The political use of encrypted messaging applications: Evidence from southeast Asia and its implications for the global public sphere
by Zelly C. Martin, Inga K. Trauthig, Katlyn Glover, and Samuel C. Woolley

Abstract
Global Internet users face rising challenges with well-organized disinformation and propaganda campaigns. Scholars have studied this challenge by examining political communication over social media platforms including Facebook, YouTube, and X (formerly Twitter). Much less work has examined the manipulative political role of encrypted messaging applications (EMAs), despite their massive popularity around the world. Our research examines EMAs as elements of the global public sphere through 16 qualitative interviews with people who design and track propaganda campaigns online in three ASEAN nations: Indonesia, Myanmar, and the Philippines. Interviewees report that: 1) politicians and political groups harness EMAs in coordinated efforts to inorganically amplify their own agendas; 2) disinformation proliferates on EMAs, but civil society works to address this; and, 3) while citizens see the encrypted aspect of EMAs as powerful for civic engagement, they also feel it presents unique barriers to addressing what has become a serious problem with disinformation on EMAs.

Contents
Introduction
Literature review
Method
Findings
Discussion
Conclusion

Introduction
From the UNESCO New World Information and Communication Order in the 1980s to the World Summit on the Information Society in the early 2000s, organizations in the Global North have long called for a worldwide information society that would produce a global public sphere (Raboy, 2004). Many looked to the Internet as a potentially democratizing global force, capable of disrupting authoritarianism — a concept summed up as “liberation technology” by Diamond (2010). But this optimistic conception of a global
The political use of encrypted messaging applications: Evidence from southeast Asia and its implications for the global public sphere

public sphere has been complicated by rampant disinformation and Internet control in all regions of the world (Bradshaw and Howard, 2019). Social media companies have a particularly weak handle on information problems in the Global South. The 2021 “Facebook Papers” leak of internal documents by former Facebook employee Frances Haugen illuminated Meta’s failure to manage coordinated disinformation, violent content, and hate speech from South America to the Indian subcontinent (Elliott, et al., 2021).

Meta’s program Free Basics, designed to facilitate free access to certain Internet services in Global South countries, was touted by the company as a program to further connections and promote democracy (Deejay and Wells, 2021), in theory allowing for global public discourse. However, experts have argued that the program is more akin to an imperialist cooptation of the online landscape — a way for Meta to capitalize on the data of users in the Global South while tightly controlling their experience of the Internet (Nothias, 2020).

Parallel to Meta’s efforts to corner the global online sphere and control emerging markets, other platforms continue to be simultaneously used for political endeavors both democratic and repressive (Diamond and Plattner, 2012). Empirical evidence, however, increasingly points towards illiberal ends (Jones, 2020). The majority of research into the political use of online media tools relies upon analysis of platforms like X (formerly Twitter) and Facebook — before Elon Musk purchased X, it continuously allowed researchers and others access to its API. Prior to the summer of 2021, Facebook had increased scholarly access to data through CrowdTangle. Encrypted messaging applications (EMAs — WhatsApp, Telegram, Viber, etc.), meanwhile, are understudied in this regard — despite touting massive popularity across the Global South and countries like Germany, the United Kingdom, and United States (Statista, 2022b).

Better understandings of the political use of EMAs — which began outstripping “traditional” social media like Facebook, YouTube, and X in terms of monthly added users in 2017 and now boast billions of users across the globe (Chesney, et al., 2018) — are very likely to disrupt and shift our ideas about democracy and control online. This study aims to fill a gap in our understandings surrounding the production of political communication campaigns — from disinformation efforts to grassroots organizing — over EMAs in three ASEAN (Association of Southeast Asian Nations) countries: Indonesia, Myanmar, and the Philippines. Each is home to tens of millions of EMA users, with Indonesia boasting more WhatsApp users (84.8 million in June 2021) than any country, bar Brazil and India (Statista, 2022a).

We investigate four intersecting elements that pertain to the nature of the global public sphere in these countries: disinformation and propaganda on EMAs (influence of the state), organized democratic activism and fact-checking on EMAs (civil society), the use of these platforms by the public, and EMAs as an imperial force (power of platforms). Utilizing data from 16 in-depth qualitative interviews with the makers and trackers of political content on EMAs and other social media in these countries, this study aims to understand the boundaries of the global public sphere in parts of Global South and beyond by analyzing the entanglements of these four elements. We query whether the global public sphere truly exists, and whether the rise and usage of EMAs in these countries has implications for previous understandings of the concept of a global public sphere as defined by Western scholars. We conclude that these EMAs have become integral to the global public sphere. The state, the public, and civil society are all communicating in these spaces. They are not doing so on equal footing, however, and scholarship must take into account the level of control exercised by powerful and well-resourced actors on and across various EMAs. Across all three countries, politicians and political groups harness EMAs in coordinated efforts to inorganically amplify their own agendas and attack their opposition. Citizens and civil society see the encrypted aspect of EMAs as powerful for civic engagement and organizing, but they also feel it presents unique barriers to addressing what has become a serious problem with dis- and mis- information on WhatsApp and Telegram, in particular.
Literature review

Global public sphere

Castells (2008) argued that the Internet and globalization have brought about a new public sphere for discussing socio-political life: the global public sphere. This iteration for civic life advances Habermas’ normative conception of the public sphere — as a “network for communicating information and points of view” [1] — from the national to the global. The global public sphere optimistically aims for transnational, individualized communication from many-to-many. It is organized by the global network society (Castells, 2013) around the media, which now includes the Internet, a many-to-many system that transcends traditional forms of mass media, government control, and geographic borders.

But while Castells’ global public sphere has the same components as Habermas’ — the state, civil society, and the public — it is uniquely characterized by a brand of globalization wherein nation-states adapt and form mediated networks of world-wide governance (i.e., ASEAN). Concurrently, civil society encompasses both local civil society actors like grassroots organizations as well as global non-governmental organizations (NGOs) while the global public sphere is organized around Internet platforms (like Facebook) that have global reach despite typically being dependent upon state regulation. In this multi-national space traditional mass media and the Internet combine to allow for a space wherein “nonstate actors influence people’s minds” and “societies can ... diverge from the values and interests institutionalized in the political system” [2].

But scholars have questioned whether this fundamentally Western theory can actually be applied to a global context (Ndlela, 2007). The Western conceptions of democracy and sovereignty are integral to the initial conceptual framework of the public sphere (Fraser, 2014), meaning any application of the concept to nascent democracies or authoritarian states needs to formulate clearly which aspects exactly are studied and the purpose of that research. Further, a space does not become a public sphere merely by facilitating communication — it must also “enhance democracy” [3]. Are Internet platforms capable of enhancing democracy across the globe? We propose global public spheres as a framework for this study as this approach helps us to undertake a nuanced analysis encompassing different types of activity and their impact. This is most useful compared to other theoretical approaches that would also be feasible but examine either the democratic potentials of EMAs (such as mobilization into bottom-up protest movements) when applying social movement theory (della Porta, 2013) or the survival of authoritarian states when focusing on regime propaganda in these spaces when applying conceptual frameworks like authoritarian resilience (Huang, et al., 2019). The framework of the global public sphere allows for an investigation into the democratizing potential of EMAs while also critically assessing the simultaneous limiting of this potential due to state propaganda on the same platforms. We examine what it means for a platform on which the power of the state, the public, and civil society are in tension, to “enhance democracy.” Finally, because “encrypted” typically implies private, it is especially worth examining in what ways EMAs have become public spheres. If the digital public sphere does exist, social media platforms still govern speech and participation (DeNardis and Hackl, 2015; Gillespie, 2017), potentially limiting the possibilities of global digital spaces to be true public spheres.

Platform imperialism

In recent years Internet access has expanded in Indonesia, Myanmar, the Philippines, and beyond through programs like Meta’s Free Basics. This program allows people access to a limited digital experience controlled exclusively by Meta. On the one hand, this provides new populations a modicum of collective power by connecting them to some online resources for facilitating organization and communication. On the other, it allows Western companies the right to tightly control people’s mediated lives.

Jin (2017) argues that because the most powerful social media platforms (YouTube, Facebook, and Google) are U.S.-owned and operated and primarily accumulate capital for U.S.-based owners, they represent “a new form of imperialism — platform imperialism” [4]. This brand of distributed global influence,
The political use of encrypted messaging applications: Evidence from southeast Asia and its implications for the global public sphere

epitomized by seemingly benevolent endeavors like Free Basics, contributes to U.S. dominance and U.S. cultural hegemony, even as they play a major role in the dissemination of culture from outside the West. Because of this, some scholars contend that the U.S. remains dominant in the digital sphere (Kwet, 2019; Nieborg, et al., 2020). Others argue that Internet platforms have geopolitical influence beyond the nations that they are tied to (Bremmer, 2021), so that Meta is not necessarily furthering U.S. dominance but instead, Meta’s dominance. As Castells (2008) highlighted, these platforms must contend with state regulations, but are not necessarily working in tandem with governments. Indeed, Meta and the U.S. government are often at odds, as evidenced by suits filed against Meta for violating antitrust laws (Durkee, 2021).

**Platform limitations on the global public sphere**

Facebook and other platforms’ efforts to expand and corral life online abroad exert power across the Global South in ways beyond limiting access or enriching Western shareholders, however. Although Free Basics was touted by Meta as a way to encourage open communication and spread democracy, it is actually increasing the spread of disinformation (Deejay and Wells, 2021), purposefully spread false content most generally spread by the powerful in bids to control the majority. The continuous barrage of this manipulative, spurious content makes it difficult for users to differentiate between false and real news (Solon, 2017). Simultaneously, platforms’ algorithms — underscored by their financial motivations and cultural perspectives — lead to a pushing of Western content (Solon, 2017). These dynamics mean that Facebook may be stymying the global public sphere — and democratic communication broadly speaking — rather than enabling them.

Internet usage and expanded global communication may correlate with an increase in democratic characteristics such as increased political expression in China. Dijk and Hacker (2018) pick up this line of argument, suggesting we cannot contend that the Internet, and expanded global communication, will lead to revolutionized communication or an increase in democracy. Crucially, however, they argue that new communication technologies are not mere continuations of past iterations. Because of this, we must investigate emerging technologies anew. How, for instance, might new media tools allow for control rather than freedom in informational spaces? Demirdis and co-authors (2023) illuminated one such use in the case of political elites using X to spread government propaganda in Turkey. Might the perspective of platform imperialism, and particularly as it considers the power of the corporation and country which host the technology itself, further complicate political action taking place in these digital spaces? In essence, the democratic potential of increased global communication is limited by the power and goals of the entities and organizations facilitating such communication. Given Castells’ argument that the public sphere is now networked across platforms, the platforms’ ability to limit public discourse must be taken into account. It is necessary, then, to investigate political action on emerging communication tools which effectively *host* the public sphere. EMAs including Meta’s WhatsApp are massively popular but understudied digital media tools unique in this regard. The following analysis explores the ways in which these particular types of digital platforms may limit discourse among the public, the state, and/or civil society in three ASEAN nations.

This work is organized by three interrelated research questions:

*RQ1*: How and why are EMAs relevant for a global public sphere as it exists and operates within and between Indonesia, the Philippines, and Myanmar?

*RQ2*: What are the differences in how civil society, the public, and the state engage on EMAs?

*RQ3*: What, if any, constraints do Western-owned platforms impose on the possibilities of global public spheres?
The political use of encrypted messaging applications: Evidence from southeast Asia and its implications for the global public sphere

Method

Case studies

Countries

We investigate EMA usage in Indonesia, the Philippines, and Myanmar for three reasons:

First, Indonesia, The Philippines and Myanmar are all considered “transforming systems” by the Bertelsmann Stiftung’s Transformation Index (2022), albeit on different levels with Indonesia ranking 47 (out of 138), the Philippines ranking 54, with Myanmar lagging far behind ranking 121 in the most recent index from 2020. BTI analyzes and evaluates whether and how developing countries and countries in transition are steering social change toward democracy. The fact that all three countries are considered in transformation between political systems (authoritarian regime on the one end of the spectrum and liberal democracy on the other) is relevant for our study as countries in transformation are more volatile to any emerging issues carrying potential impact for societal polarization, including emerging technological changes such as the spread of chat apps (Zeitzoff, 2017).

Second, Freedom House ascribes varying levels of global and Internet freedom across these three country cases. This allows for intra-study comparability of pivotal nations in the ASEAN region on a useful level as the levels are similar but not the same. The Philippines and Indonesia are both characterized as “partly free” (the Philippines scores marginally higher), while Myanmar is “not free” (Freedom House, 2022). Myanmar has recently returned to authoritarian rule following a brief period of democracy.

Finally, the three cases display similar usage of the Internet, social media, and smart phones. Facebook is widely used in all three of our countries of interest. Facebook penetration in Indonesia is currently at 62 percent (Statista, 2021b). Indonesia is WhatsApp’s (owned by Facebook) fourth largest country user globally, with 68.8 million users in the country (Dean, 2021). In the Philippines, 99 percent of Internet users (63 percent of the country) use Facebook and 98 percent use Facebook Messenger (Malig, 2021), while only five percent use Viber (a growingly popular Japanese-owned EMA) and two percent use WhatsApp. In Myanmar, nearly 52 percent of the population utilized Facebook in January 2021. By October 2021, this had dropped to 39.2 percent of the population (NapoleonCat, n.d.). A likely explanation for this drop may be the coup on 1 February 2021, in which the military junta seized control and overthrew the democratically elected government, the National League for Democracy, led by Aung San Suu Kyi (Cuddy, 2021). The military junta periodically shut off the Internet, cutting off access to Facebook and all other social media. This has furthered a dearth of credible information in the country (Guest, 2021). Despite this, smart phone usage in Myanmar is shockingly high—smart phone penetration was at 127 percent in February 2021, meaning there are more phones than people (Kemp, 2021). Indonesia and the Philippines have lower, but still high, smart phone saturation, at 67 percent and 72 percent in 2020, respectively (Statista, 2021a, 2021c).

Although Myanmar is inarguably undergoing the most political turmoil at this juncture, the Philippines and Indonesia too have faced turmoil such as disinformation campaigns. The Philippines’ President Rodrigo Duterte’s use of troll farms to falsely increase support for his campaign has been well-documented in academic work (Ong and Cabañes, 2018) and investigative reporting (Mahtani and Cabato, 2019). Similarly, Indonesian troll farms that spread fake news to influence elections have been exposed in the news (Paulo, 2019).

EMAs

The intended purpose of end-to-end encryption (E2EE) is to ensure that only the sender and receiver of a message can view a message. Some commonly used apps that use E2EE are WhatsApp (Meta-owned, U.S. corporation), Signal (non-profit), and Viber one-on-one and group chats (Rakuten-owned, Japanese
corporation). Some apps have elements of E2EE in that it can be turned on manually in some parts of the
world (Facebook Messenger) or selected from several options (Telegram public channels versus Telegram
private chats). The use of these apps is increasing around the globe (Mehner, 2020) and just as Facebook
and X once changed the media landscape, EMAs may further change the nature of communication.

Literature on the use of EMAs for the purpose of democratic organizing is nascent but increasing (Lokot,
2018; Moore-Gilbert and Abdul-Nabi, 2021) and has thus far shown that these spaces can be ideal for
activism given their affordances of intimacy and security, but also demonstrated that EMAs are hotbeds of
disinformation in many countries across the globe (Banaji, et al., 2019; Recuero, et al., 2020). Thus, it
becomes necessary to investigate this within ASEAN countries to gain a deeper understanding of the role of
EMAs in the global public sphere.

**Data collection**

In line with previous scholarship (Ong and Cabañes, 2018; Woolley and Guilbeault, 2017), this study relies
on qualitative, semi-structured interviews with both makers and trackers of political content on EMAs in
order to facilitate free-flowing conversations in which the insight of these interviewees can be uncovered.
The interviewees consisted of activists, experts, fact-checkers, journalists, politicians, and producers of
disinformation to glean insight from members of civil society (fact-checkers, organized activists), the state
(politicians and propagandists), and the public (experts who spoke on the general public). We began by
contacting experts, fact-checkers, and politicians in each region and then utilized snowball sampling to
contact hard to reach populations, such as activists and disinformation producers. We conducted 16
qualitative interviews from June 2021 to October 2021 virtually of interviewees in, from, or knowledgeable
about the spaces of Myanmar, the Philippines, and Indonesia. Our interviewees in the Philippines consisted
of two presidential communications employees (one of which was a social media specialist), a political
manipulation researcher, a former Facebook public policy director for global elections, and a
politician/cybersecurity expert. Our five interviewees in Indonesia consisted of an OSINT journalist, an
academic, the founder of a fact-checking organization, an employee of a fact-checking organization, and an
employee of a “public relations” firm, who we identified as a producer of political propaganda. In
Myanmar, our interviewees consisted of a Burmese journalist forced to flee the country, a journalist
knowledgeable about current events in Myanmar, an academic, and three activists fighting against
disinformation produced by the Tatmadaw: one founder of an organized activist network, and two
individual activists. Institutional Review Board approval was granted, and all interviewees provided
informed, verbal consent.

**Data analysis**

Interviews were analyzed using open, thematic coding (Braun and Clarke, 2006; Charmaz, 2006).
Following Charmaz (2006), we employed an “open-ended yet directed” analysis, in which we sought to
further understand the nature of the global public sphere through these case studies yet remained grounded
in the data [5]. We aimed to remain cognizant of our “active role ... in identifying patterns/themes” in the
data [6]. Referencing interview recordings, interview memos were written following each interview to
summarize the key takeaway observations from each interview. After three interviews in a region were
conducted, thematic memos were written to connect themes across interviews. The process of memo
writing allows for the consolidation of findings to identify trends or dissimilarities across regions of
interest.

**Findings**

Our analysis has elucidated trends that contribute to the understanding of how established theories of the
global public sphere and platform imperialism fare with regard to the emerging but increasingly relevant
platforms of EMAs in the three cases of Indonesia, the Philippines, and Myanmar. We compare the role of
The political use of encrypted messaging applications: Evidence from southeast Asia and its implications for the global public sphere

Our findings are that the three major players in the global public sphere — the public, the state, and civil society — exist simultaneously on EMAs but without equal power — the state’s ability to manipulate the public remains quite high in these spaces. Although interviewees did state that Meta products continue to dominate in two out of the three countries, we did not find that this had considerable influence on the nature of these platforms as public spheres, particularly given that in the case of WhatsApp, Meta monitors differently than it does Facebook or Instagram (Kimball, 2021). While Facebook and Instagram are open and public social media platforms in which content is accessible to Meta for the purposes of monitoring using both humans and AI (Facebook, 2023), WhatsApp’s end-to-end encryption means that Meta employees do not have access to the content on the platform. Yet ProPublica revealed that when users report content on WhatsApp, Meta moderators are able to see five contextual messages (Elkind, et al., 2021). However, WhatsApp remains primarily intimate and private in comparison to Facebook and Instagram.

(1) The role of the state

In Indonesia, our data indicate the use of EMAs for politically motivated propaganda by the regime. “Certainly, we are seeing coordinated efforts all the time in WhatsApp,” an Indonesian fact checker told us. This was supported throughout the interviews. One interviewee we spoke with runs a digital marketing firm, which is more akin to a troll farm. He is hired by political candidates (through a third party), among other clients, to falsely increase support for them online. He does this on traditional social media platforms such as Facebook and YouTube, as well as EMAs. On Facebook and YouTube, “buzzers” (what we know as “trolls” or people who run fake accounts) run 50 or so fake accounts that engage in orchestrated arguments over who the better candidate is: Candidate A or Candidate B. Eventually, the one they were hired to support wins out. The digital marketing associate told us that this specific strategy is not yet happening on EMAs, at least in his experience. He said the structure of the platforms makes it difficult to have these conversations and track the success of such strategies. When we asked him how he measures success, then, he responded, “My candidate, the people I represent, they win. I think that’s the only measurement.” Although it is clear that forces supporting the current regime propping the nation-state are venturing onto EMAs with their propaganda, it is also clear that EMAs hamper the previous tactics of state propagandists.

Instead, other strategies are used to influence public opinion on EMAs. The digital marketing associate we spoke with simply pushes out positive information about the candidate he’s hired to support. He writes 10 positive things about the candidate and pushes this out onto WhatsApp, and this is then multiplied by all of the fake accounts he runs, and all of the fake accounts run by his team. In this case, the propaganda is primarily textual, and he specifically targets extant networks of young people and religious people, he told us.

An expert on Southeast Asian troll farms highlighted a similar strategy that they called “negative campaigning.” “In Indonesia a really common kind of campaign during an election might be to put out on WhatsApp that the candidate is not very pious or ... in other instances saying well he’s cheated on his wife. You know that’s disinformation.” Disinformation is used to fuel propaganda about certain candidates, and to change public opinion about them. On WhatsApp, the expert said, provoking messages like the one above go viral, which aligns EMAs into the same trend that social media platforms like Facebook already established. The expert and the digital marketing associate told us it remains difficult to measure the success and impact of these strategies, but ultimately, it works: “Because my candidate, the people I
represent, they win. I think that’s the only measurement. They already won,” the associate said. Here we see the anti-democratizing power of the Internet and EMAs. Social media and EMAs are being used in Indonesia to actively and purposefully interfere with and influence democratic elections with the aim of perpetuating non-democratic procedures.

In the Philippines, EMAs may be the next frontier for political propaganda pushed by an aspiring authoritarian leader Rodrigo Duterte. Government officials who work in the communications office of the president articulated their use of Viber to target large swaths of the population and manipulate public opinion online. A cybersecurity expert told us that Viber has been “invaded by the government.” Government employees host Viber chats (they showed us one example with 2.6 million citizens) to share information about Duterte. This, on its face, is not problematic. However, Duterte’s use of troll farms to corrupt elections makes this concerning. The politicians we spoke to within Duterte’s government refused the notion that they use troll farms, but admitted to catering to millennials and younger generations by aiming to be “as entertaining as possible” to create a “ubiquitous” president. Here, then, the propaganda pushed out is a combination of text and other strategies, like memes, that cater to younger community members. The channels consist of huge numbers ofFilipino citizens aiming to receive necessary government information — they are then beset by Duterte propaganda. “I like to think that Filipinos want to go to social media as an escape,” the government employee in the social media communications role said, “so you must package your content in the most entertaining and trendiest way as possible to relate.” Rather than putting out legitimate information, information that paints Duterte in an exclusively positive light that plays on entertainment rather than facts is being pushed out on Viber and other Internet platforms.

At the same time Facebook remains central. One former Facebook employee told us, “The Philippines is one of the first places where we see Duterte’s campaign utilize Facebook to mobilize voters” and the government officials we spoke to told us they continue to use Facebook, in addition to EMAs, in their multi-layered strategy to foster support for President Duterte. Further, they are expanding into TikTok in an effort to target younger communities. The cybersecurity expert highlighted the potential dangers for the country’s democratic development when he reported that Duterte’s office requested a 1,000 percent increase for “social media associates” — a euphemism for troll farms who would also work on EMAs. In sum and confirming findings from Indonesia, EMAs are utilized by forces interested in hindering a further development into a democracy. These forces, aligned to the current regime and most importantly President Duterte, work towards keeping their own man in power and perpetuating existing power structures instead of promoting an exchange of ideas and accepting a variety of different opinions.

In the authoritarian state of Myanmar, EMAs are also used by state forces for political propaganda and disinformation in order to manipulate public opinion. The Internet writ large has been co-opted as a tool for restriction, threat, and state power by the military junta (the Tatamadaw) who has power in Myanmar. The Tatamadaw and their supporters run Telegram channels which spread pro-military propaganda and fake news stories, such as the story that Aung San Suu Kyi had been released. Here, a combination of textual and visual misinformation is used as well, as they spread out-of-context images and videos alongside other propaganda. That said, it’s supposedly easy for Myanmar citizens to tell this disinformation apart: “It’s really obvious for Myanmar people to understand which [Telegram] groups are pro-military and which groups are not,” a journalist told us. According to him, it continues to spread because the population in Myanmar will share it regardless of whether it’s true. “When someone found out that this news is fake news ... you know what the response of people was? ‘Whatever if it’s fake or accurate or true. We are happy to share that.’ So how can we confirm things? How can we fact check? Because people don’t really care about the facts and information.” This statement, though certainly not true for all citizens of Myanmar, reveals a problematic trend of sharing news based on emotion rather than legitimacy, allowing fake news and disinformation to spread through the communities.

However, our interviewees articulated that this is less likely to occur on EMAs than on traditional social media platforms, like Facebook, because the military tend to share disinformation within their own Telegram channels of military supporters, but not outside of it. In the case of Myanmar, the power of the state to control the population is much weaker on EMAs, where civil society are more able to speak freely,
than on traditional social media. As one activist told us: “I don’t bring my phone when I go out, because if [the Tatmadaw] check Facebook Messenger, I would be sentenced for life.” The military’s power to control EMAs comes primarily from being able to shut the Internet down entirely: “When the Internet is shut down, we can’t do anything,” another activist told us.

(2) The role of civil society

Just as the state propagandists struggle to measure success on EMAs, interviewees informed us that it is difficult for civil society groups to track the disinformation and propaganda on these platforms in Indonesia. A fact-checker informed us, “WhatsApp is very popular in Indonesia, and it operates in a different system than Facebook. We can see the kind of hoaxes in Facebook, we can report it, and also ask the platform to flag it or something like that. But who knows in WhatsApp because that closed group is encrypted ... So, it is our main concern right now.” It is also clear that any attempt of content moderation or fact checking is severely hampered by the characteristics of the platforms (such as end-to-end encryption) while at the same time EMAs also hamper the previous tactics of state propagandists. Another fact-checker told us: “One of the reasons we created [our company] is to avoid giving a chance for the government to censor the interceptions and things like that, spying, to our private messages, so we are very understanding about WhatsApp not sometimes submitting to requests from the government. But on the other hand, the encrypted nature of WhatsApp is also causing issues when we are trying to monitor the current situation.”

In the Philippines, we were again told that civil society struggles to fact-check on EMAs. The cybersecurity expert we spoke with highlighted that encryption affords and presumes a certain level of privacy, which fact-checking through content moderation may interfere with. They first must decide what constitutes fake news, he told us, “and as soon as you do that, that will have an impact on privacy.” He’s highlighted not only the difficulty of monitoring disinformation on EMAs due to encryption, but also the concern that this type of monitoring can interfere with the privacy that EMA users expect.

In Myanmar, EMAs there are not populated by fact-checking organizations, but there are large groups of young activists (regular citizens and students turned democratic activists) engaging in live fact-checking by countering misinformation they see on EMAs. “When I see false information, I have to tell the post owner,” one activist told us. They get trustworthy news from Indonesia media outlets on EMAs: “We communicate mostly on Signal and Telegram ... we all like Telegram more” and then share this real news with their followers. For these civil society groups, EMAs are a space to obtain and share real information, and counteract the bad.

The democratic activists in these channels also use EMAs to spread legitimate information about what’s happening in Myanmar beyond geographic borders. One activist we spoke to runs a large organization of young activists that work to share legitimate news about what the Tatmadaw is doing within Myanmar, but in the U.S. and other countries as well. He and his co-activists gather on Telegram in smaller groups to coordinate the strategies they will utilize on traditional social media (Facebook and X): “Telegram is safer,” he said, “because our Facebook page has a lot of followers.” Although traditional social media platforms are more dangerous, they are still useful for reaching large swaths of people within Myanmar and across the globe. By utilizing virtual private networks (VPNs) that hide or change their location, activists are able to create trending hashtags about Myanmar on X in other countries. EMAs are used to choose hashtags and coordinate timing for mass tweeting (what this activist calls “mass trending parties”) among thousands of young activists. This method of organizing makes EMAs a necessary element for transnational information spreading. Traditional social media are the mode through which the information has the most reach, but this would be largely impossible without the protection of encryption that EMAs afford.

(3) The role of the public

EMAs are widely used to connect family and friends in Indonesia, where groups are often created to connect people with shared interests. For instance, groups for individuals with a shared religion, ethnicity, or location provide a space for people with like-minded interests to engage. That said, such groups are often
infiltrated by disinformation, which as we’ve noted, is difficult to both monitor and correct. These threats are especially dangerous in these groups for two main reasons. First, these groups largely consist of users who know each other personally, making the information shared there feel trustworthy. Second, these groups are outwardly innocent — they are created to connect similar people for a likeminded cause. Hence, threats of false information are not on the radar for the majority of users in these groups. A fact-checker we spoke to said, “People [think] it’s a very good group, talking about religion all day, but from time to time [disinformation producers] will report their message there and they package it in very negative emotion and it spreads like wildfire. But normally to laypeople it seems to be a very innocent group.” This threatens the normative conception of a public sphere as that which promotes democracy — the general public may believe that they are in a space in which everyone’s voice has equal weight, but that is not the case when certain members are utilizing known communities and emotion to manipulate the public.

In the Philippines, WhatsApp and Viber are the most used EMAs, according to our interviewees. However, they are mainly used by “political junkies,” the former-politician-turned-expert told us. He explained that consequently, there is a lot of disinformation flowing between family and friends in these large, politically oriented chats, very similar to our findings in Indonesia. Further, the majority are not very interested in politics until “it’s time to vote.” Similar to Indonesia, this is a limit on how much we can consider these spaces public spheres. The public can speak freely, but they are at high risk of manipulation. “Biased perspectives displace civil, sensible, and sane political discourse,” we were told. Facebook use remains extremely high in this locale — traditional social media remains more popular than EMAs here for the general public.

In Myanmar, our interviews revealed that the general public has largely moved to Telegram from Facebook, where they previously congregated, following the coup. “I think Telegram has been quite useful there because Telegram does have some open architecture where you can be in a bit more of a public space,” a journalist told us. Telegram, then, not only provides an insular space for activists to organize but also a community space. Other interviewees articulated that disinformation is less prolific on Telegram than traditional social media, such as Facebook: a college student we spoke with said that she would prefer her parents and grandparents use Telegram for news over Facebook for this reason. As our research has uncovered this is due to three dynamics: first, the regime’s penetration of Facebook with disinformation; second, the fact that regime propagandists are more insular on Telegram than Facebook, mainly congregating and spreading disinformation in pro-military channels; and third, the civil society-led fact checking mechanisms that infiltrated EMAs in Myanmar.

(4) The role of the platforms

According to our interviews, Meta continues to dominate in Indonesia. “WhatsApp is pretty much the biggest one here,” an expert told us. This is backed up by statistical data: as of 2021, Indonesia is now Facebook’s third largest market after the United States and India (Statista, 2021b). The interviewees in this study articulated that Meta-owned Facebook and WhatsApp are both used to spread disinformation and propaganda. Meta products are the dominant platforms in the Philippines as well. In the Philippines, Facebook is widely used. “Really it’s all Facebook in the Philippines,” an expert told us. Only five percent of the Internet-using population utilizes Viber in comparison to the 99 percent that uses Facebook (Malig, 2021).

Myanmar is the outlier, as people have moved away from WhatsApp and Facebook Messenger, because Telegram and Signal are perceived as safer from government surveillance. When previously “the entire society [was] built on Facebook,” now “it’s almost as if [Myanmar] has left Facebook ... and has shifted towards that sort of private messaging format” an OSINT journalist told us. The drop in usage in Facebook in Myanmar following the coup (NapoleonCat, n.d.) is in line with what interviewees told us &mdash; Meta products are more dangerous than apps like Telegram and Signal. This appears to be a limit on Meta’s dominance in the region. When an authoritarian state limits access to or makes a platform dangerous for the people to speak freely on, people find a way to communicate somewhere else.
The control of the platform is somewhat limited on WhatsApp in comparison to Facebook and Instagram given that WhatsApp is E2EE. Typically, this means that only the sender and receiver can view the message, though on WhatsApp, if a user reports a message, WhatsApp is then able to read that message and several contextual messages (Kimball, 2021). In this instance, WhatsApp then has the power to ban a user. However, our participants were much more concerned about government surveillance than platform surveillance, and did not mention the potential alliance between governments and platforms, should WhatsApp choose to hand data over to authorities. The Burmese citizens were the only interviewees who told us that they believed Signal and Telegram to be safer than WhatsApp. Perhaps implicitly referencing this alliance, they believed that Signal and Telegram afforded more safety from governmental surveillance than WhatsApp did.

Discussion

Overall, our data indicate that EMAs complicate the idea of a global public sphere. All three elements of the public sphere (the state, civil society, and the public) are active in these spaces, and there is evidence of transnational communication facilitated by these platforms, some of which is democratizing because activists silenced by the government can be heard. However, the state retains considerable power to manipulate and control the public in all three countries. Platform imperialism is similarly both supported and challenged by our findings. Meta products remain largely dominant in Indonesia and the Philippines, but in the authoritarian country of Myanmar, the power of the state to threaten the public has caused the public to move to other platforms, thereby challenging the control of the formerly dominant Meta. At the same time, this may be due to the power wielded by Meta to surveil and expose its users when asked to by law enforcement. The power of the platform and the power of the state both limit the extent to which we can understand these platforms as democratizing and thus, as public spheres, yet this does not indicate that the global public sphere framework is entirely inapplicable in this context.

The state retains considerable power to manipulate the public in Indonesia, where paid political propagandists are working to create real support for candidates through falsifying mass support (what Woolley and Guilbeault [2017] call “manufacturing consensus”) on both traditional social media and EMAs. Although the public and civil society have voices in these spaces, they are also being influenced by those who are working to change their minds through manipulative tactics — including textual and visual disinformation. While the digital marketer we spoke with illuminated the challenges associated with spreading propaganda on EMAs, those who run these firms are innovative, and constantly adopting new strategies. In the future, EMAs may become more useful than social media, particularly as the rate of adoption of EMAs continues to grow (Statista, 2022b) alongside the use of EMAs for authoritarian ends (Trauthig, et al., 2023).

This aligns with a general challenge for democratic developments in Indonesia such as the government issuing a directive to police to combat alleged disinformation about the COVID-19 pandemic and criticism of the government and president’s response to it (Freedom House, 2021). Similarly, in the Philippines, some EMAs are largely the domain of the government, according to our interviewees. Duterte’s social media team are actively working to garner support for him, arguably taking over these spaces, in which it can be difficult for civil society organizations, such as fact-checkers, to operate. These cases support extant research demonstrating the power of the government to spread propaganda in digital spaces (Demirdis, et al., 2023). In Myanmar, the state power goes beyond manipulation to surveillance and the threat of violence, but this is interestingly not the case on EMAs as much as on traditional social media. EMAs are a safe haven for fact-checkers and activists to work and for the public to express their true opinions, with the knowledge that they can delete their activity after the fact. Although the Tatmadaw does have a presence on these apps, our interviewees reported that they are more insular on EMAs — spreading disinformation within their own groups, but not in others. Even when disinformation does make its way into activist or citizen groups, members are quick to counteract it. In this way, the strongest case for EMAs as a public
sphere is in Myanmar. While Myanmar is far behind Indonesia and the Philippines on the BTI (at 121, 47, and 54 respectively with 138 being authoritarian), civil society there are most active in democratic activism on EMAs, portraying a potentially counterintuitive insight as you’d expect countries that are further ahead on the transformation to democracy to use tools like EMAs more in pushing for democratic reforms and freedom of speech. This is an illuminating insight into the democratizing power of EMAs in authoritarian states.

Across the countries, WhatsApp was an especially fruitful place for disinformation to spread, challenging Meta’s purported goal of furthering global connectivity. We found that Meta products were less likely to be used for encouraging democracy than Telegram. Meta products remain widely used, especially in Indonesia and the Philippines. This is supported by data from Statista, showing that WhatsApp and Facebook Messenger are by far the most popular messaging apps across the globe (Statista, 2021d). This supports some form of platform imperialism, but aligns more closely with Bremmer’s (2021) idea that these corporations are not tied to the nation-state in which they originated but are more focused on their own profits and influence. These platforms may have originated in global world powers: America (WhatsApp and Signal), Russia (Telegram), and Japan (Viber), but that did not appear to play a role in the discourse in these spaces. Interestingly, Meta dominance is challenged by the power of the state to induce fear in their citizens: after the coup, Burmese fled from Facebook to EMAs for fear of surveillance by the military. While in our other countries of interest state manipulation limits the extent to which we can call EMAs a global public sphere, in the case of Myanmar, the state has facilitated the use of EMAs as a public sphere for those who are not free to speak publicly on other platforms. This calls into question the extent to which Meta products can be a public sphere in an authoritarian state, but provides support for EMAs like Telegram as having more qualities of a public sphere. As we grapple with information and communication equity in an increasingly globalized world, it is imperative that we consider the disinformation landscape in the Global South in tandem with democratic activism online as integral elements of the global public sphere.

Limitations and future research

This study’s strengths are also its limitations. A narrow selection of countries and qualitative interviews with varied participants allowed for deep conversations and investigation into the information landscapes of these three countries, but this study is hardly generalizable. The data in this study is limited, just as it is enhanced, by who we were able to speak to. Many people we contacted, especially politicians and producers, were unwilling to speak to Western researchers. Future researchers would do well to continue this work by interviewing activists, politicians, and producers as they are able to access those populations — keeping in mind local needs. Researchers should continue to watch these countries for evidence of activism and disinformation and explore the role that EMAs are playing as these events unfold. This work could be further expanded through quantitative methods, or through further interviews with actors in other ASEAN countries. Our study provides an exploratory window into the tensions between disinformation and activism on EMAs in ASEAN countries.

Conclusion

This study illuminated emergent communication trends on EMAs in Indonesia, the Philippines, and Myanmar. Characterized both by liberatory (democratic activism) and oppressive uses (state propaganda), EMAs in ASEAN countries are an integral element of political communication, and thus, the public sphere, even as they contribute to its disruption. In some ways they enhance the global public sphere through affording many-to-many communication across geographic borders, while at the same time, they remain an effective tool of state control and state manipulation, thereby enhancing the power of the state. Ultimately, they are tools of both liberation and oppression.
About the authors

Zelly C. Martin is a graduate research assistant at the Center for Media Engagement and a Ph.D. candidate in Journalism and Media at the University of Texas at Austin.
Direct comments to: zelly [at] utexas [dot] edu

Inga K. Trauthig is the head of research of the propaganda research lab at the Center for Media Engagement at the University of Texas at Austin.
E-mail: inga [dot] trauthig [at] austin [dot] utexas [dot] edu

Katlyn Glover is an affiliate fellow at the Center for Media Engagement and an M.A. graduate from the School of Journalism and Media at the University of Texas at Austin.
E-mail: katlyn [dot] glover [at] austin [dot] utexas [dot] edu

Samuel C. Woolley is an assistant professor in the School of Journalism and Media at The University of Texas at Austin and program director of the propaganda research lab and Knight faculty fellow at the Center for Media Engagement. He is an assistant professor (by courtesy) in UT’s School of Information and a research affiliate at the Project for Democracy and the Internet at Stanford University.
E-mail: swoolley [at] utexas [dot] edu

Acknowledgments

The authors thank the interview participants for their willingness to speak with us and for providing critical insights. 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 the Omidyar Network, Open Society Foundations, as well as the John S. and James L. Knight Foundation. We are sincerely grateful to Jacob Gursky and Alexandra Whitlock for their research contributions, and to Dr. Martin Riedl and Dr. Joseph Straubhaar for feedback and revisions.

Notes


References

The political use of encrypted messaging applications: Evidence from southeast Asia and its implications for the global public sphere


The political use of encrypted messaging applications: Evidence from southeast Asia and its implications for the global public sphere


Jonathan Corpus Ong and Jason Vincent Cabañes, 2018. “Architects of networked disinformation: Behind the scenes of troll accounts and fake news production in the Philippines,” *University of Massachusetts Amherst, Communication Department Faculty Publication Series*, number 74. doi: [https://doi.org/10.7275/2cq4-5396](https://doi.org/10.7275/2cq4-5396), accessed 18 January 2022.


doi: [https://doi.org/10.1080/1030431042000256108](https://doi.org/10.1080/1030431042000256108), accessed 2 December 2021.

doi: [https://doi.org/10.5210/fm.v26i1.10551](https://doi.org/10.5210/fm.v26i1.10551), accessed 2 December 2021.


Editorial history

Received 20 July 2023; revised 20 September 2023; accepted 23 September 2023.

This paper is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

The political use of encrypted messaging applications: Evidence from southeast Asia and its implications for the global public sphere
by Zelly C. Martin, Inga K. Trauthig, Katlyn Glover, and Samuel C. Woolley.
First Monday, volume 28, number 10 (October 2023).
doi: https://dx.doi.org/10.5210/fm.v28i10.13172