


Chat Apps and Cascade Logic: A Multi-Platform Perspective on India, Mexico, and the United States

Social Media + Society
April-June 2022: 1–11
© The Author(s) 2022
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/20563051221094773
journals.sagepub.com/home/sms


Jacob Gursky, Martin J. Riedl , Katie Joseff,
and Samuel Woolley

Abstract

Chat apps such as WhatsApp, Telegram, and Signal are increasingly popular platforms for communication. Their sometimes-closed nature and encryption affordances present researchers, governments, and law enforcement with unique problems of access, traceability, and, ultimately, understanding. It also makes them useful vectors for sowing disinformation. This research assumes a multi-platform perspective, describing the particularities of how chat apps can be used toward disseminating mis- and disinformation by way of *cascade logic*—the means by which information in chat app ecologies is trafficked upstream (making its way from private conversations into the mainstream) as well as downstream (allowing information to withdraw from the public eye), providing space for distortion along the way. Cascade logic also describes how chat apps allow the gradual withdrawal and self-segregation of individuals into, or emergence out of, layered spaces of privacy and obfuscation. We present an interview-based study exploring chat apps in three countries, synthesizing unifying dimensions across cultures and contexts: India, the United States, and Mexico. We analyze data from in-depth conversations with 33 individuals who work to either produce or track political content on chat apps. These interviewees work for a wide array of organizations: political parties, governments, extremist groups, digital political consultancies, news entities, and civil society organizations. We reveal key insights into the tactics of producers of political content on chat apps and show how these platforms are particularly suitable for harnessing human connections, or leveraging communities of trust, to sow disinformation.

Keywords

chat apps, disinformation, United States, India, Mexico, cascade logic, social media

Introduction

Honestly, listen, I was invited here through Parler by the proud boys. I think we need to join groups like that and make a big . . . make a *movement* if it comes down to it, and . . . just take back our country, but we can't do it by ourselves. You know the constitution talks about militias . . . ([Username redacted], 10 January 2021)

The above statement was transcribed from a continuous, publicly accessible voice chat hosted on the chat app Telegram. The speaker, self-identified as a 50-year-old trucker living in Pennsylvania, explains how they found their way to Telegram. The venue where the chat was hosted, *Parler Lifeboat*, was a rebranded channel associated with the proud boys—a white supremacist hate group—and designed as an open space for people who were deplatformed following the shutdown of the social media platform Parler in the

wake of the 6 January 2021 insurrection at the US Capitol (DFRLab, 2021; Rogers, 2020). Telegram's recent growth has been linked to the banning of individuals on other social media platforms (Urman & Katz, 2020). The platform's ability to provide some forms of encryption, public and private channels, and its lax moderation have made it a popular platform not just for the proud boys (Tynes, 2021), but also for other groups seeking to perpetuate violence and disinformation such as ISIS (Shehabat et al., 2017) or Atomwaffen (Walther & McCoy, 2021).

The University of Texas at Austin, USA

Corresponding Author:

Martin J. Riedl, Center for Media Engagement, The University of Texas at Austin, 2504 B Whitis Avenue (A0730), Austin, TX 78712-1879, USA.
Email: martin.riedl@utexas.edu



The fallout from the attack on the Capitol illustrates a larger set of issues that accompany the communicative use of chat apps such as Telegram, WhatsApp, or Signal: their grasp on different aspects of social life (Cruz & Harindranath, 2020; Matassi et al., 2019), the difficulty (or impossibility) of moderating content on them (Semenzin & Bainotti, 2020; Urman & Katz, 2020), the privacy and immediacy they provide (Gil de Zúñiga et al., 2021), the broad reach they offer (Aneez et al., 2018; Perrin & Anderson, 2019), and the fact that many boast both private, encrypted chats and large-scale public channels similar to a Facebook or Twitter newsfeed (Rogers, 2020). These features make chat apps powerful communication tools and an important platform domain to explore for scholars concerned with disinformation and social media.

While research shows that chat apps can facilitate the spread of mis- and disinformation and broader political manipulation efforts (Rossini et al., 2021), it is also true that they fulfill crucial roles for political activism (Agur & Frisch, 2019; Treré, 2020), everyday political talk (Kligler-Vilenchik, 2021), and political campaigning (Banaji et al., 2020). Rather than focusing on one particular platform or locale, we discuss several chat apps across three countries—India, the United States, and Mexico—and work to contextualize them within a broader media ecology (Zuckerman, 2021) and hybrid media system (Chadwick, 2017).

We present the concept of *cascade logic* as central to chat apps: as information is trafficked upstream (making its way from private conversations into the mainstream) as well as downstream (allowing information to withdraw from the public eye), it can get distorted, decontextualized, and thereby, transport false information. Cascade logic also describes how chat apps allow the gradual withdrawal and self-segregation of individuals into, or emergence out of, layered spaces of privacy and obfuscation. This, in combination with chat apps being communication technologies that congregate communities of trust, makes fertile ground for mis- and disinformation to fester. We showcase the roles that various chat apps play in the dissemination of mis- and disinformation—within as well as across different platforms (Krafft & Donovan, 2020).

Literature Review

The Rise of Chat Apps

WhatsApp enjoys great popularity in many parts of the globe, such as India (Aneez et al., 2018), Israel (Kligler-Vilenchik, 2021), or Brazil (Banaji et al., 2020). While it is less widely used per capita in the United States, the Pew Research Center reports outsized importance of WhatsApp among US Hispanic people (42% use it), compared with Black people (24%) and white people (13%) (Perrin & Anderson, 2019). In India, more than 400 million people use WhatsApp (Hariharan, 2021), making it the most popular

chat app in the country. In Mexico, WhatsApp is the third most popular social media platform for news consumption (39% of Mexicans use it for this purpose) after Facebook and YouTube (Newman et al., 2020).

Chat apps have taken on broader infrastructural importance among digital platforms, mediating the contexts of work as well as social/private life. WhatsApp, for instance, has been described by researchers as a *technology of life* that is effectively impacting “a wide range of quotidian activities, from personal to economic, from spiritual to political” (Cruz & Harindranath, 2020, n.p.). In the Argentinian context, Matassi et al. (2019) hold that WhatsApp fulfills a central role in people’s lives, a “passage point for the management of friendship, family and work routines (. . .) [and] all-encompassing space of encounter, meaning-making, and coordination” (pp. 2194–2195). Baulch et al. (2020) point to the divergent set of motivations undergirding the use of chat apps such as WhatsApp—taken up by some for being readily available and cheap means of communication, whereas others gravitate toward them motivated by their encryption affordances.

Chat apps are focal points for political talk and assume an important role in the exchange of opinions, and the sharing of news (Kalogeropoulos, 2021). Rossini and colleagues (2021) find that discussions about politics on WhatsApp can correlate with the sharing of false information, but also that “those who actively participate in political discussions (. . .) are also more likely to share misinformation accidentally simply because they already tend to share news more frequently” (p. 15) on the platform. In the Israeli context, Kligler-Vilenchik (2021) establishes that although political conversations may unfold in a disruptive manner on WhatsApp, it is important to have those conversations anyway given that they “may be the only kind of political talk with the chance to change hearts and minds” (p. 131). Chat apps serve groups of friends and family members, as well as wider circles of trusted communities as technological accompaniments that afford permanently being connected.

Politics, Disinformation, and Encryption

Chat apps can also allow for the organization and coordination of social causes. Civic action that may be persecuted in authoritarian states if conducted in public can blossom within the (relative) privacy of chat apps (Johns, 2020). Backstage activities afforded by closed chat apps may help to form social cohesion and collective identity (Pang & Woo, 2020). The role of WhatsApp, in particular, allows different degrees of civic engagement and publicness—summarized as “front-line engagement, passive facilitation, and relational engagement” (Pang & Woo, 2020, n.p.).

Chat apps have attracted attention not only as intermediary spaces of collective action but also as incubators and crossroads for trafficking mis- and disinformation (Gursky et al., 2020; Treré, 2020). Disinformation is commonly

understood as intentionally spread false information, whereas misinformation is unwittingly shared false content (Jack, 2017). Chat apps allow for both types of information to circulate, and intention can change once content passes through groups, chats, and broadcast lists on chat apps. Focusing on cross-platform activities on chat apps in this vein is important. Krafft and Donovan (2020) have illuminated how disinformation hops between a variety of digital platforms. Marwick and Lewis (2017) have broadened the scope of disinformation research into alternative platforms, influencer networks, and other spaces that rely on trust and social capital more than the largest social media platforms. Considering such work, researchers have slowly but steadily expanded the scope of their endeavors toward tracking cross-platform effects of disinformation campaigns (Lukito, 2020).

One critical provision of many chat apps is encryption and the privacy that is afforded by them (Gil de Zúñiga et al., 2021). Different apps provide different forms and degrees of encryption. WhatsApp, for instance, uses end-to-end encryption (E2EE) as a default, a move enacted in 2016 interpreted by some as a decision to avoid political interference from state governments (Santos & Faure, 2018). On Telegram, only one-on-one communications in a so-called “Secret Chat” are end-to-end encrypted, while other forms of interaction remain encrypted, though less securely than E2EE (Marlinspike, 2021). E2EE means that information is secured between sender and recipient, and protected from the eyes of the companies themselves, as well as from states and other interested parties (Rogers, 2020). This is particularly important in light of the fact that Facebook’s CEO, Mark Zuckerberg, in 2019, declared that the company was planning on bringing E2EE to Facebook Messenger, in addition to the already end-to-end encrypted WhatsApp (Welch, 2019). Governments have developed interests in reviewing content on chat apps and advocate for law enforcement access to counter illegal activities (Veen & Boeke, 2020). In opposition, privacy experts state that such admittance could also be used to surveil activists and other groups (Encryption Working Group, 2019), and government-mandated backdoors put users at risk of security breaches from non-government actors (Veen & Boeke, 2020). Encryption stands as a double-edged sword, protecting important pillars of democratic activity (Johns, 2020), but it also shields abusive behavior (Semenzin & Bainotti, 2020) or the spread of disinformation (Banaji et al., 2020). And while chat apps are neither a force of evil nor of good, precisely how they operate and how people use them for various communication tasks are important domains of research.

Cascade Logic and Public–Private Dichotomies

Chat apps operate in the borderlands between the conventional publicness of social media and the privateness of interpersonal communication. They contain “elements of social media” (Rogers, 2020, p. 216) in that they provide social

functions, but are first and foremost private messaging platforms. Abidin (2021) describes how the contemporary internet has shifted toward *refracted publics* from something that has previously been described as *networked publics* (Varnelis, 2008). According to Abidin, *refracted publics* are “mobilized to avoid detection, promote deflection, and facilitate the dissemination of specific messages away from or toward target audiences,” crucially “alternating the public/private” (p. 10). By this logic, chat apps are both tools for mass and private communication, akin to what others have theorized as *masspersonal communication* (O’Sullivan & Carr, 2018).

Considering the spaces mediated by chat apps as *refracted publics* also helps to better understand and conceptualize their idiosyncrasies. Some chat apps allow broadcast groups similar to email listservs that may be publicly accessible, joinable, and through which content can be shared (Rogers, 2020). Such content can then trickle in cascades into more private conversations in the same app—or vice versa—launch out of private conversations into a more public realm (Urman & Katz, 2020). Chat apps are also key in offering alternative degrees of publicness in a larger ecology of digital platforms. For example, Agur and Frisch (2019) observe that in the 2014 Hong Kong umbrella movement, platforms were used differently depending on the degree of publicness they afforded—that is, Facebook being primarily public, WhatsApp being in the middle, and Telegram being primarily private.

Sharing and resharing of content has received interest from researchers looking at it through the lens of the cascade—interested in how content cascades manifest once users start sharing things (Cheng et al., 2014). Communication research has proposed a cascading activation model (Entman, 2003), in which information “travel[s] along interpersonal networks,” morphing into a “cascading flow of influence” (pp. 418–419). While the original model assumed relatively linear hierarchical communication across different institutions and levels in society—mediated through legacy media—updated renderings have begun to take note of the important role that platforms play in cascades (Entman & Usher, 2018).

Building on this, our research focuses not on content, but on the undergirding *cascade logic* that describes how information circulates on chat apps. The notion of a *logic* orients itself after research on *media logic* (Altheide & Snow, 1979), which has been further developed into *social media logic*, defined as “strategies, mechanisms, and economies underpinning these platforms’ dynamics” (van Dijck & Poell, 2013, p. 3). We define *cascade logic* as the way in which information in chat app ecologies is trafficked upstream (making its way from private conversations into the mainstream) as well as downstream (allowing information to withdraw from the public eye), providing space for distortion along the way. Cascade logic also describes how chat apps allow the gradual withdrawal and self-segregation of individuals into, or emergence out of, layered spaces of privacy and obfuscation.

The idiosyncrasies of chat apps—meandering between public and private, their immersion in a range of central aspects of life (for both work and play), mediating news content, affording discussion among friends and family, and sustaining relationships within trusted communities—provide fertile ground for dis- and misinformation to fester and to attach itself as content travels through platforms by way of cascade logic.

Methods

We focused our attention on the ecology of chat apps with a keen eye toward identifying unifying patterns and mechanics between different platforms, cultures, and contexts. Considering cross-platform dynamics (Lukito, 2020) and media and platform ecologies (Zuckerman, 2021), instead of single-platform research, is key to “to understand their effects on social movements and political parties” (p. 1504). We take chat apps to be one element of larger hybrid media systems (Chadwick, 2017)—which are defined by an emphasis on “flux, in-betweenness, the interstitial, and the liminal” (p. 5). This also means that we do not present case studies that are representative of the countries we picked but are instead interested in deciphering unifying logics of chat apps that emerge across different locales.

We studied the United States, India, and Mexico for several reasons. First, all three countries are democracies that have markedly shifted toward right-wing populism in recent years (Arteaga Botello, 2020; de Vreese et al., 2018). Simultaneously, all three countries are dealing with disinformation problems (Bradshaw & Howard, 2018). Social media plays an important role in the communication ecosystem in each of these countries (Aneez et al., 2018; Newman et al., 2020). Finally, chat apps play an important, if structurally different, role in each country. We also acknowledge the different usage dynamics surrounding chat apps—with some having niche, some having mass appeal. The unifying feature is how the platforms themselves emphasize encryption in their public communications (even if referring to different types of encryption).

Chat apps in the US have recently drawn attention in the context of white supremacists or pro-Trump activists migrating toward platforms such as Telegram after having been deplatformed (Rogers, 2020; Tynes, 2021), as well as in the context of discussions around E2EE and corresponding government interests (Veen & Boeke, 2020). While WhatsApp enjoys some popularity in the country—hovering at about 10% of the population who use it—it is more popular among diaspora communities, in particular among Latino/Latinx Americans (Gursky et al., 2021), than within the general population.

In India, WhatsApp plays a particularly important role in news consumption, with the country being defined as both a “mobile-first” and a “platform-dominated market” (Aneez et al., 2018, p. 8), and more than 400 million users (Hariharan,

2021). False news reports shared on WhatsApp have been linked to panics in the country, which have led to violent encounters (Farooq, 2018). WhatsApp, as a consequence, has restricted certain sharing functionalities (Aneez et al., 2018). Instances of violence, sometimes referred to as *WhatsApp lynchings*, have also drawn the critique that the Indian government chooses a techno-deterministic framing of WhatsApp as the scapegoat when mob violence is a much deeper-rooted societal problem which to solve entails more than simply regulating WhatsApp and the spread of rumor (Banaji et al., 2020). The ruling Bharatiya Janata Party (BJP) has been highly successful on social media, with the 2019 national election in the country being a defining moment for how WhatsApp had a central role in messaging about the election (Das & Schroeder, 2021), including for the coordinated sharing of messages by political supporters of the BJP (Jakesch et al., 2021).

Mexico, finally, is defined by its high share of mobile news users—81% consume news mobile, and only 20% on desktop, and approximately 76% of internet users use WhatsApp, while 39% use it for news (Newman et al., 2020). Cruz and Harindranath (2020) have pointed out just how central WhatsApp is to life in Mexico, especially because “mobile operators frequently offer zero-rated data for WhatsApp and Facebook use” (n.p.). The election of Andrés Manuel López Obrador in 2018 was accompanied by disinformation campaigns, the use of bots, as well as syndicated accounts that were managed by individuals, though little is known about the role that chat apps played in this regard (Atlantic Council, 2019). In 2018, rumors about child abductors spread through WhatsApp, to the extent that state governments in the country launched information literacy campaigns to counteract the spread of false information (Martínez, 2018).

Our research centers individuals who work to either produce or track political content on chat apps. Studying disinformation from a production studies perspective (Ong & Cabañes, 2019) emphasizes generating understandings of socio-technical structures and mechanics, rather than focusing on content—which aligns with the aim of our research. As Chadwick (2017) argues, in hybrid media systems, the people that are powerful are

those who are successfully able to create, tap, or steer information flows in ways that suit their goals and in ways that modify, enable, or disable the agency of others, across and between a range of older and newer media settings. (p. 285)

It is this group of dynamic interviewees that we sought out. We conducted and analyzed qualitative data from 33 in-depth interviews with individuals who work—either professionally or on a volunteer basis—for political parties, governments, extremist groups, and other political entities, as well as journalists, researchers, marketing professionals, community activists, leaders in the space of digital and human rights, and

digital political consultants. Our sample aimed to strike a balance within each country across different groups of stakeholders, to represent the voices of journalists/researchers, digital political consultants, and propagandists. Because many of our participants are currently active or were previously active in either investigating or creating propaganda and political campaigns, we conducted interviews under the condition of anonymity. Of the 33 interviews, 15 were with US participants, 11 with Indian participants, and 7 with Mexican participants (see online appendix for additional information on interviewees). Institutional Review Board approval for the project was granted on 31 October 2019.

We worked to determine suitable interviewees in the United States, India, and Mexico through various steps. First, we collected and analyzed news articles describing how chat apps were being used to organize and/or disseminate coordinated influence operations. Through this process, we identified 28 reported cases of chat app influence operations in India, 24 reported cases in Mexico, and 45 reported cases in the United States.¹ We began our collection in the fall of 2019, but the cases ranged from 2015 to 2020. We then used these cases and previously established contacts from prior work on social media dis- and misinformation as jumping-off points to identify potential interviewees in each country, for instance, reporters who wrote stories, sources that were mentioned, and ancillary information that would point us to other informants. We also leveraged snowball sampling, a strategy common in research domains such as ours (e.g., Das & Schroeder, 2021), to expand our sample beyond our original compilation of prospective contacts.

Interview subjects were recruited through email outreach and other online channels, and interviews were conducted in English and Spanish language between February 2020 and December 2020 via video chat software. Conversations typically lasted 40 min to an hour. During interviews, researchers took notes and produced thematic memos after each interview. Most interviews were carried out by two interviewers, and therefore, memos and notes were triangulated between interviewers. To analyze our interview recordings, we immersed ourselves in the notes and thematic memos and grouped them into overarching categories (Creswell, 2007) with an eye toward identifying the key dynamics of how information morphs through chat apps by way of cascade logic, and the idiosyncrasies of chat apps that are conducive to the sharing of dis- and misinformation.

Results

Harnessing Human Connections in Communities of Trust

One of the defining features of chat apps are the human connections they afford and, consequently, authenticity and intimacy that go hand-in-hand with information shared by friends, family, and trusted acquaintances. Communication

strategists, therefore, focus on individuals as political messengers to leverage existing relationships, a strategy common in both covert manipulation and grassroots political organizing. The director of a US political advertising firm who specializes in nudging users to create organic political content to share in their networks, particularly in the WhatsApp channels of Spanish-speaking diaspora communities, stated: “UGC [User Generated Content] allows us to create manipulative messages that are effective because of their intimacy.” The strategist, using what he describes as “real stories from real people,” stated that his firm has the ability to reach audiences in the United States through WhatsApp by activating individuals with large followings on their WhatsApp channels. A WhatsApp group moderator in a Latino/Latinx community in Florida, describing the value of the app to his community, pointed out why relational organizing on the app could be effective,

A WhatsApp group is right in your hands, right on your phone, right on your messaging that you use to talk to your mother, your siblings, your business partners . . . I don’t think there’s anything more powerful or direct than a SMS text message or WhatsApp text message.

A prominent Mexican journalist and disinformation expert described the utilization of familiar relationships as part of a larger international trend away from bots and toward human-centric disinformation:

In Latin America and in Mexico we don’t use bots or software. It was left behind a few years ago because it was really easy to detect on Twitter or Facebook and by researchers like me. The trend now is to use individuals.

This is especially relevant in spaces like WhatsApp, where its adoption into everyday life has made it a space where people communicate and receive news from those they trust. The pattern is particularly conspicuous in India, where the BJP has used WhatsApp to coordinate vast networks of political manipulators and hyper-targets messaging to voters (Jakesch et al., 2021). According to our interviews with current and former BJP members and Indian disinformation researchers, party operatives coordinate large numbers of WhatsApp groups, which are, in turn, run by local volunteers who create groups of approximately 50–100 community members that mirror offline networks of likeminded people. Members of these groups are then targeted with messaging informed by hyper-specific data purchased from data brokers. A journalist for a major newspaper in India believes that the BJP’s system of creating hyper-local, targeted WhatsApp groups, en masse “is probably one of the most sophisticated digital campaigns globally . . . It’s very well executed, it’s very sophisticated and I use that word very responsibly.” Throughout our interviews, and across country contexts, multiple participants accentuated not only how it was important in relational organizing to send the right message to the

right recipients, but also how it was crucial that those messages came from the right messenger. Chat apps afford those interested in spreading information—factual or not—to harness the power of intimate messengers with small and established followings, and within communities of trust.

Misinformation Enters the Fray

Our interviews with WhatsApp group moderators, political strategists, and polling experts revealed that chat apps played a role in the spread of false electoral information among diaspora communities in the United States. We define diaspora communities as communities that regularly use chat apps to communicate with people in their country of origin, individuals who share their cultural context, and people living in the United States from that same community. Usage of chat apps is the defining feature of these communities in our research; we are not seeking to conflate groups together or make an argument about the complicated nature of racial/ethnic/national identity in diaspora and immigrant communities (Gursky et al., 2021).

Focusing on Latino/Latinx communities in the swing state of Florida and the South Asian American community in the swing state of North Carolina, participants described to us that WhatsApp groups formed for connection and connecting people with aid during the pandemic saw the emergence of contentious political content, opening the door for misinformation, disinformation, and conspiracy theories. Several interviewees felt that the evolution of discourse echoed manipulation techniques used in their community's country of origin. The group moderator for WhatsApp groups in a Latino/Latinx community in Florida who was cited earlier estimated that 20%–30% of members of his WhatsApp groups attempted to “evangelize” or “convert” people to their own political views regarding the 2020 US election as it neared, with some groups having hundreds of postings in a matter of hours. In another case, a prominent local Latinx figure started a group to connect immigrants to public services during the pandemic. It eventually became overrun with content ranging from “religion, to things on George Soros, to things about Biden, Obama and Harris.” Misleading content capitalized on issues such as abortion, Catholicism, and communism, often through subtleties like translation choices. A Latina Democratic strategist who was a member of numerous WhatsApp groups in Florida noted a particular video in which Joe Biden described himself as a “Progressive.” She felt that the translation of the video purposefully cast Biden in a bad light by using the term “Progresista,” which made Biden seem farther to the political left than he is in reality, “If you’re a first-generation Latin American it’s similar to Socialista or Comunista.” While such an association could have been accidental, it demonstrates the difficulty of establishing intentionality in political messages that are forwarded through WhatsApp.

The problem of differentiating unintentional from intentional associations, misinformation from disinformation, good-faith actors from malicious actors existed in the South Asian American community in North Carolina as well. A community organizer gave a specific example of WhatsApp election law disinformation that claimed “if you mark your ballot with a pen, then your ballot will be considered not acceptable. But in North Carolina, that’s not true.” She described a national organization dedicated to mobilizing South Asian American voters for Democratic candidates whose members, presumably unintentionally, shared voting laws from California that did not apply in North Carolina, spreading dangerous misinformation. While she felt that voting-related mis- and disinformation were the most immediate threats to her community, persisting even after the election was over, she also noted inflammatory false information relating to US relations with India and Pakistan aimed at suppressing Indian voters. She felt this aligned with the BJP’s tactics in India: “I think [content in India and content in the US] is parallel in the sense that division is probably the key goal, but maybe the issues might be slightly different.”

Coordination and Manipulation

According to a member of the BJP who coordinates their WhatsApp strategies for one of India’s most populous states, the BJP uses hyper-local channels to source emotional stories from local news sources, such as a story about a murdered lawmaker, stories he and the party “believe people will connect with.” His team then repackages the information, factual or not, with customized graphics and videos he commissions to frame the story in a pro-BJP light, and he distributes it nationwide through other WhatsApp channels. He spoke with pride about his “crowdsourcing,” saying “[t]he approach is top-down as well as bottom-up. . . This is how the democratic system should work.” Not everyone is enthused about this circumvention of traditional media to create fervor around stories that support the BJP’s agenda. As described by a leader of one of India’s most prominent digital rights organizations, “Our top trends are essentially manufactured by political IT cells of regional and national parties dominated by the Bharatiya Janata Party.” In contrast to this, one Indian disinformation specialist we interviewed warned against ascribing too much power to the BJP’s operations: “Even the opposition, I find, has a weird narrative about the IT cells—that mystical, sort of, technological machine to persuade minds . . . I think it really is a bunch of kids in a room forwarding stuff.” He also asserted, however, that even if the narrative surrounding them was overblown, the IT Cells “are very proficient in overcoming whatever bullshit regulations WhatsApp is going to put out there.”

In the Mexican context, disinformation on chat apps was described to us as one tool within a larger political manipulation industry. As stated by a prominent Mexican journalist:

They [paid propagandists] have contacts with publicity agencies and with the chief of government, of any party and at any level. Left, right, center, municipal, state, federal—these government officials meet with people from publicity agencies and the agencies charge quite a bit of money to put them in contact with people [propagandists].

A paid propagandist stated that he and his colleagues used WhatsApp as part of a toolkit that included apps that they had built themselves, Facebook, Telegram, and Instagram. Regarding WhatsApp, they pointed out:

Right now, we are only capitalizing on Facebook and Instagram. WhatsApp works with different strategies, 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 propagandist claimed his ability to run undetected campaigns opened doors with many political figures and parties. He claimed he was a “provider” for the Mexican Senate and had eight clients for the gubernatorial elections in 2021.

Chat Apps’ Cascade Logic

Chat apps enable both broadcast, one-to-many channels and individual, one-to-one, direct messages. In the political realm, chats are not only targets of disinformation, but are also places where disinformation campaigns are planned, individuals are recruited, and content is created to be distributed on mainstream social media platforms, as well as television, and radio. We define cascade logic as key mechanisms within chat apps, allowing information to be cultivated and to trickle downstream into (at times) encrypted chats, as well as vice versa: Information that emerges within chat apps can traffic upstream and into the public (for instance, social media platforms such as Twitter), and even be picked up by legacy media. Cascade logic also encompasses information that moves between platforms—from obscurity into the public eye, as well as the gradual withdrawal and self-segregation of individuals and the information they circulate into, or emergence out of, layered spaces of privacy and obfuscation.

In the United States, an interview with a former member of a violent white supremacist group showcased the important role that chat apps can play in mediating publicness and privacy. Individuals who seemed to support white supremacy on Discord and other public, non-chat app platforms would be sent links to group chats on Telegram and other chat apps with the invitation “to talk with a little bit more freedom.” The interviewee clarified that this perceived “freedom” on Telegram often has more to do with lax content moderation than encryption:

The purpose of Telegram is outreach . . . of making a channel which would then be completely public and groups will be able to post their propaganda there. . . so people can broadcast and get more followers on Telegram. They don’t want to make it a secret.

Another former white supremacist reiterated that the promise of encryption is not the only deciding factor in adopting chat apps, explaining: “Something being encrypted definitely does help but most of them don’t care because they don’t think ahead. I know a few white supremacists who think ahead, but it is not common.”

Jumping back to the first-mentioned former white supremacist, the person described how they had been involved in a campaign that had successfully used chat platforms such as Discord and Gab to convince news organizations of the lie that a mass shooter had been a member of a small white supremacist group, capitalizing on cascade logic and the trafficking of information up a cascade and between platforms:

Once we already made contact with media, it was moving into 4chan so that other people would start spreading it, getting smaller news outlets—especially the local ones to start reporting on it, and then it would carry to larger platforms (CNN, NYT). Obviously, it is mostly when a story is first coming out. It is when there is the most confusion and most tension . . . That is something we would exploit.

The case of white supremacist chat app usage demonstrates the importance of approaching chat apps, and their potential for manipulating public opinion, within a larger media ecology.

A pollster from South Florida who had been studying diaspora and immigrant communities there for years described how WhatsApp conspiracy theories such as that Joe Biden was allegedly a pedophile were having a measurable effect on what he was encountering in focus groups that he ran: “you have this modern thing, that’s WhatsApp, but the stuff that comes out of it is being analyzed over the radio waves, and it’s having an impact.”

In India, the BJP uses a large number of coordinated WhatsApp groups, known as “IT Cells,” to create and spread disinformation. As described by a researcher who studies political disinformation and manipulation in India:

There’s headquarters . . . there’re state-level groups, there’re district-level groups, and finally there’re booth-level groups, these booths as in booth-poll-voting level groups and these are the ones that are usually public. The rest are usually private, within party communication.

The private, within-party WhatsApp channels are used to curate and spread disinformation on Twitter. As stated by an Indian disinformation expert:

Someone in an IT Cell sitting in Delhi will create a Google doc that contains a hundred example tweets that people can tweet about that contain hashtags. (. . .) These are all real people, and that's what gets these hashtags trending.

In Mexico, our interviews pointed to the critical role that chat apps play in moving mis- and disinformation between public and private spaces. A Mexican journalist and disinformation expert described to us the “multilayered,” or cross-platform, strategy of paid political propagandists: “peer-to-peer on WhatsApp” to “tighter-knit” Facebook communities to Twitter or to the news media. Much like white supremacists in the United States, the goal is the manipulation of mainstream media: “when these campaigns reach the media, when I’ve interviewed people who work in disinformation, or work as bots or create fake news, their objective is to reach the media. That’s when they get paid.”

What became clear throughout interviews was that chat apps are not only spaces where disinformation is seeded, but also where manipulation of mainstream discourse on social media platforms and news media is coordinated. Due to the cascade logic of chat apps—information traveling upstream into established news spaces and traveling downstream into at times encrypted, direct messages—it is important to consider dis- and misinformation on public forums such as Instagram, Facebook, Twitter, and legacy media as deeply intertwined with chat apps.

Discussion

The purpose of this study was to shed light on how chat apps are employed for the distribution of dis- and misinformation, and how the idiosyncrasies of chat apps and their respective logics promulgate their important role in a platform and media ecology in which information spreads not only within but also across platforms. We identified four key themes that describe chat apps and their mechanics as they pertain to the spread of dis- and misinformation:

- (1) Political strategies on chat apps involve harnessing human connections. Trust relationships, the authenticity of individual contacts, and intimacy afforded through chat apps allow for the dissemination of content that often defies verification precisely because it already comes vetted by trusted friends, family members, or members of communities organized into WhatsApp groups or feeds. Those who utilize chat apps for their political activities, in turn, benefit from the private relationships that fuel chat app use—allowing for campaigns to fly under the radar once they manage to penetrate these spaces.
- (2) Misinformation can enter the fray because context can easily get lost, and frames of interpretation can change as content moves through chat apps and gets forwarded. For example, in the United States,

people in diaspora communities that use chat apps are sometimes confronted with false content from their closest contacts with little recourse and ways to verify source attribution, and groups designed to be public are being co-opted to spread false information. What is intentional and what is unintentional, in addition to what is coordinated and what is uncoordinated, becomes incredibly difficult to parse apart for users.

- (3) Chat apps allow for coordination and manipulation of the sharing and spreading of certain content. For example, violent right-wing groups use chat apps to create public channels that anyone can join, to recruit, as well as to coordinate manipulation of other platforms. In India, the BJP has organized a network of political volunteers over WhatsApp, sources emotional stories and repackages them, and uses these mechanisms to leverage impact over local and national conversations (Jakesch et al., 2021). In Mexico, the disinformation industry appears to be moving away from automation such as WhatsApp bots, and propagandists use encrypted chats on Telegram to coordinate influence campaigns.
- (4) Distinctive for chat apps is their cascade logic. This means that, within chat app ecologies, platforms operate at a neuralgic point that allows both upstream communication—information making its way from private conversation into mainstream media—and downstream communication—people and information getting gradually immersed into ever-more-private spaces. This study illustrates how chat apps in India allow the BJP to disseminate and repackage information through hierarchical content dissemination infrastructures that the party built with the specificities of the app in mind. In the United States, chat apps afford small, dedicated (and at times nefarious) groups avenues to influence public conversation on social and in legacy media. In Mexico, cases discussed in this study highlight how chat apps can allow for cross-platform organizing in peer-to-peer networks.

In line with previous research, our study showcases how chat apps are important spaces for dis- and misinformation—for political parties, propagandists, marketers that help political agents, political activists, but also for people acting in a nonprofessional capacity who simply want to talk about politics (Banaji et al., 2020; Kligler-Vilenchik, 2021; Rossini et al., 2021). As chat apps broach all areas of life (Cruz & Harindranath, 2020), it emerges as a crucial task for communication researchers to investigate the ways in which information moves through these platforms, and what problems might emanate along the way.

Previous studies have explored how disinformation morphs between platforms by “trading up the chain” (Marwick & Lewis, 2017, pp. 38–39). Indeed, our research

also reports on examples in which disinformation was trafficked and coordinated through chat apps to feed into public debate on social media and in legacy media. But in addition to amplification processes, chat apps also function as important downstream channels of communication. Cascade logic allows people to withdraw from the public eye, yet to exist and communicate among their private contacts and to engage with content in shielded spaces and gradations of public/privacy. As propagandists utilize tactics that mesh with these infrastructures, it becomes important to identify strategies that can assuage and alleviate issues that may emerge as disinformation, rumor, and other harmful communication spreads.

Conclusion

Our findings describe chat apps as venues used by communities of trust, and in which information can easily (and unwittingly) turn into misinformation. Importantly, this study elucidates a *cascade logic* inherent to these platforms. Chat apps function as funnels for information and groups of individuals to withdraw into private spaces. At the same time, chat apps serve as trading points for manipulation and coordination—for example, for information to be trafficked from hidden chats into the public eye. Chat apps are venues in which trusted communities talk to each other—trust that sometimes gets abused when disinformation is seeded, gets forwarded, and (unwittingly) morphs into misinformation.

Acknowledgements

The authors thank Joel Carter, Claire Coburn, Emily Flores, Romi Geller, Katlyn Glover, and Jimena Pinzon for their assistance on this project.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This study is a project of the Center for Media Engagement (CME) at Moody College of Communication at the University of Texas at Austin, and was supported by Omidyar Network, Open Society Foundations, as well as the John S. and James L. Knight Foundation.

ORCID iD

Martin J. Riedl  <https://orcid.org/0000-0003-2411-1998>

Supplemental material

Supplemental material for this article is available online.

Note

1. List available from authors upon request.

References

- Abidin, C. (2021). From “networked publics” to “refracted publics”: A companion framework for researching “below the radar” studies. *Social Media + Society*, 7(1), 1–13. <https://doi.org/10.1177/2056305120984458>
- Agur, C., & Frisch, N. (2019). Digital disobedience and the limits of persuasion: Social media activism in Hong Kong’s 2014 Umbrella Movement. *Social Media + Society*, 5(1), 1–12. <https://doi.org/10.1177/2056305119827002>
- Altheide, D. L., & Snow, R. P. (1979). *Media logic*. SAGE.
- Aneez, Z., Neyazi, T. A., Kalogeropoulos, A., & Nielsen, R. K. (2018). *Reuters Institute India digital news report*. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-03/India_DNR_FINAL.pdf
- Arteaga Botello, N. (2020). The populist transition and the civil sphere in Mexico. In J. C. Alexander, P. Kivisto, & G. Sciortino (Eds.), *Populism in the civil sphere* (pp. 96–124). Wiley.
- Atlantic Council. (2019, March 28). *Disinformation in democracies: Strengthening digital resilience in Latin America*. <https://www.atlanticcouncil.org/in-depth-research-reports/report/disinformation-democracies-strengthening-digital-resilience-latin-america/>
- Banaji, S., Bhat, R., Agarwal, A., Passanha, N., & Pravin, M. S. (2020). *WhatsApp vigilantes: An exploration of citizen reception and circulation of WhatsApp misinformation linked to mob violence in India*. London School of Economics and Political Science. <https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/WhatsApp-Misinformation-Report.pdf>
- Baulch, E., Matamoros-Fernández, A., & Johns, A. (2020). Introduction: Ten years of WhatsApp: The role of chat apps in the formation and mobilization of online publics. *First Monday*, 25(1). <https://doi.org/10.5210/fm.v25i12.10412>
- Bradshaw, S., & Howard, P. N. (2018). The global organization of social media disinformation campaigns. *Journal of International Affairs*, 71(15), 23–32.
- Chadwick, A. (2017). *The hybrid media system: Politics and power, second edition*. Oxford University Press.
- Cheng, J., Adamic, L. A., Dow, P. A., Kleinberg, J., & Leskovec, J. (2014). Can cascades be predicted? In *Proceedings of the 23rd International Conference on World Wide Web, WWW’14, April 7–11, 2014, Seoul, Korea* (pp. 925–936). <https://doi.org/10.1145/2566486.2567997>
- Creswell, J. W. (2007). *Qualitative inquiry and research design: Choosing among five approaches* (2nd ed.). SAGE.
- Cruz, E. G., & Harindranath, R. (2020). WhatsApp as “technology of life”: Reframing research agendas. *First Monday*, 25(1). <https://doi.org/10.5210/fm.v25i12.10405>
- Das, A., & Schroeder, R. (2021). Online disinformation in the run-up to the Indian 2019 election. *Information, Communication & Society*, 24(12), 1762–1778. <https://doi.org/10.1080/1369118X.2020.1736123>
- de Vreese, C. H., Esser, F., Aalberg, T., Reinemann, C., & Stanyer, J. (2018). Populism as an expression of political communication content and style: A new perspective. *International Journal of Press/Politics*, 23(4), 423–438. <https://doi.org/10.1177/1940161218790035>
- DFRLab. (2021, February 11). Extremists on Telegram exploit Parler’s de-platforming to ramp up recruiting. *Medium*. <https://>

- medium.com/dfirlab/extremists-on-telegram-exploit-parlers-de-platforming-to-ramp-up-recruiting-eb1256227a5d
- Encryption Working Group. (2019). Moving the encryption policy conversation forward. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/files/EWG_Encryption_Policy.pdf
- Entman, R. M. (2003). Cascading activation: Contesting the White House's frame after 9/11. *Political Communication*, 20(4), 415–432. <https://doi.org/10.1080/10584600390244176>
- Entman, R. M., & Usher, N. (2018). Framing in a fractured democracy: Impacts of digital technology on ideology, power and cascading network activation. *Journal of Communication*, 68(2), 298–308. <https://doi.org/10.1093/joc/jqx019>
- Farooq, G. (2018). Politics of fake news: How WhatsApp became a potent propaganda tool in India. *Media Watch*, 9(1), 106–117. <https://doi.org/10.15655/mw/2018/v9i1/49279>
- Gil de Zúñiga, H., Ardèvol-Abreu, A., & Casero-Ripollés, A. (2021). WhatsApp political discussion, conventional participation and activism: Exploring direct, indirect and generational effects. *Information, Communication & Society*, 24(2), 201–218. <https://doi.org/10.1080/1369118x.2019.1642933>
- Gursky, J., Glover, K., Joseff, K., Riedl, M. J., Pinzon, J., Geller, R., & Woolley, S. C. (2020, October 26). *Encrypted propaganda: Political manipulation via encrypted messages apps in the United States, India, and Mexico*. Center for Media Engagement, University of Texas at Austin. <https://mediaengagement.org/research/encrypted-propaganda>
- Gursky, J., Riedl, M. J., & Woolley, S. (2021, March 19). The disinformation threat to diaspora communities in encrypted chat apps. *Brookings Techstream*. <https://www.brookings.edu/techstream/the-disinformation-threat-to-diaspora-communities-in-encrypted-chat-apps/>
- Hariharan, S. (2021, January 9). WhatsApp's privacy policy pushes users to Signal, Telegram. *Times of India*. <https://timesofindia.indiatimes.com/business/india-business/whatsapps-privacy-policy-pushes-users-to-rivals/articleshow/80178485.cms>
- Jack, C. (2017). Lexicon of lies: Terms for problematic information. *Data & Society*. https://datasociety.net/wp-content/uploads/2017/08/DataAndSociety_LexiconofLies.pdf
- Jakesch, M., Garimella, K., Eckles, D., & Naaman, M. (2021). Trend Alert: How a cross-platform organization manipulated Twitter Trends in the Indian General Election. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1–19. <https://doi.org/10.1145/3479523>
- Johns, A. (2020). “This will be the WhatsApp election”: Cryptopublics and digital citizenship in Malaysia's GE14 election. *First Monday*, 25(1). <https://doi.org/10.5210/fm.v25i12.10381>
- Kalogeropoulos, A. (2021). Who shares news on mobile messaging applications, why and in what ways? A cross-national analysis. *Mobile Media & Communication*, 9(2), 336–352. <https://doi.org/10.1177/2050157920958442>
- Kligler-Vilenchik, N. (2021). Friendship and politics don't mix? The role of sociability for online political talk. *Information, Communication & Society*, 24(1), 118–133. <https://doi.org/10.1080/1369118X.2019.1635185>
- Krafft, P. M., & Donovan, J. (2020). Disinformation by design: The use of evidence collages and platform filtering in a media manipulation campaign. *Political Communication*, 37(2), 194–214. <https://doi.org/10.1080/10584609.2019.1686094>
- Lukito, J. (2020). Coordinating a multi-platform disinformation campaign: Internet Research Agency activity on three U.S. social media platforms, 2015–2017. *Political Communication*, 37(2), 238–255. <https://doi.org/10.1080/10584609.2019.1661889>
- Marlinspike, M. (2021, December 23). It's amazing to me that after all this time, almost all media coverage of Telegram still refers to it as an “encrypted messenger.” [Tweet]. *Twitter.com* <https://twitter.com/moxie/status/1474067549574688768?s=21>
- Martínez, M. (2018, November 12). Burned to death because of a rumour on WhatsApp. *BBC News*. <https://www.bbc.com/news/world-latin-america-46145986>
- Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation online. *Data & Society*. <https://datasociety.net/library/media-manipulation-and-disinfo-online/>
- Matassi, M., Boczkowski, P. J., & Mitchelstein, E. (2019). Domesticating WhatsApp: Family, friends, work, and study in everyday communication. *New Media & Society*, 21(10), 2183–2200. <https://doi.org/10.1177/1461444819841890>
- Newman, N., Fletcher, R., Schulz, A., Andi, S., & Nielsen, R. K. (2020). *Reuters Institute digital news report 2020*. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf
- Ong, J. C., & Cabañes, J. V. A. (2019). When disinformation studies meets production studies: Social identities and moral justifications in the political trolling industry. *International Journal of Communication*, 13, 5771–5790. <https://ijoc.org/index.php/ijoc/article/view/11417>
- O'Sullivan, P. B., & Carr, C. T. (2018). Masspersonal communication: A model bridging the mass-interpersonal divide. *New Media & Society*, 20(3), 1161–1180. <https://doi.org/10.1177/1461444816686104>
- Pang, N., & Woo, Y. T. (2020). What about WhatsApp? A systematic review of WhatsApp and its role in civic and political engagement. *First Monday*, 25(1). <https://doi.org/10.5210/fm.v25i12.10417>
- Perrin, A., & Anderson, M. (2019). *Share of U.S. adults using social media, including Facebook, is mostly unchanged since 2018*. Pew Research Center. <https://www.pewresearch.org/fact-tank/2019/04/10/share-of-u-s-adults-using-social-media-including-facebook-is-mostly-unchanged-since-2018/>
- Rogers, R. (2020). Deplatforming: Following extreme Internet celebrities to Telegram and alternative social media. *European Journal of Communication*, 35(3), 213–229. <https://doi.org/10.1177/0267323120922066>
- Rossini, P., Stromer-Galley, J., Baptista, E. A., & Veiga de Oliveira, V. (2021). Dysfunctional information sharing on WhatsApp and Facebook: The role of political talk, cross-cutting exposure and social corrections. *New Media & Society*, 23(8), 2430–2451. <https://doi.org/10.1177/1461444820928059>
- Santos, M., & Faure, A. (2018). Affordance is power: Contradictions between communicational and technical dimensions of WhatsApp's end-to-end encryption. *Social Media + Society*, 4(3), 1–16. <https://doi.org/10.1177/2056305118795876>
- Semenzin, S., & Bainotti, L. (2020). The use of Telegram for non-consensual dissemination of intimate images: Gendered affordances and the construction of masculinities. *Social Media + Society*, 6(4), 1–12. <https://doi.org/10.1177/2056305120984453>
- Shehabat, A., Mitew, T., & Alzoubi, Y. (2017). Encrypted Jihad: Investigating the role of Telegram App in lone wolf attacks in

- the West. *Journal of Strategic Security*, 10(3), 27–53. <https://doi.org/10.5038/1944-0472.10.3.1604>
- Treré, E. (2020). The banality of WhatsApp: On the everyday politics of backstage activism in Mexico and Spain. *First Monday*, 25(12). <https://doi.org/10.5210/fm.v25i12.10404>
- Tynes, R. (2021). Gavin McInnes's hate machine. *First Monday*, 26(2). <https://doi.org/10.5210/fm.v26i2.11424>
- Urman, A., & Katz, S. (2020). What they do in the shadows: Examining the far-right networks on Telegram. *Information, Communication & Society*. Advance online publication. <https://doi.org/10.1080/1369118X.2020.1803946>
- van Dijck, J., & Poell, T. (2013). Understanding social media logic. *Media and Communication*, 1(1), 2–14. <https://doi.org/10.12924/mac2013.01010002>
- Varnelis, K. (Ed.) (2008). *Networked publics*. MIT Press.
- Veen, J., & Boeke, S. (2020). No backdoors: Investigating the Dutch standpoint on encryption. *Policy & Internet*, 12(4), 503–524. <https://doi.org/10.1002/poi3.233>
- Walther, S., & McCoy, A. (2021). US extremism on Telegram: Fueling disinformation, conspiracy theories, and accelerationism. *Perspectives on Terrorism*, 15(2), 100–124.
- Welch, C. (2019, March 6). Read Mark Zuckerberg's letter on Facebook's privacy-focused future. *The Verge*. <https://www.theverge.com/2019/3/6/18253472/mark-zuckerberg-facebook-letter-privacy-encrypted-messaging>
- Zuckerman, E. (2021). Why study media ecosystems? *Information, Communication & Society*, 24(10), 1495–1513. <https://doi.org/10.1080/1369118X.2021.1942513>

Author Biographies

Jacob Gursky (BA, University of Pennsylvania) is a research affiliate with the Center for Media Engagement at the University of

Texas at Austin. His research interests include disinformation, digital literacy, privacy activism, and the repercussions of surveillance capitalism. His work has been published through the *Brookings Institution* and *MIT Tech Review*.

Martin J. Riedl (PhD, University of Texas at Austin) is a postdoctoral fellow at the Center for Media Engagement, and a research associate with the Technology and Information Policy Institute, both at the University of Texas at Austin. His research interests include platform governance, digital journalism, and dis/misinformation. His work has been published in *Information, Communication & Society*, *Computers in Human Behavior*, and *Policy & Internet*, among other journals.

Katie Joseff (MA, Stanford University) is a research affiliate with the Center for Media Engagement at the University of Texas at Austin. Her research interests include political disinformation and election manipulation, the psychological biases underlying propaganda, harassment of marginalized groups, and the ethics of emerging technologies. Her work has been published through organizations such as the *National Endowment for Democracy*, the *Anti-Defamation League*, and the *Institute for the Future*.

Samuel Woolley (PhD, University of Washington) is an assistant professor in the School of Journalism and Media and a project director for propaganda research at the Center for Media Engagement, both at the University of Texas at Austin. His research is focused on how emergent technologies are used in and around global political communication, particularly in the context of computational propaganda and how social media are used to manipulate public opinion. He is the author of *The Reality Game: How the Next Wave of Technology Will Break the Truth*. His research has been published in the *International Journal of Communication*, *New Media & Society*, and *First Monday*, among other journals.