ENCRYPTED PROPAGANDA: POLITICAL MANIPULATION VIA ENCRYPTED MESSAGING APPS IN THE UNITED STATES, INDIA, AND MEXICO

Jacob Gursky, Katlyn Glover, Katie Joseff, Martin J. Riedl, Jimena Pinzon, Romi Geller, and Samuel Woolley

ABSTRACT

Encrypted messaging applications (EMAs) such as Signal, Telegram, Viber, and WhatsApp have experienced a usership boom in recent years. This uptick in adoption, with WhatsApp growing its user base by over a billion from 2016 to 2020, has occurred for several reasons: EMAs are a free alternative to SMS texting, they offer secure communication, and they are an alternative to embattled ‘traditional’ social media platforms like Facebook, Twitter, and YouTube. But as EMA use skyrockets worldwide, political groups around the world are working to leverage them as tools for sowing propaganda and manipulating public opinion.

Over the last year, the Center for Media Engagement propaganda research team studied political manipulation on EMAs. Our analysis is focused on the production of influence operations in three countries: the U.S., India, and Mexico. We conducted 32 interviews with producers of EMA-based propaganda and experts on this phenomenon and combined insights from these interviews with an analysis of country-specific and global news coverage of EMAs, dis- and mis- information, and propaganda in order to identify trends in political usage of these apps.

SUGGESTED CITATION:

INTRODUCTION

In the midst of the chaotic bickering of the first U.S. Presidential debate on September 29, 2020, Donald Trump called out to the well-known white supremacist group the proud boys. The moderator had asked President Trump to condemn such hate groups, many of which have offered support for his presidency. His response was, “Proud boys, stand back and stand by.” This call-to-action has been rapidly adopted by the organization’s online adherents as a slogan of sorts. On Telegram, an increasingly popular space for communication and organization amongst U.S. extremist groups, the group has begun using Trump’s comment as both an endorsement and a rallying cry.

“STAND BACK AND STAND BY” on proud boys’ Telegram Channels

The proud boys used Telegram to proclaim a perceived ‘victory’ to staunch supporters, potential recruits, and internet users traveling down Presidential debate-fueled research rabbit holes. While often viewed as spaces used exclusively for private conversations, Telegram has an option for publicly accessible, large-scale, broadcast groups where one user can spread content to many others. In the case of extremist groups, these one-to-many messages offer a space where users that have been banned from other platforms can reach their networks. For such organizations, broadcasts can be used to funnel potential recruits into concentrically smaller and more hidden spaces, such as actual end-to-end (e2e) encrypted chats in Telegram. These public groups are accessible for researchers and others hoping to analyze communication on this particular portion of Telegram. In fact, anyone who looks up “proud boys” using Google after the first presidential debate could find and access their Telegram broadcasts.
In other circumstances, however, both extremist groups and mainstream political organizations use EMAs for their private communication capacity. For instance, these secure spaces can serve as useful incubators for designing disinformation campaigns intended to be amplified over publicly-accessible media—on Facebook, YouTube, and Reddit and amongst the broad ecosystem of media outlets—in networked propaganda efforts. Political actors around the globe are now using EMAs in attempts to rally their bases, recruit new members, broadcast party content, plan influence operations, share disinformation, and, ultimately, manipulate public opinion.

**OUR RESEARCH**

**The Production Side of Propaganda on EMAs**

To understand who designs, builds, and launches propaganda efforts on EMAs in the U.S., India, and Mexico, the Center for Media Engagement propaganda research team collected and analyzed instances in which EMAs were used to organize and/or disseminate coordinated influence operations. Through this process, we identified and cataloged 28 distinct cases of such EMA influence operations in India, 24 cases in Mexico, and 45 cases in the United States. We began our collection in fall 2019, but the cases themselves range from 2015 to 2020. Each country’s cases are divided by topic: elections, incitements of violence, and coronavirus-specific mis- and disinformation. Here we showcase some of these instances to illuminate country-specific strategies for the political use of EMAs and emerging international trends of a phenomenon we term encrypted propaganda.

Encrypted propaganda is a novel form of political manipulation that occurs over EMAs. It includes efforts to both sow disinformation and scale misinformation. Disinformation is defined as purposefully-spread false information, whereas misinformation is false information that is spread unintentionally or unknowingly. The term propaganda includes politically inclined versions of both, but also speaks to more general attempts by political groups to leverage communication tools in both veiled and overt efforts to affect peoples’ socio-political views and actions. Similarly, influence operations “describe efforts to influence a target audience, whether an individual leader, members of a decision-making group, military organizations and personnel, specific population subgroups, or mass publics.”

“Encrypted propaganda is a novel form of political manipulation that occurs over EMAs. It includes efforts to both sow disinformation and scale misinformation.”
Along with this case list, we have also conducted 32 interviews, primarily with people in each country who make and build propaganda campaigns on EMAs. We interviewed propagandists who work professionally or on a volunteer basis for political parties, governments, extremist groups, and other political entities. To enrich our understanding of their efforts—particularly in India and Mexico, where we have limited cultural and political understanding—we also spoke with journalists, researchers, marketing professionals, and digital political consultants.

We focused our attention on the U.S., India, and Mexico for several reasons. First, the U.S. and India are democracies that have shifted towards authoritarianism and populism in recent years. Mexico, meanwhile, is a democracy that has struggled with political corruption for decades. How might these countries’ political problems, and illiberal machinations be reflected in their political groups’ propagandistic use of EMAs? Each country is going through, or has recently gone through, a competitive, contentious election. Social media plays a significant, ever-growing role in political communication across all three. Finally, EMA usage is diverse, in terms of penetration or reach, in all three countries.

Take WhatsApp usage in each country: In the United States, 13% of internet users use the Facebook-owned EMA. In Mexico, approximately 76% of internet users use it. In India, there were over 400 million active users in 2019. Though this figure accounts for just 30 percent of the Indian population, it is larger than the total population of people living in either the U.S. or Mexico. India is, in fact, WhatsApp’s largest market.

**EMAs: Trust, Secrecy, and Disinformation**

Encrypted messaging applications are growing in popularity and amassing large active user bases. In India and Mexico, the popularity of EMAs (particularly WhatsApp) has increased in places where it is the most viable option for communication and developing an online presence. WhatsApp, in particular, provides incentives aimed at making adoption easy and feasible for new digital populations. Apps like WhatsApp and Telegram have become increasingly popular, although the convenience of the platform is often more important to adoption than an accurate understanding of the level of security provided. Nevertheless, content shared through EMAs is largely unmoderated by platforms, not to mention mostly private, making the tracking and correcting of disinformation and misinformation very difficult.

In the age of constant connectivity, propaganda—and the threat it poses to democracy—is amplified and accelerated. Discussions around the issue of “computational” or “network” propaganda have primarily revolved around platforms such as Facebook and Twitter, and broader “mainstream” media ecosystems. But EMAs have become increasingly important spaces in which propaganda thrives and spreads online. The central appeal of these
platforms, for both users and for those seeking to manipulate them, is the ability to create relationally close-knit information silos. These more secure digital spaces are populated by anywhere from two to several hundred people who have a broader shared identity (e.g., Brazilian Americans based in Austin, Texas). Encrypted spaces are uniquely vulnerable because they require the development of specialized strategies to counter disinformation without compromising the security of a given platform.

**Trends in Political Usage of EMAs Across the U.S., India, and Mexico**

Drawing on the case list and our interviews, there are several high-level trends in the ways in which encrypted messaging applications are impacting political discourse and decision-making in the U.S., India, and Mexico:

- There are feedback loops between networks on encrypted platforms and politicians’ content on mainstream platforms, such as Twitter.
  - In both the United States and India, the President and Prime Minister, respectively, have actively cultivated relationships with content creators and distributors who use EMAs to manipulate the mainstream media.
  - Offline violence tied to lies spread on EMAs has occurred.
  - In all three countries, violent and extremist individual organizations seek to use EMAs to stoke offline violence. In India and Mexico, there are particularly similar occurrences of rumors spread on EMAs leading to mob violence.

- In all three countries, we see increasingly complex tactics for organizing disinformation campaigns.
  - In the United States, alternative platforms are populated by radical groups that actively seek to get their message into the mainstream. Events like the White House Social Media Summit and the advent of “digital armies” in India seek to better capitalize on those relationships.
  - In India, there are explicit government-coordinated disinformation campaigns conducted by “IT Cells” across WhatsApp. It is public knowledge that these cells often mass-share scripted content that has been approved by the Bharatiya Janata Party’s digital head.
  - EMAs do not follow international boundaries and thus allow for harmful information to flow across borders. For example, cartels in Mexico are able to harass their victims even after they have left the country by using WhatsApp. In the U.S., communities seeking to communicate internationally often rely on EMAs, as opposed to traditional SMS text messaging, because
they allow for free and easy communication. Disinformation and radicalism have spread to the chats of these communities. International communities in Miami and Los Angeles have been particularly affected by this infiltration of harmful information.37

Country by Country Summary

United States

In the U.S., the creation of mis- and disinformation often happens in message boards like 4chan,38 alternative social media platforms like Gab,39 Mastodon,40 or Parler,41 and private groups in EMAs such as Discord42 and Telegram.43

- Alternative social media platforms, like Gab and Mastodon, are used by radical groups to spread hate speech that could potentially be regulated on mainstream social platforms.44 New trends indicate that radical groups are using video games, like Fortnite, to recruit members and further spread their ideology.45
- Disinformation pertaining to COVID-19 has spread anti-Asian sentiment, potentially dangerous fake “cures” for the virus, and conspiracy theories regarding the origin of the virus.46
- Disinformation is flourishing in EMAs used by several immigrant communities in the U.S., for instance in Latinx communities in Miami (on WhatsApp)47, or in Korean-American communities in Los Angeles (on KakaoTalk).48

As mentioned in our introduction, EMAs in the United States are often havens for actors who have been pushed off of Twitter, Facebook, YouTube, and Instagram onto platforms that are more secretive or specialized, such as Telegram, Gab, and Parler. They act as places for groups that have been banned from the mainstream to create large followings, communities, and broadcast messages in their own, unregulated, news feeds that can be accessed by anyone.49

Extremist Groups

As illustrated by the proud boys becoming part of the national conversation after the president name-dropped them in a debate, and their subsequent capitalization on the resulting media storm, the goal of groups on EMAs is often to manipulate the mainstream media. The idea is to take content from smaller spaces, like EMAs, and get it into the mainstream, as outlined in Claire Wardle’s “Trumpet of Amplification.” 50

One of our interviewees, a self-described former member of a “violent white power movement,” argued that the value of Telegram and Discord lies not only in secrecy, but also
in broadcast and outreach as a step toward mainstream media (the subject also named Riot. IM and Wire as common platforms). On Telegram, users have the option to make messages end-to-end encrypted, but on Discord, messages are only encrypted in transit. Thus, Discord is used to broadcast and bring interested parties into the encrypted fold. EMAs serve a multi-faceted purpose for followers of radical groups who have been kicked off other platforms—it would be a mistake to only define them by their ability to afford the possibility of secret chats.

The interviewee walked us through the details of how spaces like Discord and Telegram are used to spread messages into the mainstream, using the specific example of a fraudulent, opportunistic, and small white supremacist group who managed to convince the mainstream media of the lie that the Parkland shooter was a member of their organization. The specifics included a detailed chat log of their real-time media manipulation as they organized on Discord:

“It was taking advantage of a national tragedy. The way to do that is: (1) to get people to talk about it whether it is through 4chan, spreading it to other people and (2) being able to get that into the public eye... The overarching goal is to create enough chaos and discomfort that people will want to fight back, so they create distrust in the media and that is one of the largest goals. Disinformation campaigns are a way to do that.”

Of course, Telegram and Discord are not the only secretive information silos. Facebook, too, enables groups of a closed (one must request membership to see content, but the group is publicly searchable) and secret (groups that cannot be found by those who have not been invited) nature. While many groups are used to share legitimate information and encourage comradery, other groups have also been commonly used to spread hate speech and disinformation. Concerningly, Facebook has made it easier for people to be brought into these potential echo chambers with a recent integration of group posts into the newsfeeds of nonmembers. Fringe figures have created a presence on Facebook through these groups, where they have been able to create communities and spread disinformation that then finds its way onto mainstream newsfeeds.

Immigrant Communities in the U.S.

Although WhatsApp’s penetration in the U.S. isn’t as extensive as it is in India or Mexico, it is a popular form of communication in immigrant communities in the U.S. Deceptive claims started to spread through the Korean chat app KakaoTalk in Los Angeles and caused widespread fear and panic about infections of the coronavirus. Similarly, radicalism and
conspiracy theories emerged in Latinx chats in Miami that were originally designed for community engagement and connection.\textsuperscript{57} For example, an interviewee described to us that they witnessed how WhatsApp groups originally created to connect families displaced by the pandemic with food banks and other services slowly became inundated with politically-motivated conspiracy theories. A Miami community leader and administrator of about 10 of these WhatsApp groups also attested to the increase in mis- and disinformation. They said: “Sometimes, in a period of 5 hours you could have hundreds of postings... When we’re close to an election, I would say 20-30\% of them (users) tend to want to convert people or evangelize their political views.” At times, the messages promote harmful conspiracy theories like QAnon.\textsuperscript{58} After speaking with a member of Miami WhatsApp groups who also works as a political strategist, we were able to understand more deeply how serious these deceptive messages can be: “It hurts me that they would abuse my community this way.” This disinformation sometimes targets existing lines of tension across both the United States and the countries in which immigrant communities have their roots. At times, this targeted messaging is spread using WhatsApp-centric strategies fine-tuned in Latin America by politicians and strategists versed in manipulating messaging on the app: “There are a lot of Latino strategists in Miami that have done Latin American campaigns in Latin America who know how to use this because that’s what they use in Latin America and now they are infiltrating it here.”

EMAs are a vector for this sort of targeted disinformation across international lines. While the infiltration of WhatsApp groups is more difficult than public Facebook groups, our subject articulated that there are strategists and politicians with interests both in the U.S. and internationally that are adapting WhatsApp-centric strategies commonly used in Latin America within the U.S.

\textbf{India}

As internet access increases and the price of data decreases, over 400 million people in India have turned to WhatsApp, making it the app’s largest market.\textsuperscript{59} The app was widely used in digital political campaigns during the 2019 election, so much so that the election itself was referred to by journalists and academics as a “WhatsApp Election.”\textsuperscript{60} The disinformation environment on the app has become so apparent that the term “WhatsApp University” has been coined on social media as a satirical jab at WhatsApp as a place for learning, given the prevalence of propaganda and disinformation throughout the app’s chat channels.\textsuperscript{61}

In an effort to quell Covid-19-related mis- and disinformation, WhatsApp implemented several new regulations in early 2020: (1) Limiting the number of users in a group to 256; (2) limiting messaging forwarding to 5 users; (3) offering the ability to search the web for the content of messages straight from the app;\textsuperscript{62} and, (4) labeling messages with “frequently
forwarded flags” after they are shared a specific number of times. Nevertheless, the disinformation inside India’s WhatsApp channels has unfortunately resulted in widespread harm and manipulation in the form of rumors, election manipulation, and violence. Politically motivated mis- and disinformation spread on WhatsApp is routinely reported to fact-checkers in traditional and mainstream media, such as the Quint’s WebQoof initiative.

Through our research, we identified several trends in WhatsApp’s role within India’s disinformation environment:

- WhatsApp rumors of child traffickers, thieves, murderers, or other public threats spread throughout channels. Fear and false information have led to the formation of violent mobs who killed dozens of innocent people who were believed to be guilty.
- Capitalizing on WhatsApp’s powerful connectivity and the opportunity for public manipulation, the ruling party runs and maintains what they refer to as “IT cells” across India. These IT cells are made up of workers and volunteers who strategically spread false content through WhatsApp channels. Content is designed by workers and leaders of the IT cells to purposely mislead voters and sway public opinion to favor their candidate. These set-ups are hardly a secret in India. In fact, the country’s ruling Bharatiya Janata Party (BJP) is widely known to deploy this campaign tactic. Such measures were widely used in the 2019 “WhatsApp Elections.”
- Most of the false political content spread through WhatsApp in India seems to be in favor of Prime Minister Modi and the BJP. Most disinformation seems to have been created to portray his opponents in a negative light or to show Modi as a strong Hindu nationalist.
- Other political messages aim to ignite religious division throughout the country between Muslims and Hindus. Modi and his party identify with strong Hindu values and have been known to be associated with anti-Muslim biases.

**BJP use of WhatsApp**

With a large population in India using WhatsApp, political campaigns began to use WhatsApp as a tool to connect with voters, push their agendas, and spread disinformation. Operations were established to systematically collect data from voters and create and disseminate content to them via WhatsApp. In an interview with a former Indian electoral campaign consultant, we learned about the use of this data in creating messages. “All of these data sets that we compiled and all of these groups that we made of individuals are ultimately used to target people with messaging.” IT Cell workers and volunteers create thousands of WhatsApp groups with users compiled from these data sets and strategically push targeted content to them via WhatsApp chats. A senior member of the BJP’s IT operations told us that they work with “volunteers, graphic designers, a few who are good
“It works in our advantage... if you have people at every level, if you have people-to-people contact, then it doesn’t stop... It’s like you just pass the baton from one to each other...WhatsApp does not say you cannot forward the message to anyone. WhatsApp, in a way, they are just stopping the tools.”

Elaborate human-centered efforts, such as the BJP’s IT cells, are at the forefront of harnessing the power of encrypted propaganda, and political actors who have established networks have the advantage of staying one step ahead of regulations.

**Mexico**

Due to a high level of WhatsApp penetration, challenges with corruption, and a history of early adoption of innovative computational propaganda techniques, Mexico has had a significant share of encrypted propaganda. Here is a summary of insights from our top-level results:

- The 2018 presidential elections became a breeding ground for doctored memes, videos, and content meant to influence and intimidate voters across the political spectrum. 

- Amid the COVID-19 pandemic, false information claiming to have come from the government spread as chain messages or through group chats, often accompanied by misleading links, documents, or statements. The intent of the message varied but some pose a threat to public safety and national security.
Vulnerable moments, such as the 2017 earthquake, were used as amplifiers for false information to spread quickly about incoming quakes and people in need of aid.  

A prominent Mexican journalist described how WhatsApp interplays with other platforms to buoy and spread disinformation, tracking the case of the 2017 earthquakes described above:

“I looked at this specific case in depth...it started on WhatsApp with the help of a few fake sources on Facebook. The following day it shifted to Twitter, where the message was amplified by bots, and the third day it reached Mexico City and the media started to take note of the rumors... what blew the situation up was the media’s reaction, which helped verify the rumor.”

As in India and the United States, EMAs in Mexico are used for mass broadcast and sharing in ways that interplay with other media outlets to increase amplification and eventually make it into mainstream and legacy media. However, much like the human-run networks of the BJP in India and the trend towards human-run networks in the U.S., Mexico is seeing a shift from automated bot networks to more human-centric approaches. A Mexican political consultant and social media manager who specializes in leveraging human accounts on Instagram to generate false support for political clients told us: “WhatsApp works with different strategies [than Facebook and Instagram], like the planting of false information. You build a solid base of WhatsApp numbers and create a bot to plant the information in whatever geographic location you want. ... This has always happened, but it went from SMS to WhatsApp because it’s cheaper.”

The interviewee is one of many political actors in Mexico who consider their work to be, essentially, a form of social media marketing and an extension of the give and take between users and social media platforms. The same person further described their job as follows: “My main job focus is growth hacking, where I find new roads or new ways to reach a certain goal within social media by using different strategies and tools, a little bit of black sale and of maneuvering the terms and conditions of these different platforms ... to accelerate their algorithms and growth in general.” This person presented themselves as a social media marketer and goes as far as featuring the term “astroturfing” on their public LinkedIn profile. This is a demonstration of the diverse, cross-platform nature and shifting strategies of actors seeking to stay ahead of platform regulations—the anonymity and scale provided by an encrypted space like WhatsApp is only one strategy in a larger set of services provided.
CONCLUSION

A Diverse Propaganda Tool Mistakenly Defined by One Feature

As encrypted messaging applications (EMAs) such as WhatsApp and Telegram enjoy a large popularity among users worldwide, they are also venues prone to the dissemination of disinformation—a phenomenon we call encrypted propaganda. In this study, we showcased national and international trends in encrypted propaganda, with a particular emphasis on white nationalists in the United States, the political use of these apps in India, perhaps best illustrated by the Bharatiya Janata Party, as well as false information spreading on WhatsApp in Mexico, elevated by campaigners under the guise of social media marketing. While conversations about encrypted spaces often focus on the dangers that emanate from the lack of access for authorities, especially in the tracing of rumors that lead to acts of physical violence, EMAs are also powerful tools for strategists that utilize their human-powered networks to get their message across. Additionally, and counterintuitively, EMAs are appealing to groups seeking to publicly broadcast information, but who have been removed from mainstream social media platforms. Public channels on EMAs facilitate the recruitment of new members, who are then invited into encrypted channels within the same platform. Recognizing that the uses of EMAs are as variable as those who are using them is a first step towards designing and implementing meaningful strategies to curb the freely-flowing disinformation that has come to define them in recent years.

ACKNOWLEDGMENTS

Thank you to Joel Carter for his editorial help and Claire Coburn for her research assistance. This report was funded by Omidyar Network, Open Society Foundations, and the John S. and James L. Knight Foundation.
ENDNOTES

1 We define EMAs as digital communication platforms using both end-to-end and transport-layer encryption.


13 Case list available upon request at mediaengagement@austin.utexas.edu.


ENCRYPTED PROPAGANDA: POLITICAL MANIPULATION VIA ENCRYPTED MESSAGES APPS IN THE UNITED STATES, INDIA, AND MEXICO


26 Other than public group content on some EMAs and metadata on who is sending and receiving messages on e2e platforms. Transport layer encrypted apps, meanwhile, allow those who own the apps proprietary access to communication stored on their servers.


null


