards, and social media platforms that could be monitored by other users. Early adopters of private messaging platforms, including journalists and activists living in oppressive regimes, were attracted to the privacy and security features they offer—often in the form of encryption, which is the process of converting information into code to prevent unauthorized access. By virtue of the technology underwriting encryption, platforms offer up a degree of security that simply isn't present on open social media platforms.

> **Encryption is the process of scrambling data to prevent unauthorized access. It is an essential feature of a safe and trustworthy Internet.**

Over the next five years (2010-2015), private messaging's salience grew as widespread digital surveillance and cybersecurity threats targeted email, discussion forums, social media, and other online accounts. A boom of new private messaging services—including Messenger, Telegram, Line, Viber, Wickr, and WeChat—started offering encrypted peer-to-peer and group messaging options for everything from private family photo sharing to social and work discussions. Using low bandwidth, these platforms made it convenient and affordable (often free) to instantly send text, images, audio, documents, and video to one or many users in multiple languages, across borders, and away from prying eyes.

Responding to user demand as early as 2016, many previously open or semi-private spaces, like social media and video conferencing platforms, began adding higher standards of privacy and security and adding other features to join this special class of encrypted technologies. Then separate pressures and policy decisions surrounding Covid-19 and the 2020 US presidential election further drove up demand for and usage of private messaging platforms globally. These events also spurred many of the private messaging platforms to evolve and support voice and video calls for individuals and groups.

In early 2021, Meta announced plans to encrypt all multi-media messages on Instagram and Messenger, signaling the true mainstreaming of private messaging. Jan Koum, one of the original founders of WhatsApp, has declared "the encryption genie is out of the bottle," and the technology can (and should) no longer be ignored or denied.

In late 2021, Meta decided to delay encrypting messages on Messenger and Instagram until 2023, citing the need for more time to reckon with public safety concerns on the platforms. For many technology companies, accommodating both privacy and safety has been a stumbling block.

This moment demands a new vision: a world in which messaging platforms are more than private—they are trustworthy.

SHOWCASE: THE FIVE LEADING PRIVATE MESSAGING PLATFORMS

	Messenger	Signal	Telegram	WeChat	WhatsApp
OVERVIEW					
Monthly active users	1.3 billion	40 million	550 million	1.25 billion	2 billion
Management	Stan Chudnovsky, Head of Messenger	Brian Acton & Moxie Marlinspike, Co-founder	Pavel Durov, Co-founder & CEO	Allen Zhang, Senior Executive Vice President & President of Weixin Group	Will Cathcart, Head of WhatsApp
Ownership	Meta (formerly known as Facebook)	Signal Technology Foundation	Pavel and Nikolai Durov	Tencent Holdings, Ltd.	Meta (formerly known as Facebook)
Governance	9 board members*	3 board members (including the co-founders)	Undisclosed	8 board members	9 board members*
Company HQ	Silicon Valley, USA	Silicon Valley, USA	Dubai, UAE	Shenzhen, China	Silicon Valley, USA
FEATURES					
Nature of encryption	Users can opt-in for end-to-end encryption	Users experience end-to-end encryption by default	Some chats are encrypted; channels are not encrypted	Partial encryption; WeChat can decrypt messages sent on the platform	Users experience end-to-end encryption by default
Group size	250	1,000	200,000 Channels can have an unlimited number of subscribers	500	256
Forwarding and broadcasting	• Users can forward messages to 5 others • Standard users cannot broadcast messages	• Users can forward messages to 5 others • Users can broadcast unlimited photos and videos	• Users can forward messages 2,000 times per hour • Group admins can broadcast unlimited messages	• No forwarding • Users can broadcast to 200 people at a time	• Users can forward messages to 5 others • Users can broadcast to 256 people at a time
User controls	• Block a user • Report a message or entire conversation • Approve message requests	• Block a user or group • Report a message or entire conversation • Report security vulnerability • Approve message requests	• Block a user • Report a post • Report an individual • Report a group • Report a channel	• Report illegal information	• Report a user • Report a single message • Block a user

Forwarding involves user B sending a message that user A sent onto to multiple recipients with one click. Broadcasting involves user C sending an original message they created to multiple recipients with one click. On Telegram, "channels" are a tool for broadcasting public messages to large audiences.

*Messenger and WhatsApp executives report to the same board of directors.

The end-to-end of the world

Just like the social media platforms before them, private messaging platforms have fueled harmless connection and entertainment as well as objectionable and illegal behavior. Reports of violence, disinformation, and manipulation campaigns originating on private messaging platforms like Messenger, Signal, Telegram, WeChat, and WhatsApp have become all too common. Not only are individuals' lives and liberties impacted, but dangerous platform design choices also have devastating implications for our democratic institutions and the health and well-being of our societies.

Until recently, these instances were concentrated in the Southern Hemisphere, where the largest base of messaging platform users live. In 2018, we started seeing reports of rumor-based messages and subsequent riots contributing to dozens of deaths in India and then later in Indonesia; incendiary political messages that may have swayed elections in Nigeria and Brazil; and scams and hoaxes that allegedly manipulated users in Kenya and South Africa.

Despite warnings from civil society organizations, media, and researchers, problems surfacing on the private messaging platforms went largely unheeded by technology companies, their investors, and Western politicians until they started to see the consequences in their own backyards. These incidents should have represented the canary in the coal mine. Now with the platforms' growth in popularity, the damage has begun to spread across the globe.

January 21, 2020:

Elected officials and scientists began reckoning not only with shocking spikes in deaths and infections related to Covid-19, but also the misinformation driving the pandemic.

November 3, 2020:

A highly charged election in the US revealed that domestic and foreign groups with nefarious agendas were running strategic and highly networked disinformation campaigns on private messaging and other platforms to encourage doubt, polarize citizens, and generate national instability.

January 6, 2021:

The US Capitol was invaded by conspiracy theorists, racists, and others who were manipulated by mis- and disinformation. They organized using private messaging platforms to violently protest election results, challenge scientific recommendations related to the pandemic, and uphold white supremacy.

SHOWCASE: RECIPE FOR DISASTER

1. DESIGNS THAT EXPLOIT GROUP DYNAMICS

Private messaging companies like WeChat have recognized the opportunity to design for "group effect." They have special features that prompt users to recruit others to the platform, knowing that people will use the service more when they are connected to trusted contacts and large networks. And some platforms help introduce strangers based on location and algorithm, knowing that people are lonely and crave more real-time connection. These features have been critical to the platforms' rapid growth. Yet the "group effect" is not always as productive for society as it is for generating profits. Individuals often behave differently when in community. Sociologists have found people are less likely to exercise their agency, question information, call out bad behavior, or report crimes when in groups—all of which are needed to combat mis- and disinformation online.

2. DIGITAL MEGAPHONES THAT ECHO

A key differentiator between open social media and private messaging platforms has been that the former serves as the public "town square" and the latter as the private "living room." Signal and Telegram, however, offer users the ability to broadcast and exchange ideas within extremely large groups—1,000 and 200,000 people, respectively. This feature, which breaks away from the original vision for private messaging platforms, is particularly attractive to users who want to organize and influence at scale while also benefitting from privacy, like subversive political movements and extremists.

3. CONVENIENCE THAT SPREADS RISK

The pressures stemming from the Covid-19 pandemic forced governments and private messaging platforms to redouble their efforts to confront the viral spread of false information. The ease with which users can now forward messages without verifying their accuracy means misinformation can spread quickly, secretly, and at significant scale. Research shows that conspiracy theories and racist beliefs are more likely than fact-based information to be forwarded on Messenger.

4. BUSINESS OBJECTIVES THAT ERODE PRIVACY

In 2021, WhatsApp attempted to change its privacy policy to allow businesses that provide services and collect payments via the platform to use customer data in new and invasive ways. The plan triggered a global protest and an exodus of WhatsApp's users to competing platforms. WhatsApp ultimately backed down on its plans to delete accounts or limit functionality if users did not agree to the new terms.

More than private

Privacy is essential to building trust, but it is not a singular standard for safety. **We believe online safety is the result of trustworthy technology and enlightened regulation.**

While the shift toward adopting end-to-end encryption has reinforced trust between users, the technological architecture that encourages scale, virality, and monetization has ultimately facilitated the rapid and large-scale spread of dangerous, distorted, and deceitful content. Therefore, many of the platforms' other design choices and business decisions make them objectively unsafe and unworthy of our trust.

To be truly trustworthy, private messaging platforms, their leaders, and their investors must prioritize:

1. **Un-surveilled communications; and**
2. **Responsible design choices, policies, incentives, and rules that mitigate and anticipate the harms these technologies can cause.**

> **"Not-so-public, digital spaces demand more contemplation, and will inevitably serve an important role in the next generation of social media. My guess is it'll be in these smaller spaces, not the big public platforms, where we'll build some of our most valuable infrastructures of care." (New_Public)**

The future is trustworthy

Our roots in Silicon Valley and global outlook give us deep insight into these problems and an informed perspective on how to approach this complex task—one that often pits the rights of some against the rights of all.

To be clear, we lean toward solutions that protect everyone's liberties. We recognize this belief can be unpopular and requires tradeoffs and difficult decisions. For example, we believe the most effective solutions lie in confronting the suboptimal design choices of platforms themselves, rather than trying to censor

What is trustworthy?

Messaging platforms and the companies who operate them should:

- Facilitate private communication and prohibit surveillance
- Respect all other human rights
- Modulate virality
- Grow responsibly without harmful design
- Clearly communicate design and policy changes
- Share insights about risks as well as the effectiveness and impact of their product decisions and policies
- Offer clear and accessible ways for users to report abuse and other harms
- Provide responsive remedies to risks and harms

problematic content and objectionable behavior, which can quickly result in many questions and concerns about users' rights to privacy and freedom of speech.

Content moderation that respects human rights is a thorny proposition that requires every member of society to be in alignment. Picking winners and losers in the marketplace of ideas is not the role of technology companies. The companies managing private messaging platforms, however, have total control over their design choices and business decisions. **If they had the will or were required by regulation, they would find a way to make their platforms safer and more trustworthy.**

We believe technology design and governance choices have had an outsized influence in affording private messaging platforms the massive scale, unprecedented velocity, and extraordinary reach that fuels hate speech, disinformation, manipulation campaigns, and calls for violence.

Naturally, focusing on the underlying design choices or governance decisions of the platforms will not, in and of itself, eliminate all risk. The marketplace enables all types of users—be they families and colleagues, dissidents or activists, or spreaders of hate speech and disinformation—access to private messaging services. However, pursuing industry-wide changes in product design, policy, and business decision-making will fundamentally reduce the ways private messaging platforms can be exploited without compromising users' right to private communication. With better understanding of the technology's architecture, we can change the tools that bad actors depend on, make the platforms less reactive to their strategies, and stay ahead of their next move. And instead of finding and fighting bad actors individually, we can make sure private messaging platforms are no longer hospitable places for hate, violence, and lies.

New settings

All technologies are active choices and constructs, and, like markets, they are shaped by society. We have always believed in the power of markets and technology to build a world where everyone has the power to thrive. Collectively, we must design and govern private messaging platforms responsibly, based on two crucial priorities.

1. Uphold encryption to protect the right to privacy

Private communication is an important element of a dignified and independent life. We believe protected, un-surveilled communication is essential for individual agency, civic participation, social connection, personal safety, and democracy.

When advocating for vulnerable members of society, law enforcement and children's protection groups understandably point out the challenges of doing so on closed messaging platforms. Indeed, societies must innovate to identify targeted tools and thoughtful policy responses to lawfully find and address illegal behavior in private spaces, but without resorting to polarized and absolutist positions. Attacks on encryption from governments or companies via "back doors" or by weakening privacy and security via malware, spyware, or ill-conceived traceability requirements makes us collectively less safe and makes private messaging platforms less trustworthy. And ultimately, solutions that require access to content are rarely effective as demonstrated in recent research by Stanford University's Riana Pfefferkorn.

While the idea of maintaining the online privacy of criminals, racists, and extremists may be hard to accept, breaking encryption comes at a significant societal cost—one we cannot afford if we want to remain or aspire to a free and open society.

History has shown that without the ability to organize privately, social movements that have promoted everything from scientific inquiry, women's safety, and LGBTQIA+ rights to democracy and worker power would never have been able to take root and thrive. The same goes for the right to dissent, to challenge human rights abuses, and to protect children, marginalized groups, and vulnerable communities—particularly in non-democratic and restrictive societies. Today, technological features like encryption provide one of the only means by which important, geographically diverse movements and whistleblowers can organize beyond the invasive reach of governments and companies.

> **"Without robust encryption, human rights everywhere—on- and offline—will erode."**

2. Change the industry's incentives to drive responsible product design choices and accountability

To maximize scale, market share, and profits, platform companies are incentivized to target and acquire massive user bases, engineer for convenience and minimal friction, and maximize engagement and virality. Some go as far as harvesting reams of data about users that can then be monetized (e.g., via targeted advertising). Unfortunately, these are the same design features that are exploited for more nefarious purposes like online radicalization or the spread of disinformation. Because of these incentives, more responsible and less risky (i.e., less engaging and profitable for companies) platform designs, architecture choices, and safety research are often deprioritized in the innovation process.

The current model of capitalism is failing. We must confront key incentives—market share, data, and money— and reimagine them such that markets reward businesses that contribute to the common good while simultaneously curbing the pressures that drive negative outcomes for people and planet.

In this space, we need new incentives designed to generate trustworthiness. For example, consumer pressure and government rule-making can motivate and reward the technology companies that demonstrate transparency and invest in product design changes that create friction—such as responsible forwarding limits, smaller group sizes, and slowing down transactions. We know these design choices significantly inhibit virality—that is, the fast and wide sharing of dangerous, distorted, and deceitful content—while also building trust and credibility.

We see many opportunities to tackle these incentive issues right now, as the technology companies are actively trying to find sustainable revenue models for private messaging services. Some have leaned on the experience of the open social media platforms, as we saw in the recent case of Meta revoking its promise to never monetize WhatsApp user data. These same companies have also refused to change their platforms' architecture to improve safety and build trust with users because they see these moves as conflicting with growth. That is a false dilemma.

Signal and Telegram are not yet revenue-positive, and WeChat is only sustainable because it is integrated into an e-commerce platform. How these platforms approach making money—hopefully without doubling down on the incentives that lead to risky design and exacerbating the harms associated with surveillance capitalism—will be a key indicator of our collective success. We must change the incentives to include other stakeholders' interests before these platforms lock in profitable but harmful business models. For example, society can preference companies that co-design solutions and invest in user agency and empowerment via features that preserve privacy while allowing for better tagging of problematic content and reporting of abuse. We believe platform companies that prioritize encryption and build trustworthiness with "content oblivious" solutions could ultimately become market leaders in the next 5-10 years.

Eyes off, responsibility on

For our vision to become reality, we propose three immediate actions that will shift power from a few influential technology companies to a wider group of stakeholders, including nonprofits, researchers, governments, and purpose-driven investors. We must give these leaders a much larger role to play in establishing a new set of conditions: greater disclosure and transparency, a system of distributed governance and accountability, and more collaborative research and innovation with technologists. And to ensure the future is always trustworthy, it also will be critical that any technological fixes, policies, governance structures, and learning networks remain flexible and dynamic to respond to evolving technology and an ever-changing landscape.

Disclosure and transparency

The closed nature of private messaging platforms makes it nearly impossible to identify where and how problematic content originates, how much of it is organized versus organic, or to predict how viral it might become. This necessary shield severely complicates the mitigation—let alone elimination—of these problems.

Technology companies have used this dilemma and their desire for competitive advantage to defend their lack of cooperation in addressing the weaponization of their private messaging platforms. Yet we know that even with encryption, technology companies have access to relevant data because they use those insights to entice advertisers and make product changes. Private messaging companies must be forthright with to researchers and regulators about the nature and extent of the data they do collect, who it's being shared with, and how it's analyzed to influence design and business decisions.

To be clear, we do not believe information that is typically referred to as "metadata" should be shared. While end-to-end encryption prevents outsiders (and even the platform companies) from seeing content, metadata can include other information about specific individuals and can be deeply personal to users, such as one's name, email address, mobile number, close contacts, and even payment information. It is important to protect the privacy of this type of personal metadata, which is why the United Nations Office of the High Commissioner for Human Rights rightly considers a user's metadata to be covered by the right to privacy when applied to the online space.

Yet anonymized, aggregated datasets, or the "metadata of metadata," can shed light on important patterns, such as how many users a platform has, where the majority of accounts are created, how users engage on the platforms, how groups form, what patterns and behaviors they exhibit, what percentage of messages goes viral, what types of messages are commonly reported, how many users are blocked or banned, and which features effectively enable or stem usage. This type of data can, without compromising encryption and privacy, be used by platform companies and independent stakeholders alike to recommend and pursue game-changing improvements in product design, policy, and incentives. Unlocking what companies know about how the platforms perform and sharing those insights with regulators and civil society organizations is

essential to bridging the gap between simply private messaging platforms and trustworthy ones. Defining new and limited ways that companies can offer non-personal data for research purposes can help all stakeholders skillfully navigate the tensions that exist between confronting societies' ills without undermining the rights we all hold sacred.

To catalyze this shift, civil society organizations, philanthropic organizations, and shareholders can campaign for disclosure, transparency, and tangible commitments from technology companies. And government institutions, legislators, and independent regulators can impose clear disclosure metrics and transparency requirements, including usage patterns, information flows, data collection, monetization, and commitments to trustworthiness. Technology companies that own and operate private messaging platforms must also conduct risk and impact assessments related each of its features and services, make trackable, public commitments toward reducing the negative impacts, clearly communicate policy and design changes, and open up access to non-personal data for independent research partners.

Distributed governance and accountability system

Following a series of investigations into the major technology companies' actions, lawmakers and oversight agencies are becoming more involved in establishing and enforcing policies specific to private messaging platforms. Government institutions, legislators, and independent regulators can support the vision of trustworthy platforms by mandating transparency in key areas and holding companies accountable for responsible and limited data collection. With such clear rules and expectations for the companies, government can incentivize better innovation and quicker responses toward addressing harmful issues on their private messaging platforms. These companies cannot be relied upon to do this voluntarily. Enlightened regulation— with the help of sustained societal pressure—can help set standards, articulate requirements, and enforce behaviors that help resolve problematic design choices and business decisions. At the same time, such governance must not be a Trojan horse for the suppression of dissent or create exceptional access that erodes privacy.

Additionally, private messaging platforms should incorporate independent experts, including academics and rights-based advocacy groups, into their operations with advisory and oversight prerogatives. Right now, roughly 20 people govern the five market leaders: Messenger, Signal, Telegram, WeChat and WhatsApp; this is an insular and unrepresentative group with concentrated power and little accountability. Making room at the table for other perspectives and objectives can help identify new issues, co-design solutions, and implement changes that best protect users' and societies' interests. For example, external experts can help identify clear and accessible procedures to be responsive to user reports of abuse and harm, and propose mechanisms for redress and remedies. At the same time, civil society organizations must continue to actively hold both technology companies and governments accountable in cases of overreach and surveillance.

Meanwhile, philanthropic organizations, shareholders, and social impact investors should use their power to support and advocate for this vision. They can invest in research and advocacy organizations that sustain pressure, identify new performance metrics that align with trustworthiness, and incentivize better design choices. Those that invest directly in startups and new alternatives must provide new incentives and expectations that compel companies to pursue trust and safety enhancements—even if takes longer to reach scale and profit.

Collaborative research and innovation

We've now reached a point in the evolution of private messaging services when the design and governance choices of a few companies (or rather a handful of leaders and their boards) are of national (and international) interest. We must reckon with the fact that the same convenience, scale, and speed that enable virtuous communications on private messaging platforms have also become vehicles for danger, causing injury to the same democracies, economies, and societies that helped build those tools in the first place. When all segments of society are experiencing negative impacts as the result of private sector companies' decisions, we must all collaborate to install necessary consumer protections.

Technology companies with private messaging platforms must conduct robust research and innovation to improve platform design. We also strongly encourage them to prioritize transparency and collaboration with global civil society organizations from the start. Organizations that protect children, defend human rights, and support those marginalized in society and by technology have important perspectives on how to stop private messaging platforms from being so easily exploited, as do researchers and academics. Greater public understanding of the platforms' architecture will yield more "content-oblivious" solutions, and public involvement will ensure design and governance choices are auditable and accountable to society at large.

The message

We believe that in making popular technology more trustworthy, powerful companies and institutions will become more trustworthy as well. With this foundation, we can all learn to trust information—and each other. We believe these conditions are essential for social change as well as for the safety and security of families and physical communities and the sanctity of our democracies.

Private messaging should be our best ally. By nature, it exists to facilitate trust, candor, belonging, and solidarity among connected users and safety within society. This technology can, when used for its highest good, empower people and communities with diverse perspectives, help develop new forms of understanding, and create a dialogue that is grounded in respect for humanity. The platforms' current design choices unfortunately do not yet fulfill that vision. As currently designed, governed, and regulated, they actively contribute to complex societal problems instead.

The dilemmas posed by today's private messaging platforms are not just technological; they are also relational. Messages sent from loved ones and trusted connections make the ideas within even more potent. Misinformation and calls for violence shared via private messaging platforms are often the manifestation of strained offline relationships between people, ideas, institutions, and societies. In addition to protecting people's right to privacy, pursuing inclusive research and innovation that mitigate risk online, and overpowering the incentives that uphold the status quo, we must also address the root causes.

In light of mounting risk and need for nuanced solutions, Omidyar Network has committed $10 million toward:

- **helping the world to better understand how private messaging platforms work and where their design contributes to these problems;**
- **preserving the platforms' privacy-respecting features;**
- **elevating "content-oblivious" solutions; and**
- **advocating for necessary product design, policy, and rule changes so that private messaging platforms are trustworthy.**

We are actively collaborating with the researchers, technologists, policymakers, and nonprofit advocates leading on this agenda. Since we first took notice of the problems on private messaging platforms in 2018, we've supported more than 15 individuals and organizations—such as Africa Check; Junkipedia; Atlantic Council's Digital Forensic Research Lab; Institute for Strategic Dialogue; Meedan; the Stanford Internet Observatory; and the propaganda program at the University of Texas at Austin's Center for Media Engagement—that are researching and combatting mis- and disinformation in private spaces online. In the next few years, our goal is to work with more stakeholders and expand the network advancing a robust, evidence-driven, and sensible public conversation about private messaging platforms.

This work is reinforced by our broader $60 million commitment toward building a responsible technology system and demanding stronger accountability and performance from companies. Our commitment includes supporting activities related to comprehensive data protection and privacy laws; antitrust action and pro-competition regulation; corporate governance overhaul; alternative business models; new data paradigms; and other essential facets of a better tech system. It also means helping to curb pressures from equity capital markets that reinforce short-termism and benefit speculative actors at the expense of society and reorienting the rules that govern markets to better balance the interest of all stakeholders.

Problems online hardly ever start there—and they rarely end there. But it's our imperative to

Acknowlegements

Published January 2022

Established by philanthropists Pam and Pierre Omidyar, Omidyar Network is a social change venture that has committed more than $1 billion to innovative for-profit companies and nonprofit organizations since 2004. Omidyar Network works to reimagine critical systems and the ideas that govern them, and to build more inclusive and equitable societies in which individuals have the social, economic, and democratic power to thrive.

Beyond Encryption: Our Vision for Trustworthy Messaging was completed in late 2021. Contributors include Omidyar Network staff members Wafa Ben-Hassine, Subhashish Bhadra, Anamitra Deb, Beth Kanter, Emma Leiken, and Abiah Weaver. We also benefited from the expertise of Elena Cryst and Alex Stamos of Stanford Internet Observatory, David Madden of Luminate, Sam Woolley of University of Texas-Austin, and Jillian C. York of the Electronic Frontier Foundation, all of whom have collaborated with Omidyar Network to study and advocate for more trustworthy, private messaging platforms.

www.omidyar.com/privatemessaging