ENCRYPTED MESSAGING APPLICATIONS AND POLITICAL MESSAGING:
HOW THEY WORK AND WHY UNDERSTANDING THEM IS IMPORTANT FOR COMBATING GLOBAL DISINFORMATION

Katlyn Glover, Mirya Dila, Neeley Pate, Kaiya Little, Inga Trauthig, and Samuel Woolley

SUMMARY

Encrypted messaging applications (EMAs), such as WhatsApp and Signal, are utilized in the spread of political misinformation in the U.S. and around the world. However, general understanding of how they work and the differences between their features is often low. The Center for Media Engagement aims to provide valuable knowledge for journalists, policymakers, activists, and the public about the role EMAs play in the manipulation of public opinion. To this end, this report provides:

• An overview of how various EMAs work
• A review of popular EMAs and their notable features (LINE, Signal, Telegram, Viber, WhatsApp, and WeChat)
• Examples of how EMAs have been used for political manipulation

Traditional social media platforms like Twitter and Facebook play a key role in politics and have impacted elections worldwide. Hidden communication spaces such as EMAs play a critical role as safe havens for democratic activism and information sharing amid growing surveillance. However, there is also mounting evidence of EMAs’ role in the spread of political propaganda and disinformation campaigns. Therefore, there is a crucial need for research in this area — curbing political manipulation on EMAs will require new, nuanced approaches that differ from existing efforts on more public platforms.

SUGGESTED CITATION:
Glover, K., Dila, M., Pate, N., Little, K., Trauthig, I., & Woolley, S. (June, 2023). Encrypted messaging applications and political messaging: How they work and why understanding them is important for combating global disinformation. Center for Media Engagement. https://mediaengagement.org/research/encrypted-messaging-applications-and-political-messaging
Encrypted messaging apps (EMAs) provide fast, mobile, and private communication to billions of users globally.\(^1\) EMAs often offer end-to-end encryption, which ensures that only the sender and receiver can access the content of the messages. A free alternative to other text, video, and audio communication, EMAs allow users to safely connect with people in a private space without fear of their content being accessed by any third-party source — including the platforms themselves.

Encrypted messaging applications also provide users opportunities to engage with others in a multitude of ways via group chats, voice and video calls, file sharing, and stickers. Additionally, chat apps provide an alternative to expensive SMS phone plans and allow users to communicate across the world for free — especially when users have WIFI access.\(^2\)

We define EMAs as encrypted communication technologies that have become crucial infrastructures and often congregate communities of trust. While other platforms, like Instagram or Twitter, introduced encrypted features such as encrypted DMs (which were more or less successful),\(^3\) encryption — and hence perceived intimacy — is central to the identity of EMAs. Encryption stands as a double-edged sword, protecting important pillars of democratic activity, but also facilitating the spread of disinformation. We conclude that while EMAs can include large-scale public channels similar to Facebook or Twitter newsfeeds, their focus on one-on-one and group chats, less advertising and algorithmic intrusion,\(^4\) as well as encryption differentiate EMAs from other social media.\(^5\)

People are moving their online communications to these messaging apps at rapid rates — 87% of the world’s internet users communicate via a messaging app at least once a month, making instant messaging the second most popular online activity behind social media.\(^6\)

In addition to instant messaging, EMAs are increasingly used for community gathering, news sharing, and entertainment.\(^7\) Accordingly, marketers and media companies have been turning to EMAs to disseminate news and engage with consumers.\(^8\)

To fully understand the role these apps play in viral disinformation efforts, it’s important to have a grasp on the features of EMAs and how they allow for the amplification of false and misleading information. This paper serves as a descriptive guide to six popular EMAs and their unique technical features: **LINE, Signal, Telegram, Viber, WeChat, and WhatsApp**.
THE IMPORTANCE OF UNDERSTANDING EMAs

Political Relevance

Along with their global popularity, the siloed nature of EMAs makes them powerful tools for online political manipulation since misleading information can spread on them in a largely unchecked manner.9 Their encrypted nature renders futile popular methods of debunking false information by independent fact-checkers or social media platform content moderation regimes. Additionally, existing research by the Center for Media Engagement’s Propaganda Research Lab has shown that these private platforms are often more trusted, especially in the U.S. where minority communities, such as Asian Americans, rely on them as a means of communication.10 This trust can be exploited if political disinformation actors use EMAs to spread false and misleading content.

In other countries like Brazil11 or India,12 EMAs such as Telegram and WhatsApp have arguably become the main avenues for political disinformation — leaving behind Facebook or Twitter.13 And since the Russian invasion of Ukraine in the spring of 2022, the relevance of encrypted messaging apps for use in propaganda and online political manipulation has accelerated.14

Why Research is Hard(er) but Necessary

Measuring the impact and scale of false and misleading information on EMAs is a challenge. The private nature of their design means that EMA data and content is difficult for researchers to obtain. This, in turn, means that research utilizing quantitative methods or other computational data collection methods that focus on the content of messages are difficult to employ for private chats on EMAs.15 First, access to data from private groups requires user permission; second, ethical questions accompany research into these private spaces, especially if researchers are seen as disrupting safe havens for EMA users — such as those in minority communities.16 Therefore, qualitative, interview-based research is an invaluable part of conducting research on communication via EMAs both practically and ethically.
EMA USAGE AND FUNCTION

EMAs by the Numbers

EMAs have exploded in popularity across the globe as internet users turn to private digital spaces for their daily communications. WhatsApp is the most popular chat app globally with over 2 billion users. WeChat boasts over 1.3 billion monthly active users worldwide. Telegram, Signal, and Viber have also experienced a recent burst in downloads. Given these numbers, it’s no surprise that EMAs have become a focus among malevolent actors looking to manipulate public opinion.
Migration to Private Spaces

Users are increasingly moving their online communications from public social media networks to more private online spaces. Data shows that 87% of the world’s internet users utilize EMAs at least once per month, which represents a 60% increase in use from 2014. In 2018, WhatsApp surpassed Facebook in number of monthly users and its growth has been steady since. Given this migration, Meta has focused their efforts on privacy-oriented social networking services. Developers are actively implementing new technical features on EMAs that foster group communications, such as the Communities feature on WhatsApp or the Moments feature on WeChat, where users can interact in a more intimate, tight-knit manner while establishing communities on these apps — not just one-on-one chats. Likened by researchers to a sort of ‘digital campfire,’ these digital spaces afford groups of users increased privacy and control over who is able to access their content.

Though private, EMAs still host widescale group communication through large channels and group chats that resemble Facebook and Twitter newsfeeds. Longstanding business models of social media platforms like Facebook and Twitter are rooted in ad-driven revenue, and while EMAs do not currently employ similar monetization infrastructures, some EMAs like Viber have already introduced in-app targeted ads. Given the evidence of user preference for private over public social networking and platforms’ shift in focus to private messaging, it is vital for policymakers, researchers, journalists, and users alike to consider the potential repercussions of changes in data usage by these platforms and in our future infrastructures.

What is End-to-End Encryption?

Encryption is a method in which information is encoded by taking the original message and altering it in some way to protect the information. To receive the original message, the encoded information sent needs to be decrypted, which is the process of undoing the initial encoding. End-to-end encryption (E2EE) is the encryption and decryption process that happens directly between the sender and the receiver. This differs from other forms of encryption because only the sender and receiver can view the unencrypted message. For instance, client-side encryption protects the sender’s content and server-side encryption encrypts messages at destination. The Transport-Layer Security (TLS) used by Discord, for example, provides basic encryption to messages in transit, but they are still accessible to the platform itself. If messages are not end-to-end encrypted, tech platforms can share encryption keys with law enforcement agencies like the FBI. For example, iMessage is E2EE, but iCloud backups are not by default.

There are two types of encryptions: symmetric encryption and asymmetric encryption. For symmetric encryption, there is only one key. A key is the piece of information used to encrypt
For asymmetric encryption, there are two keys: a public key and a private key. Asymmetric encryption requires having both keys to successfully send and receive the message.\textsuperscript{36} End-to-end encryption utilizes asymmetric encryption because it is less likely that the message will be read by an unauthorized party.

For end-to-end encryption to work, the receiver of the message, or point B, sends out a public key. A public key is used for the encryption of messages to be sent to B and can be seen by anyone. The sender of the message, or point A, will use the public key of B to encrypt their message to B. A will then send the message to B through one or several of the application’s servers. However, neither the server owners nor others besides B can decrypt A’s message. This is because they only have access to B’s public key, not B’s private key. A private key is only known by that user and exists only on the user’s device. The message eventually reaches B, where it is decrypted using B’s private key.\textsuperscript{37}

**OVERVIEW OF POPULAR EMAs**

<table>
<thead>
<tr>
<th>Features</th>
<th>LINE</th>
<th>Signal</th>
<th>Telegram</th>
<th>Viber</th>
<th>WeChat</th>
<th>WhatsApp</th>
</tr>
</thead>
<tbody>
<tr>
<td>End-to-end Encryption</td>
<td>✔</td>
<td>✔</td>
<td>[✔]</td>
<td>✔</td>
<td>[✔]</td>
<td>✔</td>
</tr>
<tr>
<td>Video &amp; Audio Calls</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Disappearing Messages</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Lifestyle Features</td>
<td>✔</td>
<td></td>
<td></td>
<td></td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Group Chat Size</td>
<td>500</td>
<td>1,000</td>
<td>200 (group chats)</td>
<td>200,000 (supergroups)</td>
<td>250</td>
<td>500</td>
</tr>
</tbody>
</table>
To help people better understand discussions around EMAs, we provide a detailed description of six popular apps: LINE, Signal, Telegram, Viber, WeChat, and WhatsApp.

**LINE**

LINE is a popular messaging app that simultaneously functions as a one-stop-shop app and even markets itself as “the very infrastructure of your life.”

Owned by Z Holdings, LINE has several features beyond messaging built into the app, such as mobile payment systems, music streaming services, and access to news. With over 194 million monthly active users worldwide, LINE is particularly popular throughout Asia. As of 2022, Z Holdings states there are:

- 93 million monthly active users in Japan (~ 70% of the country’s population)
- 53 million active users in Thailand (~ 80% of the country’s population)
- 22 million monthly active users in Taiwan (~ 90% of the country’s population)

**Notable features:**

*Encryption:*

LINE offers end-to-end encryption through a feature called letter sealing that encrypts users’ messages, location information, and one-on-one video/audio calls. Every user has unique sets of encryption and decryption keys that are used to send and receive messages on the app and are stored on the individual device rather than the server. If a user’s account is compromised or hacked, messages would be inaccessible to the hacker, appearing as “letter sealed” without decryption keys.

*Group communication:*

- Group chats: LINE offers video/audio chats and group chats with a limit of 500 users.
- OpenChat: This feature on the messaging section of the app allows users to chat anonymously in chat rooms. According to LINE, “OpenChat aims to serve as a platform for communication beyond the scope of ‘place’ and ‘relationship’ in the community platform market where sharing live content is becoming increasingly important.” OpenChat allows users to set a different nickname and profile picture for every chat they join. Users can join chat rooms by invitation code or administrator approval. Administrators may also appoint up to 100 co-administrators to assist in the management of the groups. Chat rooms on OpenChat can support up to 5,000 users.

*Disappearing messages:*

LINE gives users the opportunity to send disappearing, or hidden, messages. Similar to the app Snapchat, content is only shown after the receiver taps on the message. Users can
specify the time limit for which the content is able to be accessed. Once this time limit has passed, the messages are deleted permanently and cannot be accessed again.44

**Lifestyle Features:**

Similar to WeChat, LINE has many features beyond messaging built into the app. These features range from job boards for job seekers, to streaming services, to fortune teller portals that connect users with readers. Some of the most popular features include:

- **LINE NEWS:** According to the platform, this is the most popular news content curation service in Asia.
- **LINE Doctor:** a telemedicine service that can book appointments, host video calls between doctors and patients, and submit payments.
- **LINE Pay:** an online payment system similar to Apple Pay.
- **LINE Music:** a music streaming service.
- **LINE CLOVA:** an artificial intelligence assistant similar to Siri or Alexa.
- **LINE Fortune:** a fortune telling portal that connects you with readers.

Learn more about the other features of LINE [here](#).

**Impact:**

The widespread popularity of LINE as a messaging app led to the platform’s evolution into a super multi-use service. This has resulted in an inevitable reliance on the app for communication and news. LINE generates revenue through the promotion and sale of their stickers and advertising functions — which has allowed for the emergence of fast-growing channels that promise freebies to entice members before using the channels to spread false information. For instance, channels on LINE in Southeast Asia reportedly attracted large followings by promising new stickers to followers. However, once they amassed a big enough following, account owners quickly changed the name and profile pictures of the channels to appear as health information groups that began spreading health misinformation.45 In particular, the app has faced a rampant health misinformation problem that includes profiles that promote scam vitamin supplements and misleading medical advice. LINE’s environment essentially allows for the consequence-free profitability of hoaxes in a way that the average person would fail to spot due to the incentivization of app features. As a result, in some of LINE’s high-user regions — Taiwan, Japan, and Thailand — there have been significant attempts at countering harm through the creation of fact-checking bots. In 2019, Japanese LINE users were able to interact with the tool “Corowa-kun” to get answers to their COVID-19 vaccine concerns. Data shows that vaccine hesitancy decreased in surveyed users after they engaged with the chat bot.46
Signal

Founded in 2014 by Moxie Marlinspike and WhatsApp’s former co-founder Brian Acton, Signal was created with a mission “to develop open-source privacy technology that protects free expression and enables secure global communication.”[^47] Signal offers one-to-one or group messaging, audio and visual phone calls, and supports the sharing of voice messages, photos, videos, GIFs, and files. The app has amassed 40 million users worldwide with the highest download rates in the U.S., the U.K., and Germany.[^48] It also sits among the top three messaging apps in India, Brazil, and Singapore.[^49]

**Notable features:**

*Encryption:*

The platform is end-to-end encrypted utilizing the Signal Protocol. The Signal Protocol creates three types of keys per user: a long-term identity key pair, a medium-term signed prekey pair, and ephemeral prekey pairs. Prekeys are generated on each device when the app is installed, and ephemeral keys are only used once.[^50] These keys are then put into a “key bundle” and registered. These bundles are used to create a secure connection that allows users to begin communicating.[^51]

*Group chats:*

Signal’s private group system enables group communication while also keeping user privacy at its core.[^52] According to Signal, they keep no record of users’ group memberships, group titles, group photos, or any other group attributes. Group chats on Signal can support up to 1,000 users. Admins can control who can send messages and start calls in groups, remove users from the group, edit group information and disappearing message timer settings, and control if members need approval to join the group.[^53] Users can be invited to the group via a group link or a QR code.

*Disappearing messages:*

Signal gives users the option to send disappearing messages.[^54] Similar to Snapchat and other EMAs with this feature, users can opt for messages to be deleted from devices after the allotted time has passed.

*Blocked screenshots:*

Signal introduced a unique privacy feature that allows users to lock their screens and prohibit screenshots from being taken.[^55] If a user’s phone is stolen or compromised, this feature can block the device from taking screenshots on Signal.

*Stories:*

Similar to the story features embedded in social media platforms like Instagram, Facebook, and Snapchat, Signal offers users the ability to share photos on their accounts for 24 hours,
after which the photo will disappear. Signal allows users to customize their story settings — they can share their stories with all Signal connections or a custom list of selected users. Group chats also support stories in group chats, where users can share stories to their groups and anyone in that group can view and interact with them. Stories are protected by E2EE technology.

Proxies:
Proxy servers act as the “middleman” between the sender and the receiver, which can protect original IP addresses and allow use of the app in banned countries. Signal and several other EMAs such as Telegram and WhatsApp were blocked in Iran as a result of widespread anti-government protests in 2018. As a response, Signal worked with developers to establish proxy servers that allowed access to the platform amid extensive internet bans.

Learn more about other features of Signal [here](#).

Impact
Although Signal has been criticized for requiring users to register their accounts with their phone numbers, it is generally considered one of the safest EMAs on the market. This makes the app popular among journalists and activists who use it to share sensitive information. Signal has been an important organizational tool for protesters around the world and was notably used as a secure mobilization tool by Black Lives Matter protesters in the U.S. in 2020 and by student activists in Myanmar, who used the app to organize against the military junta in 2021 and bypass sophisticated surveillance operations by the Tatmadaw. Among journalists, Signal is used to both access and disseminate information to the public. For instance, journalists in Ukraine have used Signal to disseminate information to citizens in Ukraine and Russia amid rampant Russian propaganda campaigns during the 2022 Russian-Ukraine conflicts.

Given this use and Signal’s founding mission, the platform is widely known for its strong stance on encryption. Recently, Signal (along with WhatsApp, Viber, and a multitude of other encrypted messaging platforms) have vehemently opposed the U.K.’s Online Safety Bill, asserting that the proposed legislation would comprise end-to-end encryption “while emboldening hostile governments who may seek to draft copy-cat laws.” The bill, which is supposed to protect children from harmful content online, is being heavily debated among tech platforms and policymakers as concerns about the use of private technologies by malevolent actors continues to grow. Signal claims that the bill in its current iteration would shatter user privacy entirely and “could also create a template that would certainly be copied by authoritarian governments.” WhatsApp and Signal have both publicly denied cooperation with the legislation, suggesting that they would exit the U.K. market entirely if the bill is passed.
**Telegram**

Russian tech entrepreneur Pavel Durov, “Russia’s Zuckerberg”, was subject to heavy state surveillance after refusing to provide authorities with user data from his Facebook-inspired social networking site VKontakte. This event inspired the creation of the cloud-based messaging platform Telegram in 2013 as a means for Durov to communicate under Russian state surveillance. The app was developed to provide an encrypted and secure channel for users to communicate without interference or surveillance. Since then, the platform’s user base has increased over 40% each year since 2013, with over 500 million active monthly users as of 2023. Telegram’s biggest market is India with over 70 million monthly active users. The app is the second most popular chat app in the country, behind WhatsApp. Russia and the U.S. are Telegram’s second- and third-largest markets. While they are not top markets for the app, Telegram is still the most popular messaging app in Iran and Uzbekistan.

**Notable features:**

*Encryption:*

Telegram supports two different types of encryptions. For groups, channels, and one-to-one chats, Telegram offers client-server encryption, specifically Advanced Encryption Standard (AES) 256 encryption which “uses a 256-bit key to convert your plain text or data into a cipher” to protect data. In other words, messages are only encrypted between the sender and Telegram servers by default. Users may opt-into E2EE using secret chats, which is described below.

*Secret Chat:*

Telegram provides the ability to create secret chats, where users can opt into end-to-end encryption. Secret chats also offer self-destruct timers for messages and photos, where content is unable to be viewed or recovered after a certain amount of time. Users can determine the duration of this timeframe — ranging anywhere from one second to one week after the initial delivery of the message. Secret chats also inhibit users from forwarding messages or content sent as secret chats.

*Group Communication:*

- Large group chats: Telegram supports both public and private group chats. Group chats can include up to 200 people and allow users to upgrade chats to a supergroup that can include up to 200,000 users. Users have the option to make their group chats public or private. Private group chats require invitations and public group chats are searchable on the app. Conversations in public group chats can be viewed and joined by anyone. Administrators can be appointed to manage group chats and have advanced controls such as the ability to “mass-delete messages, control membership, and pin important messages.”
Channels: Telegram channels are a useful way to disseminate messages to large audiences and can support an unlimited number of subscribers. Telegram offers both public and private channels. Public channels are searchable, have a username, and are open for anyone to join. Private channels are closed and require an invitation from the owner of the channel to join. The owner, or administrator, of the channel can broadcast or delete messages and add the first 200 subscribers to the channel. After that, administrators can share invite links publicly, such as on social media sites, to attract subscribers. These admins can appoint more admins to help with the regulation of the channel and are able to curate individual administrator rights for each admin appointed. When a message is posted in a channel, it is attributed to the channel’s name rather than the individual poster. However, group administrators can develop a feedback loop by adding a discussion group chat, where users can engage in conversation similar to a discussion board. Given these features, channels are useful for those looking to disseminate information to large numbers of people. For instance, channels have been used by news outlets and politicians in Ukraine to share information with the public amid the Russian-Ukrainian conflict. Politicians worldwide, such as Brazil’s former President Bolsonaro who has over 1 million subscribers, have also utilized this feature to disseminate information.

Bots:
Serving as small applications within Telegram, bots can be used to add customizable features to the app. Users can create bots within chats to perform various tasks such as hosting websites, converting files, receiving payments, and even reporting the daily weather. Users may interact directly with these bots, as well as add them to groups and channels to implement these features. According to Telegram’s website, the app’s bot platform hosts over 10 million free bots created by third-party developers. Bots are also supported in other chat apps like WhatsApp.

Proxies:
Telegram offers proxy servers as an “anti-censorship tool.” EMAs like Telegram were used by citizens and protesters in Iran to access uncensored news but were banned in 2018 amid widespread political unrest. Proxies on Telegram have allowed for users in areas with internet bans, such as Iran where 45 million people are still using the app despite its ban, to bypass the restrictions.

Learn more about other features of Telegram here.
Impact:

Given the circumstances that inspired Telegram’s development, the platform is known for its strong dedication to encryption and user privacy. The platform also has a hands-off approach to content moderation, asserting that “censorship often makes it harder to fight [conspiracy theories].” Telegram’s vocal dedication to anti-censorship approaches to platform governance has earned them profound popularity with many in the U.S. who oppose online content moderation efforts. Given that the platform has a lax approach to content moderation and hosts features such as private and public channels that blend private messaging and social media, Telegram has been known to attract bad actors. Cybercriminals and extremist groups such as the Proud Boys and ISIS have utilized the app to spread information and mobilize in private.

Although Telegram’s security capabilities have been criticized by security experts due to the fact that only secret chats are encrypted by default, the app continues to be a top choice among users looking for privacy. The platform has played an important role in activism and news sharing during political unrest and government surveillance in Belarus, China, Iran and other countries. Particularly popular in Russia and Ukraine, the platform recently received increased attention due to its integral role in Russia-Ukraine conflicts. Telegram served as a valuable source for Russian and Ukrainian citizens and activists seeking to access independent information after the Russian government shut down the few remaining independent news channels. However, Russian propagandists caught on to the public’s reliance on EMAs and began using Telegram as a vehicle to spread propaganda and disinformation. They have evolved their online strategies to this shift to EMAs by establishing Russian state-sponsored channels that blast propaganda and disinformation, which they frame as “leaked information” to appear trustworthy.

Viber

Purchased by Japanese tech conglomerate Rakuten in 2014, Viber is a cross-platform voice over IP (VoIP) and messaging app which supports instant messaging capabilities as well as video and audio communication between users. The app uses E2EE to protect users’ communications but requires users to register using a phone number, which is visible when a user joins a group on Viber. According to 2021 data, Viber has around 250 million active monthly users. Viber’s largest market is in Eastern Europe where it holds 90% of the market share of EMAs. Its largest user base is in Ukraine, which accounts for over 24% of the app’s traffic, followed by Russia, which accounts for almost 20% of the app’s traffic. Viber is also growing in popularity in Myanmar and Iraq, where 40-50% of the population are users.
However, unlike some other EMAs, Viber collects personalized data to be used to place in-app ads, which account for approximately 20% of the platform’s revenue.\textsuperscript{104} According to the company’s CEO Djamel Agaoua, Viber discloses IP-based location, gender, and age data on users to inform targeted ads. Alternatively, users have the option to prohibit the platform from using gender and age information. In those cases, non-targeted ads are shown to those users.\textsuperscript{105}

**Notable features:**

*Encryption:*  
Viber protects all messages (both one-on-one and group chats) and private voice calls with E2EE by default.\textsuperscript{106}

*Group Communication:*  
Viber supports group communications through several different features:

- **Group Chats:** For audio or video calls, Viber can support up to 60 users. Group chats can have up to 250 members.

- **Public Accounts:** In 2016, Viber introduced Public Accounts to connect brands with their target audiences for marketing and customer service needs without needing either party to have the other as a contact.\textsuperscript{107} Public Accounts are conducive to cross-channel functionality, allowing businesses to promote the account to customers both inside and outside the app. Public Accounts also facilitate broadcasting opportunities, where businesses can push personalized content to customers, and host digital payments.\textsuperscript{108} The Huffington Post, Yandez, and The Weather Channel were among the first organizations to debut Public Accounts upon launching.\textsuperscript{109}

- **Communities:** Introduced in February 2018, Communities are group chats that provide more admin control and support unlimited members (compared to the traditional group chat feature which can only support 250 members).\textsuperscript{110} Unlike the group chat feature, Communities protect user phone numbers from administrators and other members.\textsuperscript{111} Viber also supports Community insights that detail the page’s statistics including members’ location and age, how the page is growing, and what content gets the most engagement.\textsuperscript{112} Communities are not protected by E2EE.

- **Channels:** Channels differ from communities in that they are designed to provide one-to-many communication. In other words, only admins can post in the channel. This feature is often utilized by politicians, governments, and public figures around the globe to blast information widely. Notably, Viber channels were used by the President Duterte regime of the Philippines to spread political propaganda to millions across the country.\textsuperscript{113}
• Broadcast lists: This feature is only available on mobile devices. It allows any user to send the same message to several other users without creating a group chat or notifying other users that they were part of a broadcast message. Broadcast messages can be sent to up to 50 users at a time.\textsuperscript{114}

\textit{Viber Out:}

Viber gives users the option to buy a subscription to Viber Out, which allows the user to call any landline or mobile phone number worldwide.\textsuperscript{115}

\textit{Device synchronization:}

Viber chats automatically sync across all devices for a given account. This allows the user to be up to date in all chats on all devices.

\textit{Disappearing messages:}

Viber supports the option to send disappearing messages. Similar to other EMAs like WhatsApp and Telegram, this feature is optional and allows for additional privacy. Disappearing messages may also be set as the default for all one-on-one chats. Differing from WhatsApp, messages will stay visible for 10 seconds, 1 minute, 1 hour, or 1 day depending on the sender’s settings and beginning when the receiver first opens the message. Disappearing messages are supported in one-on-one and group chats.\textsuperscript{116}

\textit{Hidden chats:}

For more privacy than disappearing messages, Viber allows users to hide chats altogether with hidden chats. Hidden chats keep certain chats out of a user’s regular chat list and require a pin to gain access. Face ID and Touch ID are also supported for iPhone users. When a pin is reset, all hidden chat histories are cleared. Hiding a chat on one device does not hide that chat on other users’ devices.

\textit{Proxies:}

Though Viber does not appear to directly endorse proxies, proxy connections are available for this application for users in areas with internet restrictions or bans.\textsuperscript{117}

Learn more about other features of Viber \texthref{https://www.viber.com/en/features}{here}.

\textbf{Impact:}

Viber has been vital for communication between government entities and the public worldwide. The most popular chat app in Ukraine, Viber was used by the Ukrainian Ministry of Health to communicate with citizens about COVID-19.\textsuperscript{118} Our previous \texthref{https://www.nisc.umd.edu/research}{research} details how apps like Viber and Telegram serve as an important infrastructure for journalists and politicians who have used EMAs to disseminate information to massive audiences.\textsuperscript{119}
Our research has also shown that governments and politicians have utilized Viber to spread political disinformation and propaganda to their citizens. For instance, Viber was used by the Filipino government as a main channel for distributing news and information to the public during President Duterte’s term. Our interviews with journalists, fact-checkers, and government employees revealed that apart from disseminating official announcements, the government often included political propaganda in messages to nationwide groups on Viber, which included over two million users across the Philippines. Following Russia’s invasion of Ukraine, Viber has also become an important tool for political communication in Eastern Europe, where pro-Russian propaganda is leaking into large groups chats throughout Ukraine. The affordances of privacy and separation from official fact-checking initiatives has made Viber, and other EMAs like Telegram, a powerful digital propaganda tool for Russia’s effort to control online narratives surrounding the ongoing Russia-Ukraine conflict.

**WeChat**

Owned by the Tencent Group, WeChat is a free app that offers texting and calling capabilities as well as an array of lifestyle features that make it a full-service app. The most popular app in China, the platform functions as both a messaging service and a social media site. WeChat requires accounts to be linked to a unique phone number. Features allow users to communicate in private or public groups, as well as establish their own profiles on the “Moments” feature that functions similarly to a Facebook page. Companies, businesses, and government organizations also utilize a feature called Official Accounts on WeChat to amplify content to wide audiences. Mini Programs on the app also supports a variety of lifestyle features, ranging from rideshare services to mobile payment services. Similar to LINE, WeChat’s popularity in China can be directly linked to many of the features it offers through these Mini Programs, which can essentially be described as apps within the app. WeChat is most popular in China, but also holds particular importance to the Chinese diaspora living worldwide. According to data from 2022, the app has over 1.3 billion monthly active users worldwide.

**Notable features:**

*Encryption:*

Differing from other encrypted messaging apps, WeChat does not offer end-to-end encryption, only client-server encryption (specifically, AES 256 which is also used for Telegram).
**Group communication:**

Group communication on WeChat includes: group chats with a limit of 500 people, video chats with a limit of 8 people. WeChat also hosts private group chats that require a digital code to join.\(^{124}\)

**Moments:**

WeChat’s Moments feature functions similar to a Facebook page where users can share pictures, videos, links, and text updates with their friends. Users are given the ability to control who sees their posts on this feature.\(^{125}\)

**Official Accounts (OAs):**

Official accounts are public WeChat profiles that allow users to publish information publicly. This feature is similar to Facebook pages, where profiles and posts are public and can attract followers to particular pages. Owners of OAs can send followers push notifications and can support integration of ecommerce functions, making them a popular digital tool for businesses.\(^{126}\) These accounts require verification and payment by account owners. Media outlets and bloggers also utilize OAs to push content to audiences widely. OAs play an important role in news sharing, given that WeChat is the primary outlet by which Chinese diaspora communities worldwide receive news.\(^{127}\)

**Mini Programs:**

Released in 2017, Mini Programs have expanded the platform from a private messaging service to a one-stop-shop application. Mini Programs can be conceptualized as sub-apps within the larger app that provide a variety of different features such as mobile payments, ecommerce and shopping, ridesharing, and much more.

Learn more about other features of WeChat [here](#).

**Impact:**

WeChat has been heavily criticized for its state-sponsored censorship of information on the app. Research from Human Rights Watch found that content from media outlets must be approved by Chinese censors before it is allowed to be published on the app.\(^{128}\) WeChat is the primary source of news for many community members of the Chinese diaspora.\(^{129}\) This is alarming given they are likely receiving information influenced by the Chinese government.

Chinese influence operations deployed on WeChat in recent years have negatively impacted elections and political engagement by the Chinese diaspora community worldwide. For instance, there is evidence of coordinated manipulation efforts on WeChat that attempted to influence voting behaviors among Chinese diaspora communities living in Canada during the 2021 parliamentary election.\(^{130}\) Far-right political disinformation
has also permeated Chinese diaspora communities across the U.S. on WeChat in recent years. Ahead of the midterm elections in 2022, harmful content promoting false narratives about election fraud, social justice issues, community safety, and abortion spread widely throughout WeChat groups across the country.131

Our previous research also revealed that information shared in these chats often engages in fear-mongering tactics tied to a specific community value or concern, making them more manipulative. During the Black Lives Matter protests in response to the killing of George Floyd, biased and misleading articles regarding alleged violence committed by Black people against Asian people went viral in Chinese American parent WeChat groups.132 As a result, young Chinese Americans reported their parents becoming increasingly wary of the Black community, warning them to not interact with them or attend Black Lives Matter protests.

**WhatsApp**

As the world’s leading EMA, WhatsApp boasts over 2 billion users.133 In 2018, WhatsApp surpassed Facebook in number of monthly users134 and still remains the world’s most popular messaging app in 2023. The app is owned by Meta, which also owns popular platforms such as Facebook and Instagram. While it is the most popular messaging app in over 100 countries, WhatsApp has particular popularity in Brazil, India, Italy, and Argentina with penetration rates of 98.9%, 97.1%, 97%, and 96% respectively.135 India is the platform’s largest market with over 487 million users in 2023.136 Local and international messaging and video and voice calls are free and compatible across Android and iOS devices, making international communication easy and affordable. Users can also send GIFs, stickers, photos, and videos. A desktop version of the app also allows users to access messages on their computers and is popular among many users — similar access options are available for other EMAs. However, in previous research by our Lab, interviewees emphasized the importance of the WhatsApp desktop option specifically.

**Notable Features:**

*Encryption:*

WhatsApp offers end-to-end encryption (E2EE) on all messages and calls and ensures its users that no third party (even WhatsApp themselves), can read messages between users. Specifically, WhatsApp uses the Signal Protocol, which is also used by Signal. See the Signal encryption section for more detailed information.

*Metadata:*

Despite using E2EE for all messages and calls, WhatsApp’s current policy on metadata, or information about the actual data that was sent, remains vague. What is clear is that user metadata is not protected, meaning that Meta may use this information.137
Group Communication:

- **Group chats:** Group chats allow for joined communication between multiple app users at a time. Messages sent in the group chat will be received by every user of the group in a communal chat space. Group chat limits have increased significantly over recent years, rising from 256 to 515 users in May 2022 and doubling again in October of 2022 to 1,024 users — the current limit as of May 2023.\(^{138}\)

- **WhatsApp communities:** Released as a new feature in 2022, WhatsApp communities provide users with a space to “organize and bring related groups together under one umbrella”.\(^{139}\) WhatsApp communities differ from traditional group chats in that these communities can combine various groups and their sub-group members. WhatsApp communities are made up of admins and team members, where admins have the authority to create and manage communications in the community by: (1) sending messages to the announcement group that are received by all members of all sub-groups, (2) promoting or removing other community members as admins, (3) deciding which groups join communities by creating new groups, adding existing groups, or removing groups, and (4) deactivating the community. Some have likened WhatsApp communities to communications platforms like Slack or Teams that are popular among larger organizations. Communities can accommodate up to 50 groups in addition to the announcement group, which can house up to 5,000 members. In addition to announcement groups, admins and team members can communicate in focused chats on different topics and switch between these groups at their convenience. WhatsApp markets this feature as a way for “communities like neighborhoods, parents at a school, and workplaces”\(^{140}\) to connect and organize group communications. WhatsApp’s E2EE also extends to WhatsApp communities, where personal messages and calls in communities remain private.\(^{141}\)

- **Broadcast lists:** Broadcast lists on WhatsApp allow for users to message several contacts at once through saved lists of recipients. When users send a message in a broadcast list, a message will be delivered to all users on the list who have that phone number saved to their contacts list. These lists differ from group chats in that recipient replies to a list message will not be sent to other recipients on the list. In other words, the feature functions similar to BCC on email.\(^{142}\) However, each broadcast list is limited to 256 members.\(^{143}\) Broadcasts lists make it easy for users to send the same message to multiple people at a time. The feature is often used by journalists, influencers, entrepreneurs, and activists to distribute news and information easily.\(^{144}\)
Forwarding/Receiving:
WhatsApp’s forwarding feature allows users to copy and paste messages and content between groups and to forward a message to up to five chats at once. Using metadata (which is not encrypted), WhatsApp established forwarding limits in an effort to control the spread of false information.

Forwarding flags, which label messages that have been forwarded, were released in 2018. In 2019, the feature was expanded to include forwarding limits that prohibit users from forwarding a message more than five times.

Disappearing messages:
Disappearing messages is an optional feature that can be enabled for additional privacy. Similar to Snapchat, users can select for messages to disappear after 24 hours, 7 days, or 90 days. Since November 2020, users also have the ability to send all or just some messages as disappearing chats. WhatsApp cautions users to only use this feature with trusted individuals. They warn of the possibility that others can still forward, take screenshots, or copy and save the content of disappearing messages before they vanish.

Status:
This feature functions similarly to the story features on Instagram and Facebook. Status allows users to post text, photo, video, and GIF updates that disappear after 24 hours. To share these statuses with contacts, both users must have each other’s phone numbers saved in their contacts. Users can also individually reply to their friends’ statuses.

Bots:
Similar to Telegram, WhatsApp supports a multitude of bots that cater to a variety of purposes for WhatsApp users.

Learn more about other features of WhatsApp here.

Impact
Because WhatsApp is the most popular chat app in the world, it plays an important role in information sharing between individuals, family and friends, and communities worldwide. WhatsApp’s role can be understood through scholars’ reference to the platform as a technology that has come to “mediate almost all aspects of life.” WhatsApp is a popular avenue of communication for many diaspora communities globally, who use the app to communicate with their networks across the world due to WhatsApp’s affordances of WIFI-enabled messaging/calling and the popular group chat feature.

Issues of viral and incessant mis- and disinformation have put WhatsApp at the center of many recent discussions regarding the impact of false information online. Rumors posted on WhatsApp have led to political unrest and the spread of election misinformation,
accounts of offline violence, and the spread of harmful health information in multiple countries. Meta has been repeatedly criticized by politicians, tech experts, and public figures for their seemingly apathetic response to false information on their platforms. In the past, WhatsApp's efforts to curb misinformation were focused on forwarding limits which limited users' ability to mass forward content. Amid concerns of Meta's part in the spread of Russian propaganda and disinformation, Nick Clegg, Meta's president of global affairs, spoke about the platform's decision to crack down on Russian propaganda. However, if curbing false information on the platform involves breaking encryption, WhatsApp refuses to take part. Together with others (such as Signal), WhatsApp has been clear on their opposition to the U.K.'s Online Safety Bill and their refusal to alter the platform's encryption model.

ACKNOWLEDGMENTS

Our understandings of EMAs and their political importance have been informed by conversations with team members as well as collaborators, including but not limited to: Wafa Ben-Hassine, Anamitra Deb, Jacob Gursky, Anastasia Goodwin, Justin Hendrix, Katie Joseff, Markus Kumleben, Zelly Martin, Azza El Masri, Kayo Mimizuka, Joao Vicente Seno Ozawa, and Martin Riedl. This paper is a project of the Center for Media Engagement (CME) at The University of Texas at Austin and is supported by the John S. and James L. Knight Foundation, Omidyar Network, Open Society Foundations, and The Miami Foundation. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding bodies.
FURTHER READINGS

Provided below are a variety of writings on the use of EMAs in political mis-and disinformation globally. The list is not exhaustive but shares additional research that may provide further context for the issues discussed in this report. Readings are separated by region and appear in alphabetical order therein.

Africa

Asia


**Europe**


North America


South America


REFERENCES


Du Rove’s Channel. (n.d.). Telegram. [https://t.me/durov/163](https://t.me/durov/163)


ENCRYPTED MESSAGING APPLICATIONS AND POLITICAL MESSAGING: HOW THEY WORK AND WHY UNDERSTANDING THEM IS IMPORTANT FOR COMBATING GLOBAL DISINFORMATION


LINE OPENCHAT. (n.d.). Creative.line.me. Retrieved April 7, 2023, from [https://creative.line.me/guide/in-app-brand/75#:~:text=LINE%20OpenChat%20is%20a%20community](https://creative.line.me/guide/in-app-brand/75#:~:text=LINE%20OpenChat%20is%20a%20community)


Lomas, N. (2023, March 6). *WhatsApp agrees to clean up its user messaging in the EU | TechCrunch*. [https://techcrunch.com/2023/03/06/whatsapp-tos-commitments-eu/](https://techcrunch.com/2023/03/06/whatsapp-tos-commitments-eu/)


Ministry Of Health of Ukraine [@MoH_Ukraine]. (2020, March 21). *The MOH has officially started working with Rakuten Viber. The MOH is expanding the communication platforms and creating an official @Viber-community ‘Coronavirus Info’, where it will publish up-to-date and reliable information regarding the spread of coronavirus in the country*. [Tweet; thumbnail link to article]. Twitter. [https://twitter.com/MoH_Ukraine/status/1241326400835117058](https://twitter.com/MoH_Ukraine/status/1241326400835117058)


Nast, C. (2021, April 14). Covid lies are tearing through India’s family WhatsApp groups. Wired UK. https://www.wired.co.uk/article/india-covid-conspiracies-whatsapp


Stelter, B., & Golodryga, B. (2022, March 3). *Journalists from Russia’s last independent news network are fleeing the country.* CNN. [https://edition.cnn.com/2022/03/02/media/journalism-crackdown-russia/index.html](https://edition.cnn.com/2022/03/02/media/journalism-crackdown-russia/index.html)


What is End-to-End Encryption (E2EE) and How Does it Work? (n.d.). *SearchSecurity.* https://www.techtarget.com/searchsecurity/definition/end-to-end-encryption-E2EE


ENCRYPTED MESSAGING APPLICATIONS AND POLITICAL MESSAGING: HOW THEY WORK AND WHY UNDERSTANDING THEM IS IMPORTANT FOR COMBATING GLOBAL DISINFORMATION

ENDNOTES


5 While ads are part of some EMAs, EMAs are not business models run mainly on ad revenue like other social media platforms.


ENCRYPTED MESSAGING APPLICATIONS AND POLITICAL MESSAGING: HOW THEY WORK AND WHY UNDERSTANDING THEM IS IMPORTANT FOR COMBATING GLOBAL DISINFORMATION


ENCRYPTED MESSAGING APPLICATIONS AND POLITICAL MESSAGING: HOW THEY WORK AND WHY UNDERSTANDING THEM IS IMPORTANT FOR COMBATING GLOBAL DISINFORMATION


42 LINE OPENCHAT. (2023). Creative.line.me. https://www.adchina.io/wechat-moments-ads/#:~:text=WeChat%20Moments%20are%20status%20updates


85 *Du Rove’s Channel.* (2021, July 9). Telegram. [https://t.me/durov/163](https://t.me/durov/163)


95 Stelter, B., & Golodryga, B. (2022, March 3). *Journalists from Russia’s last independent news network are fleeing the country*. CNN. https://edition.cnn.com/2022/03/02/media/journalism-crackdown-russia/index.html


ENCRYPTED MESSAGING APPLICATIONS AND POLITICAL MESSAGING: HOW THEY WORK AND WHY UNDERSTANDING THEM IS IMPORTANT FOR COMBATING GLOBAL DISINFORMATION


118 Ministry Of Health of Ukraine [@MoH_Ukraine]. (2020, March 21). The MOH has officially started working with Rakuten Viber. The MOH is expanding the communication platforms and creating an official @Viber-community “Coronavirus Info”, where it will publish up-to-date and reliable information regarding the spread of coronavirus in the country. [Tweet; thumbnail link to article]. Twitter. https://twitter.com/MoH_Ukraine/status/1241326400835117058


122 Kraus, R. (2022, March 2). In the Russia-Ukraine information war, encrypted messaging apps provide opportunity and risk. Mashable. https://mashable.com/article/whatsapp-telegram-russia-ukraine-disinformation


156 Nast, C. (2021, April 14). *Covid lies are tearing through India’s family WhatsApp groups*. Wired UK. https://www.wired.co.uk/article/india-covid-conspiracies-whatsapp


