moz://a

Party Politics and WhatsApp Pramukhs: Messaging Platforms and Electoral Integrity in India

Divij Joshi

Doctoral Researcher at the Faculty of Laws, University College London

Mozilla Foundation

February 2024

The Indian General Elections are a massive enterprise. A projected 950 million people will be eligible to vote across the country in the 2024 elections, for 543 electoral constituencies,[1] featuring dozens of national political parties and tens of thousands of election workers and party operatives. On this massive stage of elections to the world's biggest democracy, what voters hear matters – and the landscape of political communication and media has been radically altered over the last decade.

Some more numbers – India has an estimated 760 million 'active' internet users,[2] accessing the internet more than once a month. 400 million of those are active on WhatsApp – the messaging platform's largest user base.[3] Several million others use alternative platforms like Facebook Messenger, Telegram and Signal. According to a study by the Reuters Institute, WhatsApp is the second largest, and Telegram is the fifth largest online platform for Indians to access news.[4] Flying under the radar of election authorities, media regulators and policymakers, these messaging platforms have now become a core feature of electoral communications and media in India.

Given its reach and popularity of use, it's no surprise that political parties, candidates, campaign management firms and the plethora of other actors involved in understanding and winning over the Indian electorate have adapted their strategies to utilise WhatsApp's potential for elections. Unsurprisingly, this has led to several familiar concerns around electoral media now being reflected in the use of messaging platforms – disinformation and hate speech are rampant, while the grey-market of personal information fuels targeted propaganda.

However, even as its importance has grown, there is surprisingly little study or analysis of the means by which the use of WhatsApp and other instant messaging tools are influencing elections, and the implications of the rising use of the platform. Moreover, there is little academic or political consensus on how legal or technological measures might address these issues. Despite the increasing influence of messaging systems, the focus of regulation and analysis of electoral influence through online platforms has been on social media platforms typically characterised by their 'open', public or broadcast nature, as opposed to the 'closed' systems characterised by messaging platforms.

If we want to make sense of how contemporary digital platforms are impacting electoral integrity and political communication, particularly in the Global South, we need to pay close attention to how messaging platforms are fundamentally altering media

---

[1] Press Trust of India, 'India Sees Six-Fold Jump in Voters since 1951; Total Electorate on January 1 Is over 94.50 Crore' *The Hindu* (5 February 2023) <https://www.thehindu.com/news/national/india-sees-six-fold-jump-in-voters-since-1951-total-electorate-on-january-1-is-over-9450-crore/article66473978.ece> accessed 18 December 2023.

[2] 'Internet in India, 2022 Report', IAMAI and KANTAR, <https://www.iamai.in/sites/default/files/research/Internet%20in%20India%202022_Print%20version.pdf>

[3] Manish Singh, 'WhatsApp Reaches 400 Million Users in India, Its Biggest Market' (*TechCrunch*, 26 July 2019) <https://techcrunch.com/2019/07/26/whatsapp-india-users-400-million/> accessed 18 December 2023.

[4] Nic Newman and others, 'Reuters Institute Digital News Report 2023', <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf>.

ecosystems, the dynamics of their use, and the challenges they pose for election authorities and media regulators. In this case study, I examine how WhatsApp's nature as a closed, extensible platform, along with its rise as a core communications infrastructure, are shaping electoral communication practices in India, why existing regulations have failed to contend with closed messaging platforms, and how platform governance practices can begin to comprehend and tackle these issues.

From Messenger to Platform to Super App? WhatsApp's Evolution in India

WhatsApp is a platform owned by Meta Platforms Inc., the US-based technology giant that also owns social media services like Facebook and Instagram. While initially released in 2009, the platform's growth rapidly expanded from the mid-2010s, owing to no small extent to the growing internet infrastructure in countries like India, Nigeria, Indonesia and Brazil, which remain its largest user bases. As smartphone internet connectivity saw massive growth, so did WhatsApp, and it quickly became the most widely used communications platform in countries across the Global South.

This period of growth in WhatsApp coincided with a major change in its security infrastructure – in 2016, WhatsApp made a decision to enable end-to-end encryption by default on its platform,[5] rendering it impossible to intercept communications shared between WhatsApp users, and widely considered a best practice in increasing the security and safety of online communications. Even as encryption improved communications security and trust, rolling out encrypted communications infrastructure at the switch of a button (or in this case, through a software update), raised the shackles of law enforcement and national security agencies around the world. Encrypted communications lead to what some term as the 'going dark' problem - an inability to monitor and intercept communications for surveillance purposes, and consequent challenges to investigating criminal activity or other unlawful conduct through the platform.[6] WhatsApp's switch to end-to-end encryption, meant, in effect, that law enforcement (or any other third-party, including ISPs or threat actors) would not be able to access private communications without access to a person's device. End-to-end encryption also implied that communications on WhatsApp could not be moderated in the same way as on other platforms, as there was no way to monitor and govern these systems. As discussed later, this particular bugbear is repeatedly raised in discussions around regulating WhatsApp and other encrypted messaging apps, and presents unique challenges for regulating online disinformation and hate speech.

Another event, from 2014, is crucial to understanding WhatsApp and its evolution. In 2014, the social media firm Facebook (now Meta Inc.) purchased WhatsApp in one of the

[5] Natasha Lomas, 'WhatsApp Completes End-to-End Encryption Rollout' (*TechCrunch*, 5 April 2016) <https://techcrunch.com/2016/04/05/whatsapp-completes-end-to-end-encryption-rollout/> accessed 18 December 2023.
[6] Ian Walden, '"The Sky Is Falling!" – Responses to the "Going Dark" Problem' (2018) 34 Computer Law & Security Review 901.

biggest acquisitions by technology companies.[7] Subsequent to this acquisition, WhatsApp has transformed from a one-to-one communications application into a broader 'platform ecosystem'. WhatsApp today is best conceptualised as a 'platform' – a system that allows for a range of activities between a diverse set of users, but the 'rules' of which are established centrally, usually by a private body, and enforced through the technical and organisational architecture of the platform.[8] In the case of WhatsApp, the decision-making rests with Meta, a corporate firm, which can unilaterally make changes to policy, extend new technological features on the app, and determine the extent and means of usage of the app. Even as it facilitates interactions between its various users (who are often also differentiated by WhatsApp as business users and 'regular' users), it places itself as the intermediary between these interactions, primarily, as a for-profit firm, to extract rent from these activities. These 'rents' have taken different forms – including monetising commercial use of the platform through its APIs, but also through the control and monetising of user data.[9]

Conceptualised as a platform, WhatsApp can also be studied through its 'extensibility' – the manner in which new features and services are made a part of its core data infrastructure. For example, WhatsApp has gradually transformed from its role as a one-to-one communications system, by incorporating public communication and broadcasting features, including the expansion of narrowcasting facilities like 'private' groups, where messages can be sent to up to 1024 individual accounts, a number which has consistently risen.[10] Similarly, WhatsApp regularly changes its privacy policy and the nature of information it shares with its parent company, Meta, and its other affiliates, like Facebook and Instagram.[11] As a platform, and part of a broader data ecosystem within its parent company, Meta, WhatsApp is able to leverage its position as a popular (in some cases, ubiquitous) messaging service to facilitate its growth and leverage its network in one domain into newer markets or features – for example, through its recent forays into digital payments, where its payments infrastructure was rolled out to its millions of users in India who had primarily been using WhatsApp as a messaging application.[12]

One-Step Forwards, Two Steps Back: WhatsApp's Use in Indian Elections

If you were to open a database of fact-checked political misinformation circulating on WhatsApp during the 2019 Indian General Elections, you would find not only laudatory

---

[7] 'Facebook to Buy Messaging App WhatsApp for $19bn' *BBC News* (19 February 2014) <https://www.bbc.com/news/business-26266689> accessed 18 December 2023.
[8] Thomas Poell, David Nieborg and José van Dijck, 'Platformisation' (2019) 8 Internet Policy Review 1.
[9] Techcrunch, 'WhatsApp to Share User Data with Facebook for Ad Targeting — Here's How to Opt out' <https://techcrunch.com/2016/08/25/whatsapp-to-share-user-data-with-facebook-for-ad-targeting-heres-how-to-opt-out/>.
[10] 'Communities Now Available!' (*WhatsApp.com*) <https://blog.whatsapp.com/communities-now-available> accessed 18 December 2023.
[11] Techcrunch, 'WhatsApp to Share User Data with Facebook for Ad Targeting — Here's How to Opt out' (n 9).
[12] 'WhatsApp Payments' (*WhatsApp.com*) <https://www.whatsapp.com?> accessed 18 December 2023.

claims of the achievements of political parties and politicians, but also hateful, often communally divisive rhetoric – using violent imagery and language to denigrate members of different castes and religions.[13] Such rhetoric is common to anyone following electoral politics in India, where hateful and violent speech is increasingly a tactic relied upon to rile up an electorate. Unsurprisingly, WhatsApp and other closed messaging platforms have proven to be a popular channel to circulate disinformation and hate speech with a view to gaining electoral advantage.[14]

WhatsApp's use in 'political' election-related communications in India first came to media attention in the 2019 General Elections. Reports noted that voters were turning to WhatsApp as a primary source of political news and information, and that political parties and their campaign teams were reaching out to potential voters by enrolling them in WhatsApp 'groups' and constantly sending a stream of election-related messages to them.[15] As per these reports, the messages consisted of a mix of regular campaign information as well as messages clearly intended to incite communal division and disinformation targeted at the leaders of opposing political parties. Reports also highlighted the circulation of specifically election-related disinformation – about particular candidates, or fake polls projecting victories for particular parties.[16]

First-party accounts from former party officials are revealing of the strategies involved in electoral communications through WhatsApp. Singh's account of working with the electoral communications team at the Bhartiya Janta Party, the party leading the current government in India, is particularly telling.[17] His account notes how the BJP's electoral propaganda machine functions as a professionalised, streamlined process, channelling data from various sources to profile and target potential voters through its massive network of party 'volunteers'. His account notes the central role that data analysis and the usage of personal data plays in collating and making lists of voters, classified according to caste, religion or other attributes that allow for easier targeting on WhatsApp groups. Personal information, including the names, phone numbers, National ID (Aadhaar) numbers and addresses of voters are easily available online, often published by electoral bodies themselves as voter lists, or otherwise gathered and sold by 'data brokers' to parties. This information is used to disaggregate lists of voters in a particular constituency into specific categories to be targeted according to campaigner's beliefs about information that is most likely to appeal to these voters.[18]

---

[13] Julio CS Reis and others, 'A Dataset of Fact-Checked Images Shared on WhatsApp During the Brazilian and Indian Elections' (2020) 14 Proceedings of the International AAAI Conference on Web and Social Media 903.
[14] Elonnai Hickock, 'The influence industry: Digital Platforms, technologies and data in the general elections in India.' Tactical Technology Collective 18 (2018).
[15] Andres Schipani, Madhumita Murgia and Stephanie Findlay, 'India: The WhatsApp Election' (5 May 2019) <https://www.ft.com/content/9fe88fba-6c0d-11e9-a9a5-351eeaef6d84>; 'In India, Facebook's WhatsApp Plays Central Role in Elections - The New York Times' <https://www.nytimes.com/2018/05/14/technology/whatsapp-india-elections.html>;
[16] Schipani, Murgia and Findlay (n 15).
[17] Shivam Shankar Singh, 'How to win an Indian election: What political parties don't want you to know', Penguin Random House India, (2019).
[18] Singh, *id.*

Similar strategies have been reported to be used by other major parties, including the Indian National Congress, who aimed to create 3,00,000 WhatsApp Groups in the 2019 elections to reach out to their base.[19]

The techniques of micro-targeting relies on data analytics capabilities provided, often, by private data analytics firms. A 2018 report looking into 'big data' analytics indicated how certain firms created electoral data repositories for use in elections which can help in generating both high-level electoral strategies, but also in targeting political communications to specific constituencies or demographics.[20] Indeed, reports indicate that the parent company of Cambridge Analytica, the SCL Group, which was at the heart of a major scandal involving the manipulation of voters on Facebook, may have been involved in building political parties' capabilities to target voters in India, as far back as the 2014 General Elections.[21]

The operation of voter targeting and the generation of propaganda, while relying on data analytics and mass messaging platforms like WhatsApp, relies on large amounts of volunteer labour. A party volunteer – called a WhatsApp *Pramukh* or a Whatsapp 'Leader' – is assigned to one or multiple lists to oversee the project of collating people into WhatsApp groups and ensuring a constant stream of pro-party messages. According to the BJP, in the 2019 General Elections, around 900,000 such *pramukhs* were assigned to these tasks – a number that will surely increase in 2024. The generation of campaign information is also streamlined, through the creation of social media 'War Rooms' and IT Cells, which essentially are tasked specifically with monitoring social media, generating propaganda, and creating dissemination strategies.[22]

The above examples indicate that electoral propaganda – hate speech and misinformation – including through WhatsApp, have become increasingly professionalised activities within political parties, existing within a broader ecosystem of the wide availability of personal data for behavioural targeting, and enrolling a whole set of technologies – including data analytics capabilities, social media, and personal communication services.[23]

Given the centrality of WhatsApp to the media ecosystem in India, a few studies have attempted to understand the social and political implications of its use, including its impact on electoral politics. A study by Narayanan et. al. based on information circulating on public WhatsApp groups (i.e. groups which are open to join based on

[19] Sunny Sen, 'Congress social media makeover bets on 3 lakh WhatsApp groups, data analytics, story engines' (7 Sept 2017) <https://archive.factordaily.com/congress-social-media-makeover/>
[20] Elonnai Hickock, 'The influence industry: Digital Platforms, technologies and data in the general elections in India.' Tactical Technology Collective 18 (2018).
[21] Itika Sharma Punit, 'Cambridge Analytica's Parent Firm Proposed a Massive Political Machine for India's 2014 Elections' (*Quartz*, 29 March 2018) <https://qz.com/1239561/cambridge-analyticas-parent-firm-proposed-a-massive-political-machine-for-indias-2014-elections>.
[22] 'For PM Modi's 2019 Campaign, BJP Readies Its WhatsApp Plan' (*Hindustan Times*, 29 September 2018) <https://www.hindustantimes.com/india-news/bjp-plans-a-whatsapp-campaign-for-2019-lok-sabha-election/story-lHQBYbxwXHaChc7Akk6hcI.html>.
[23] Anuradha Sajjanhar, 'Professionalising Election Campaigns', Economic and Political Weekly, 56(44).

publicly-available links), indicated significant amounts of 'junk news', as well as communally polarising messages circulating on groups with links to major political parties, including the BJP and the Indian National Congress.[24] Research by Garimella and Eckles has shown how multi-media (text and video) content is more likely to achieve 'virality' and contribute to disinformation, providing some more insight into what kinds of messages are more easily 'platformed' and how these contribute to campaign strategies.[25]

Some studies have also shown the limitations of current interventions against disinformation. For example, Reis et. al. have shown the limited influence of fact-checking in spreading certain kinds of political misinformation.[26] Badrinathan's study of WhatsApp use in state elections in India examines 'ground up' interventions to educate individuals about disinformation received on WhatsApp, and finds that counter-information strategies can often be unproductive in countering propaganda.[27] Detailed studies of WhatsApp use in India by scholars both how prevalent misinformation is, as well as the difficulty involved in reducing its spread. Despite the existence of a few studies of this nature, researching the dynamics of WhatsApp usage in India can be particularly difficult owing to its closed nature, particularly when seeking to understand the scale and nature of the distribution of disinformation and similar viral communications.

Left on Read: Electoral Integrity and the Failure of Platform Regulation in India

Political and election-related online media in India, of the kind described above, is governed through overlapping regimes of private content moderation practices and legal rules. It is important to unpack how these rules interact with the practices of private messaging platforms, and what implications these governance regimes can have.

In general, the practices of online platforms, including messaging platforms, are governed through India's Information Technology Act, 2000. Section 79 of the IT Act specifies that online 'intermediaries' which facilitate third-party communications, should not generally be liable for the content of that communication. However, this 'safe harbour' from liability is contingent on the intermediaries following specific rules laid down by the executive through delegated legislation. In 2021, these rules were updated

[24] Vidya Narayanan, et al. "News and information over Facebook and WhatsApp during the Indian election campaign." Oxford Centre for Democracy and Technology <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/05/India-memo.pdf>
[25] Kiran Garimella and Dean Eckles, 'Images and Misinformation in Political Groups: Evidence from WhatsApp in India' (arXiv, 19 May 2020) <http://arxiv.org/abs/2005.09784>.
[26] Julio CS Reis and others, 'Can WhatsApp Benefit from Debunked Fact-Checked Stories to Reduce Misinformation?' (arXiv, 5 August 2020) <http://arxiv.org/abs/2006.02471> accessed 18 December 2023.
[27] Sumitra Badrinathan, 'Educative Interventions to Combat Misinformation: Evidence from a Field Experiment in India' (2021) 115 American Political Science Review 1325.

to specifically regulate the activities of social media platforms as well as messaging platforms like WhatsApp.[28]

The Social Media Rules pose substantial concerns for civil liberties and the rule of law. Two aspects are particularly concerning. First, Rule 4(2) specifies that messaging platforms must, upon the receipt of a court order, "enable the identification of the first originator of the information" that has been circulated on its services. Rule 4(2) requires that messaging platforms implement traceability features into their services, which are incompatible with current standards for end-to-end encryption. According to WhatsApp, implementing traceability in this manner would compromise their ability to provide end-to-end encrypted communications.[29]

Second, Rule 3(b) states that social media intermediaries, the definition of which encompasses platforms like WhatsApp, must also comply with a host of content moderation rules, including notice and takedown rules for 'fake', 'false', or 'misleading' information identified by Government agencies known as Fact Check Units. Rule 3(b) provides a large amount of discretion to executive bodies, the Fact Check Units, to determine the truthfulness of content, and to force platforms to remove such information upon threat of losing their safe harbour.

The Government of India's response to the criticisms is that such regulations are necessary for the prevention of illegal and harmful speech on platforms. The Government has claimed, for example, that the traceability requirement for messaging platforms balances privacy interests in end-to-end encryption with law enforcement's legitimate interests in accessing information about illegal activity – claiming that traceability can be technically implemented without undermining the encryption of messages themselves. Similarly, the government has claimed that Fact Check Units are necessary to take on the problem of online misinformation. The constitutionality and legality of these provisions is currently being adjudicated before various constitutional courts around the country, and the arguments put forward on either side indicate the difficulties of regulating online speech and maintaining the balance of rights between freedom of expression, privacy and safe and responsible communications online.[30] That said, aspects of the IT Rules have impacted WhatsApp's practices on content moderation. WhatsApp has established a tiered grievance redressal mechanism, which includes providing users the option to 'report' other users by forwarding WhatsApp the content of their messages, which WhatsApp can then take action on. They have also

---

[28] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 <https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf>

[29] 'WhatsApp Moves Delhi HC against Traceability Clause in IT Rules, Calls It Is Unconstitutional | Technology News - The Indian Express' <https://indianexpress.com/article/technology/tech-news-technology/whatsapp-moves-delhi-high-court-over-traceability-clause-social-media-rules-7330558/> accessed 18 December 2023.

[30] *Id;* 'In Kunal Kamra's Petition in the Bombay High Court, the Government Undertakes Not to Constitute Its Fact Check Unit' (*Internet Freedom Foundation*, 27 April 2023) <https://internetfreedom.in/in-kunal-kamras-petition-in-the-bombay-high-court-the-government-undertakes-not-to-notify-its-fact-check-unit/>.

started publishing transparency reports on their moderation practices since the release of the new Rules, which indicates that they ban millions of users every month based on user complaints mechanism as well as on 'proactive' measures to identify problematic content and accounts.[31]

Apart from media regulation, political-electoral messaging increasingly depends on targeting individuals based on personal information like caste, gender and religion, among others, and combining this information with phone numbers to target people through messaging platforms.[32] Personal information of this nature is a readily available commodity for data brokers and party agents to collate and combine into lists which allow targeted propaganda and electoral messaging, owing to a mix of lax security standards as well as the lack of data protection and privacy regulations that allows individuals to have control over the use of their personal information. While the Government of India has now adopted a regulation - the Digital Personal Data Protection Act, 2023 – its utility is untested, and its various exemptions (such as for 'publicly' available data) mean that there are several loopholes which can be exploited by data brokers who make personal data available for targeted use in elections.[33]

Another relevant body of law relates to the regulation of communications specifically during elections. Elections in India are monitored by a constitutionally-established and formally independent institution called the Election Commission of India ("ECI"), which monitors, among other things, the period of 'electoral silence' during which campaigning is not permitted, as well as establishing a 'model code of conduct' - a voluntary agreement to be followed by participating political parties, and monitoring and establishing limits on election expenditure, including so-called 'paid news' – media that is paid for by a candidate or party.[34]

Despite being the constitutional authority to oversee elections, the ECI has not been able to effectively regulate the use of social media or messaging platforms during elections. Shortly before the 2019 General Elections, the ECI established a 'voluntary' code of ethics for social media platforms,[35] which according to reports, was established in lieu of stricter legal regulations after lobbying by social media firms including Facebook.[36] According to this code, social media firms voluntarily agreed to take down content privately flagged by the ECI, which violated legal norms. There were no regulatory mechanisms to monitor or ensure compliance with this code, nor any

---

[31] 'WhatsApp Monthly India Reports' (*WhatsApp.com*) <https://www.whatsapp.com/legal/india-monthly-reports>.
[32] Singh (n19); Hickock (n14).
[33] Sayantan Chanda, 'Data Privacy And Elections In India: Microtargeting The Unseen Collective', Indian Journal of Law and Technology, 18(1), (2022).
[34] Election Commission of India, 'Model Code of Conduct', <https://eci.gov.in/faqs/mcc/model-code-of-conduct-r15/>
[35] Press Information Bureau, India, 'Social Media Platforms Present "Voluntary Code of Ethics for the 2019 General Election" to Election Commission of India' <https://pib.gov.in/newsite/PrintRelease.aspx?relid=189494>.
[36] 'Facebook Convinced Poll Panel to Settle on a Voluntary Code' (*Hindustan Times*, 22 November 2021) <https://www.hindustantimes.com/india-news/facebook-convinced-poll-panel-to-settle-on-a-voluntary-code-101637549263683.html>.

consequences for failing to adhere to it. The ECI's approach towards online platforms also suffers from a lack of clarity about the scope of its powers over social media regulation, particularly in the case of platforms like WhatsApp. For example, as recently as the 2023 state elections in Karnataka, the ECI was unclear on whether its powers to monitor the electoral silence period extended to campaigning over social media platforms.[37]

Apart from the legal and regulatory regimes, an important vector of governance of messaging platforms is through the policies established and overseen by the platform itself. Indeed, the policies and practices of platforms may be the most influential form of governance, particularly in the absence of clear regulation. In the case of WhatsApp in India, for example, WhatsApp has repeatedly claimed it is cognizant of the problems of hate speech and disinformation on its platform, and has announced that it takes steps to deter such behaviour.

For example, WhatsApp has implemented limits on 'forwarding' content – including labelling certain kinds of content, as well as preventing simultaneous broadcasts across groups.[38] They also implement spam filters to block 'bots' or accounts that might be responsible for mass automated broadcasts. In the context of elections specifically, senior WhatsApp employees have previously claimed that they are aware of political parties 'abusing' WhatsApp to send automated messages, and would take steps to ban such abuse.[39] WhatsApp also claims to ban political parties or political candidates that send WhatsApp messages to users 'without permission.'[40] WhatsApp has also 'partnered' with accredited fact-checking organisations in India, to make it easier for individuals to verify the veracity of information they have received on the platform, by forwarding suspect information to specific fact-checker accounts.[41]

---

[37] '"Poll Code Does Not Cover Social Media Platforms"' *The Times of India* (10 May 2023) <https://timesofindia.indiatimes.com/elections/assembly-elections/karnataka/news/poll-code-does-not-cover-social-media-platforms/articleshow/100113022.cms?from=mdr>.

[38] 'About WhatsApp and Elections' WhatsApp Help Center, <https://faq.whatsapp.com/518562649771533>.

[39] 'Political Parties In India Abuse WhatsApp Before Elections: Top Executive' (*NDTV.com*) <https://www.ndtv.com/india-news/political-parties-in-india-abuse-whatsapp-before-elections-top-executive-carl-woog-1989443>.

[40] WhatsApp (n37).

[41] 'IFCN Fact-Checking Organizations on WhatsApp | WhatsApp Help Center' <https://faq.whatsapp.com/505912054085566?helpref=faq_content>.

Closing the Accountability Gap for Closed Messaging Platforms

Closed platform ecosystems like WhatsApp and Telegram have led to new patterns of media consumption and sharing. The available evidence, from India, as well as Brazil,[42] Indonesia,[43] Nigeria,[44] as well as among diaspora communities,[45] clearly indicates that WhatsApp and other messaging services, particularly Telegram, are increasingly providing the infrastructure for electoral propaganda and politically-motivated hate speech to circulate. Even though it may not be possible to clearly ascribe specific developments in electoral politics to the rise of platform-mediated communications, it is clear these platforms are increasingly becoming prominent features of contemporary political and electoral media landscapes.

What lessons can we learn from the recent history of messaging platforms usage during elections in India and elsewhere? What should policymakers, civil society and platforms keep in mind for the upcoming spate of elections around the world?

It is important for policymakers to take action. For one, all relevant stakeholders need to firmly commit to the right to privacy, including the right to private communications, and abstain from undermining encryption. A number of recent proposals, from policymakers, researchers, civil society and platforms, have suggested that platforms can offer 'workarounds' to encryption through mechanisms like client-side scanning, which would scan messages before they are encrypted, in order to filter out unlawful or harmful speech. These proposals rehash age-old debates about only allowing 'good actors' access to private communications or (unchecked) power over content governance. Yet, the counter-arguments remain the same - implementing such proposals can severely undermine communications privacy, safe use of the internet, the integrity of communications, and open up very real possibilities of abuse. **The Government of India must commit to not undermine encryption and protect the constitutionally recognised fundamental right to privacy.**

At the same time, we must acknowledge that closed messaging platforms are particularly appealing for bad actors to spread harmful and illegal communications, owing to the lack of any meaningful content governance in such systems, including the lack of legal oversight or even internal governance mechanisms. Tackling the issue requires new ways to approach closed-messaging platforms as media infrastructure for different kinds of communication. In particular, **messaging platforms like WhatsApp must take steps that acknowledge how their features are providing the infrastructure for propaganda, disinformation and hate speech, particularly**

---

[42] Tactical Tech Collective, 'Brazilian Elections and the Public-Private Data Trade' <https://ourdataourselves.tacticaltech.org/posts/overview-brazil/>.
[43] Kate Lamb, 'Fake News Spikes in Indonesia Ahead of Elections' *The Guardian* (20 March 2019) <https://www.theguardian.com/world/2019/mar/20/fake-news-spikes-in-indonesia-ahead-of-elections>.
[44] Tactical Tech Collective, 'Personal Data and the Influence Industry in Nigerian Elections' <https://ourdataourselves.tacticaltech.org/posts/overview-nigeria/>.
[45] Kayo Mimizuka Trauthig Inga, 'WhatsApp, Misinformation, and Latino Political Discourse in the U.S. | TechPolicy.Press' (*Tech Policy Press*, 25 October 2022) <https://techpolicy.press/whatsapp-misinformation-and-latino-political-discourse-in-the-u-s>.

during elections, when trust in democratic institutions is vital to maintain. In doing so, WhatsApp and other closed messaging systems could develop distinct rules for communications intended to be widely broadcast, and those intended to be for limited circulation. This is particularly important given how messaging platforms are increasingly used for broadcast purposes, conflating the lines between 'social media' and private messaging uses. WhatsApp, for example, could and should consider what effective limits on 'viral' forwards look like, including limiting how many forwards can be received by groups, limiting group size, or changing how (and how many) individuals are added to group accounts.

Platform interventions should also be guided by a legal framework, instead of operating entirely of their own accord. Voluntary arrangements are generally insufficient in ensuring compliance, platforms must be bound to clear legal frameworks that allow election authorities to monitor platform compliance with election rules, including political ad spending or communication through features like the WhatsApp Business API. Platform regulations for closed messaging platforms could evolve to specifically empower counter-propaganda and fact checking through independent bodies meeting specified criteria (instead of providing the power to fact check to government executive agencies). **The Government of India should consider implementing legislative mechanisms which require platforms to share certain forms of data about their content moderation practices with regulators, researchers or publicly**. This could be similar to the DSA Transparency Database recently implemented in the EU.

More broadly, regulation must also target the broader ecosystem that enables the targeting of voters, including how personal information is collated by campaigners, for example, through clearer rules on the collection, sharing and use of personal data, including information that is ostensibly 'publicly' available through voter lists. **The Government of India must commit to implementing, enforcing and strengthening privacy mechanisms in the Digital Personal Data Protection Act, 2023, as well as ensure the privacy and security of government public databases, which have been the subject of several data breaches.**

Apart from focussing on platforms themselves, election authorities are well placed to act against the broader ecosystem of electoral communications that utilises messaging platforms as vectors of disinformation and hate speech. Election authorities must be empowered to act against parties that breach election rules on 'paid news' and electoral silence, including monitoring of electoral spending on campaigns that rely on targeting voters through closed messaging platforms. Independent election authorities like the ECI must be empowered to act against disinformation and practices that undermine electoral integrity. **In India, the ECI's powers to ask for information from and monitor action taken by closed messaging platforms during elections should be clarified, and the scope of its powers under the Representation of the People Act should be appropriately amended to strengthen its independence and allow them to effectively take action against violations of 'paid news' and other forms of electoral malpractice through online platforms.**

Finally, greater research into the nature of communication and media practices on closed messaging platforms needs to be encouraged. While some quantitative methodologies are evolving to study closed platforms at scale, and qualitative researchers are studying the issue through ethnographic work or policy analysis, there is a large vacuum of research on communicative practices on WhatsApp that can feed into policies on electoral media, particular from the Global South. **Platforms themselves should do more to open up metadata and other information available with them that may be useful for researchers, in ways that maintain the privacy of their users, including, for example, information about internal moderation practices or about design interventions made by platforms.**