

To,

Shri Rajiv Kumar,
Chief Election Commissioner,
Election Commission of India
Email: cec@eci.gov.in

Shri Gyanesh Kumar,
Election Commissioner,
Election Commission of India
Email: ecgk@eci.gov.in

Shri (Dr.) Sukhbir Singh Sandhu,
Election Commissioner,
Election Commission of India
Email: ecsss@eci.gov.in

Re: Technology accountability and digital platforms

Respected Members of the Commission,

The undersigned Indian civil society organisations are writing to the Election Commission of India (“ECI”) to voice our collective concerns about the integrity of the upcoming general elections to the Lok Sabha scheduled to commence on April 19, 2024. Listed below are our 4 major concerns and appeals to the Commission on the broad theme of the role of technology in affecting electoral process and outputs. Each of these has been elaborated on in detail in the attached Annexure.

1. **Online campaigning and surrogate advertisements:** Expenditure on surrogate advertising and targeted online campaigns by political actors to influence voter perception and beliefs are not under adequate scrutiny. The ECI must increase the accountability of political parties and digital platforms by adopting internationally acceptable, rights-respecting standards for regulating political expenditure on online ads and targeted campaigning.
2. **Use of emerging technologies such as deepfakes:** The use of generative AI technology (particularly deepfakes) by political actors with the intent to influence voter perception and impact electoral outcomes raises urgent concerns. The ECI must introduce measures to increase the accountability of political actors who deploy generative AI with the intent of influencing voter perceptions and political narratives.
3. **Inadequacies of the Voluntary Code of Ethics:** The Voluntary Code of Ethics is non-binding, has no legal force, and was drafted without any transparency and input from civil society. Lower standards are applied to digital platforms in India as compared to other jurisdictions, there is no monitoring of compliance by these platforms, and there is a lack of redressal for voters in case of non-compliance. The ECI should initiate a transparent and participatory process to arrive at a Model Code of Conduct (“MCC”) to be followed by political candidates and digital platforms - with clear enforcement guidelines and reporting mechanisms.
4. **Voter surveillance:** The use of facial recognition and video surveillance technology at polling booths can deter the right to vote without fear or coercion, may violate the right to privacy, and is antithetical to a free and fair election. The ECI should initiate a careful reevaluation of the implementation of surveillance technologies in electoral processes and assess it against strict standards of legality, necessity and proportionality.

Digital Platforms and Elections

The role of digital platforms like social media companies in elections has grown and changed since its first use in the 2014 election campaign.¹ Since then, internet connectivity and social media use in India have grown by leaps and bounds, even as overall literacy and digital literacy have remained much the same.² Digital platforms today have the ability to influence people's behaviour on an enormous scale, and, therefore, also the election process. Ahead of the 2024 general elections, this influence on electoral outcomes has to be scrutinised closely, alongside the threat India's democracy faces from the digital realm.

The existence of divisive and polarising content on digital platforms in India have been a major issue for several years, with sufficient evidence on how the design of the platforms facilitates hateful content.³ This hate speech has a direct throughline with representatives of the ruling party and various influencer ecosystems funded by them.⁴ Further, monetisation of hateful content portrays a worrying trend for India's democracy.⁵ The digital platforms have often been called out for lack of accountability to their Indian users and their inaction or often delayed response towards illegal content.⁶ This lack of transparency and accountability is especially disappointing in comparison to the platforms' prompt response and improved measures in international jurisdictions such as the United States.⁷

Recently released report by AltNews revealed that political parties are spending large sums on online advertisements, including "proxy" advertisements by publishers/ pages who support a particular party but do not have any official affiliation with the party.⁸ Their analysis of the Meta Ad Library data revealed that the Bharatiya Janata Party ("BJP") has spent the most on political advertisements, but the expenditure on advertisements by BJP's proxy pages exceeded that on their official advertisements. Such proxy ads were found to primarily "*target opposition parties, amplify contentious narratives, touch upon divisive issues, and exploit prejudices*". The report also exposed inadequacies in the data released by Meta, with certain ads by BJP's proxy advertiser not featuring in their database despite other ads by the same advertiser being listed. Such lack of accountability of political parties due to irregular tracking of their expenditure on proxy ads lead to concerns about electoral transparency.

¹ Taberez Ahmed Neyazi, Anup Kumar and Holli Semetko, 'Campaigns, Digital Media, and Mobilization in India' (Research Gate, April 2016) https://www.researchgate.net/publication/301221389_Campaigns_Digital_Media_and_Mobilization_in_India.

² Srajan Girdonia, India's Digital Literacy: Challenges, Progress and the Way Forward (The Processor, April 2023) <https://theprocessor.in/policy-puzzles/government-initiatives-to-promote-digital-literacy>

³ Sheera Frenkel and Davey Alba, 'In India, Facebook Grapples With an Amplified Version of Its Problems' (The New York Times, October 2023) [In India, Facebook Grapples With an Amplified Version of Its Problems](https://www.nytimes.com/2023/10/02/technology/facebook-india.html)

⁴ Major Human Rights and Internet Watchdog Organizations Sign On to Demands for #AuditFBIndia' (GPAHE, September 2020) [Major Human Rights and Internet Watchdog Organizations Sign On to Demands for #AuditFBIndia - Global Project Against Hate and Extremism](https://www.gpahe.org/2020/09/20/major-human-rights-and-internet-watchdog-organizations-sign-on-to-demands-for-auditfbindia/)

⁵ Gerry Shih and Pranshu Verma, 'He live-streamed his attacks on Indian Muslims. YouTube gave him an award' (The Washington Post, September 2023) [He live-streamed his attacks on Indian Muslims. YouTube gave him an award.](https://www.washingtonpost.com/technology/2023/09/20/youtube-gave-him-an-award-for-live-streaming-attacks-on-indian-muslims/)

⁶ 'Facebook continues to turn a blind eye to hate speech' (CJP, April 2021) [Facebook continues to turn a blind eye to hate speech | CJP](https://www.cjp.org/2021/04/01/facebook-continues-to-turn-a-blind-eye-to-hate-speech/)

⁷ Hibaq Farah, 'This article is more than 6 months old Social media firms 'not ready to tackle misinformation' during global elections' (The Guardian, February 2023) [Social media firms 'not ready to tackle misinformation' during global elections](https://www.theguardian.com/technology/2023/02/02/social-media-firms-not-ready-to-tackle-misinformation-during-global-elections)

⁸ Abhishek Kumar, 'BJP way ahead of others in political ad spending on Meta; proxy pages spent more than official ones' (Alt News, 02 April 2024) <https://www.altnews.in/bjps-proxy-pages-spending-more-money-in-political-ads-on-facebook-and-instagram-than-official-pages/>

These kinds of advertisements are part of a largely unregulated and non-transparent ecosystem called “surrogate advertising”. An analysis of Meta’s ads library by The Indian Express revealed that of the top 20 advertisers on Facebook and Instagram during March 17 to 23, 2024 (the first week of the MCC being applied), seven accounts ran ads favourable to the BJP and no other advertiser in the top 20 list ran surrogate ads for any other political party.⁹ As per an investigation released by BoomLive, over ₹3.7 crore was spent on surrogate ads on Facebook in the month of March 2024 alone, mainly targeting the opponents of the BJP.¹⁰ The investigation also found these surrogate pages sponsoring posts containing “hate speech, misinformation, and propaganda” to target the ruling-BJP’s political rivals along with minority communities in India. Upon asking Meta about existence of such ads which violate electoral guidelines, Meta’s spokesperson shared that although they review and take action against them, it becomes the advertisers’ responsibility to “*comply with any applicable electoral and advertising laws and regulations in the countries they want to run ads in*”. Previous analysis of political ads by The Reporters’ Collective and ad.watch also revealed the inadequacies of the existing application of law to curb the flourishing surrogate advertising ecosystem.¹¹

In 2013, the ECI instructed all Chief Electoral Officers and national as well as state recognised political parties and their candidates to include all expenditure on campaigning, including expenditure on advertisements on digital platforms.¹² The letter included clarification that such expenditure would include “*payments made to internet companies and websites for carrying advertisements and also campaign related operational expenditure on making of creative development of content, operational expenditure on salaries and wages paid to the team of workers employed by such candidates and political parties to maintain their social media accounts, etc.*” Expenditure by political parties, through formal and informal means, is generally difficult to track. Unlike official expenditure for offline campaign, digital media campaigns are often difficult to analyse as both the amount of money involved and the methodology used for targeting remain in the background, and are the exclusive domain of the digital platforms. Here, digital platforms play a key role in identifying and tracking the money spent on digital campaigning through official and unofficial channels.

A much more broad-based campaign, involving multiple stakeholders – political parties, civil society, and the Election Commission - is necessary to ensure that these platforms are not used to determine electoral results. Several interventions, from various stakeholders, are required to regulate targeted online campaigns and surrogate advertising. Considering that the watch-dog role of the media is quite vital in today’s democratic and political landscape, we ask for proactive

⁹ Soumyarendra Barik, “Lok Sabha elections 2024: In first week of poll code, surrogate ads on Meta give BJP early start”, Indian Express, March 30, 2024.

<https://indianexpress.com/elections/in-first-week-of-poll-code-surrogate-ads-on-meta-give-bjp-early-start-9241012/>.

¹⁰ Archis Chowdhury, ‘BJP Opponents Targeted With Surrogate Ads Worth ₹3.7cr On Facebook In March’(Boom, April 2024) <https://www.boomlive.in/news/bjp-congress-tmc-ysrcp-modi-facebook-ad-library-surrogate-ads-march-lok-sabha-elections-24820>.

¹¹ Maroosha Muzzaffar, ‘How Facebook’s Rules Allow Pro-BJP Advertisers to Escape Stricter Scrutiny’ (The Wire, September 2020) [How Facebook’s Rules Allow Pro-BJP Advertisers to Escape Stricter Scrutiny](https://www.thewire.in/news/facebook-pro-bjp-advertisers-escape-scrutiny/) Exclusive: Network of shadow Facebook pages Abhishek kumar, ‘Network of shadow Facebook pages spending crores on ads to target Oppn are connected to BJP’ (Alt News , April 2023) [spending crores on ads to target Oppn are connected to BJP - Alt News](https://www.altnews.in/news/network-of-shadow-facebook-pages-spending-crores-on-ads-to-target-oppn-are-connected-to-bjp/).

¹² Compendium of Instructions On Election Expenditure Monitoring by the Election Commission of India, January 2024, Document 6 – Edition 10, Page 191. <https://www.eci.gov.in/eci-backend/public/api/download>.

intervention into electoral law and the adoption of internationally acceptable, rights-respecting standards for regulating online political expenditure and campaigning.¹³

Inadequacies of the Voluntary Code of Conduct

We note that the Election Commission's consultations with digital platforms and the Internet and Mobile Association of India ("IAMA") have culminated in the adoption of a Voluntary Code of Ethics ("the Code") effective from March 20, 2019. We understand that the digital platforms have committed to bringing about a certain measure of transparency in respect of political ads, instituting a mechanism for handling complaints of misuse, and enforcing the 48 hour silence before the end of poll on social media. However this Code has been drafted without any transparency, public inputs, or civil society engagement. The participation of all key stakeholders is of crucial importance in a consultation of this nature. We also note that the Code is not binding, has no legal force, and does not address the larger issues that we have articulated in this note. Additionally, the Code is severely inadequate on three counts.

1. **Stronger Commitments Outside India:** The same social media companies offer more commitments and disclosures to federal regulatory authorities and users in other jurisdictions including the United States, Brazil, and the European Union.
2. **Lack of Transparency and Accountability on Compliance:** There is virtually no systematic information in the public domain on the monitoring of compliance of companies with the Code.
3. **Lack of Redress for Citizens:** Citizens, political parties and the electoral process all suffer from non-compliance by social media companies with the Code. There are no avenues for citizens and political parties to report violations to the Code, either to the Election Commission or to social media companies.

Conversely, there is ample evidence of explicitly forbidden speech detailed in the Code allowed to flourish on social media. This includes aggravating existing differences, creating mutual hatred, causing tensions, criticising the private lives of politicians and appealing to the caste and communal divide.¹⁴ International jurisdictions like the European Union, United States, and Brazil have put in place strong commitments to be followed by political parties and social media companies around elections and also institutionalised mechanisms for strict monitoring of these

¹³ Holly Ann Garnett, 'Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity' (*Mary Ann Liebert, Inc.*, 15 June 2020) <https://www.liebertpub.com/doi/10.1089/elj.2020.0633>.

¹⁴ Apoorva Mittal, 'Is it time to update Model Code of Conduct? Adapting to tech-driven election landscape', (Economic Times, 14 January 2024) <https://economictimes.indiatimes.com/news/politics-and-nation/is-it-time-to-update-model-code-of-conduct-adapting-to-tech-driven-election-landscape/articleshow/106818159.cms>. See Also: EC asks parties not to put out ads in Bihar that can create 'mutual hatred', (Economic Times, 31st October 2015) <https://economictimes.indiatimes.com/news/politics-and-nation/ec-asks-parties-not-to-put-out-ads-in-bihar-that-can-create-mutual-hatred/articleshow/49611825.cms>.
See also: 'Desist from criticising private life of rivals, politicians urged', (The Hindu, 8 March 2016) <https://www.thehindu.com/news/national/tamil-nadu/desist-from-criticising-private-life-of-rivals-politicians-urged/article8325581.ece>.
See also: 'Casteism, communal appeal at core of political parties' strategy in UP polls' (Economic Times, 8 February 2022) <https://economictimes.indiatimes.com/news/elections/assembly-elections/uttar-pradesh/casteism-communal-appeal-at-core-of-political-parties-strategy-in-up-polls/articleshow/89424890.cms>.

commitments.¹⁵ India needs to enforce a robust, Model Code of Conduct, specifically targeting threats to electoral integrity in the digital realm.

Emerging Technologies

One evolving and emerging technology that has contributed to altered content in the information ecosystem is deepfakes – digital content that has been manipulated or synthesised using deep learning models to appear authentic – which may be circulated through various forms of media.

Instances of creation, use, and dissemination of such AI-generated synthetic media have been increasing in the country, with use cases ranging from language translation to financial fraud.¹⁶ Prominent political representatives and parties are increasingly becoming comfortable with sharing AI-generated political content on social media through official accounts, often without any disclosure.¹⁷ Given the low rates of media and information literacy as well as the divisive politics in the country, the severity of threats posed by AI-generated synthetic media must be acknowledged at the earliest, especially in the election context.

While much of the conversation around deepfakes is centred around efforts undertaken by and regulation of the platforms, limited attention is paid to the political actors leveraging such technology for the weaponisation of content.¹⁸ ECI's current response to voter influence through AI-generated synthetic media is extremely limited. Detection of such media, for instance deepfakes, in regional languages is further restricted. The ECI may take inspiration from a bipartisan bill titled "Protect Elections from Deceptive AI Act" that was introduced in the United States Senate in September 2023 to prohibit the distribution of "*materially deceptive AI-generated audio, images, or video relating to federal candidates in political ads or certain issue ads to influence a federal election or fundraiser*".¹⁹ This bill would amend the Federal Election Campaign Act, 1971 to allow federal candidates targeted by this materially deceptive content to have content taken down and enables them to seek damages in federal court.

¹⁵ 'Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech', (LOC, 28 June 2021) <https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/>.

See also: 'First national Code of Conduct on online political advertising in the European Union signed by Dutch political parties and global online platforms', (IDEA, 9 February 2021) <https://www.idea.int/news/first-national-code-conduct-online-political-advertising-european-union-signed-dutch-political>.

¹⁶ See: Nilesh Christopher, "We've Just Seen the First Use of Deepfakes in an Indian Election Campaign", Vice, February 18, 2020, <https://www.vice.com/en/article/igedjb/the-first-use-of-deepfakes-in-indian-election-by-hjp>; Bismee Taskin, "Celeb deepfakes just the tip, revenge porn, fraud & threat to polls form underbelly of AI misuse", The Print, November 13, 2023. <https://theprint.in/india/celeb-deepfakes-just-the-tip-revenge-porn-fraud-threat-to-polls-form-underbelly-of-ai-misuse/1841666/>;

Subham Tiwari, "India among top targets of deepfake identity fraud", India Today, December 05, 2023. <https://www.indiatoday.in/india/story/india-among-top-targets-of-deepfake-identity-fraud-2472241-2023-12-05>.

¹⁷ Nilesh Christopher, "Inflection point': AI meme wars hit India election, test social platforms", AlJazeera, March 08, 2024. <https://www.aljazeera.com/economy/2024/3/8/ai-meme-wars-hit-india-election-test-social-platforms>.

¹⁸ Disha Verma and Tejasi Panjiar, "Read our Open Letter to Electoral Candidates & Parliamentary Representatives on the Impact of Deepfakes on Electoral Outcomes", (Internet Freedom Foundation, February 26, 2024). <https://internetfreedom.in/open-letter-on-deepfakes/>.

¹⁹ Khlobuchar News Releases, September 2023 <https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=AF782E4C-C2C9-4C7C-8696-374F72C03F90>

Voter Surveillance

At multiple times in the past few years, ECI has shown interest in using surveillance tools and facial recognition technologies (“FRT”) at polling booths to ensure the smooth conduct of elections. However, such interventions are antithetical to a free and fair election, with significant privacy and accuracy concerns.²⁰

The deployment of video surveillance equipment is likely to hurt individual fundamental rights, notably the right to privacy and dignity and the right to vote without fear or coercion and may also be perceived as voter intimidation.²¹ Earlier experimentation with implementing FRT in the polling process in India has revealed that such an operation can be plagued with logistical issues and inaccuracies, resulting in a “chilling effect” on enfranchisement and a decrease in voter turnout.²²

The facial data stored from FRT systems is also far more vulnerable than any other biometric identifier, as it can facilitate the creation of 360-degree profiles of citizens and can result in “dragnet surveillance”.²³ The use of any digital identifiers, especially facial biometric data, may lead to unauthorised profiling of individuals through the correlation of identities across multiple application domains. Several studies show that FRT is inaccurate, especially based on gender, age, and complexion.²⁴ The Delhi Police treats an 80% accuracy on FRT systems as “positive” results, raising concerns about reliance on a 20% inaccuracy rate, that too for elections.²⁵ Further, FRT systems are particularly sensitive to errors when encountering new faces, and with about 90 million new voters slated to cast their first vote in the 2024 general elections, the error margin is dangerously high.²⁶ We urge a careful reevaluation of the implementation of surveillance technologies in the electoral process.

²⁰ Letter Election Commission on implementation of facial recognition technology in polling stations during union and state elections, Internet Freedom Foundation, January 17, 2024
<https://drive.google.com/file/d/196UwtDfX0v3No1VW0K21buGXPwaLjI0a/view>.

²¹ Maya Tudor, “Why India’s Democracy Is Dying”, *Journal of Democracy* (July, 2023) 34(3), pp. 121–32.
<https://www.journalofdemocracy.org/articles/why-indias-democracy-is-dying/>

²² “Illegal use of Facial Recognition for Voter Verification in Telangana #ProjectPanoptic.” Internet Freedom Foundation, March 17, 2020. <https://internetfreedom.in/the-telangana-ec/>.

²³ Dragnet surveillance refers to the collection and analysis of information on entire populations or communities, instead of merely those who are under suspicion for commission of a crime. See: Sarah Brayne, “Dragnet Surveillance: Our Incriminating Lives,” in *Predict and Surveil: Data, Discretion, and the Future of Policing*, ed. Sarah Brayne (Oxford University Press, 2020), <https://doi.org/10.1093/oso/9780190684099.003.0003>.

²⁴ Jacob Snow, “Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots”, The American Civil Liberties Union (July 26, 2018), <https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28>; see also Kade Crockford, “How is Face Recognition Surveillance Technology Racist?” The American Civil Liberties Union (June 16, 2020), <https://www.aclu.org/news/privacy-technology/how-is-face-recognition-surveillance-technology-racist>.

See also: Aishwarya Jagani. “No facing away: Why India’s facial recognition system is bad news for minorities”, *Unbias The News!* <https://unbias.thenews.org/no-facing-away-why-indias-facial-recognition-system-is-bad-news-for-minorities/>.

²⁵ “Delhi Police’s claims that FRT is accurate with a 80% match are 100% scary”, Internet Freedom Foundation (August 17, 2022). <https://internetfreedom.in/delhi-polices-frt-use-is-80-accurate-and-100-scary/>.

²⁶ “The year of elections: 4 billion people will cast a vote in over 60 countries in 2024”, *Business Standard* (January 6, 2024), <https://www.businesstoday.in/latest/world/story/the-year-of-elections-4-billion-people-will-cast-a-vote-in-over-60-countries-in-2024-412123-2024-01-06>.

Appeal to the Election Commission

In this respect, certain suggestions are being made to uphold and defend the integrity of the next general elections.

1. **Move from a Voluntary Code of Ethics to a Model Code of Conduct for Social Media:**

- a. Instead of a voluntary code of conduct, the ECI should initiate a transparent and participatory process spearheaded by a third-party, independent organisation(s) to arrive at a social media code of conduct to be followed by political candidates and digital platforms.²⁷
- b. The ECI should also provide a review of the operation of the voluntary code of ethics to the general public, including the inadequacy of digital platforms in facilitating transparency in paid political advertisements, taking action on any reported violations, creating a dedicated reporting mechanism for the ECI, etc. The ECI must also include in its review the concerns around the lack of transparency and broad-based public involvement in the creation and implementation of the Code.
- c. Any agreement between the ECI and social media companies should have at least the same standards, if not higher, that are applicable in other jurisdictions like the United States, European Union and Brazil. Moreover, these standards should apply to new and evolving technology such as AI-generated synthetic media.²⁸
- d. Digital platforms must be under obligation to publicly document the moderation action taken by them in compliance with the Code. Such documentation must include information regarding the content acted against, the date of publication of the content and the date of action, whether the content was flagged by a user or proactively identified, the publisher of the content, etc.
- e. Users of digital platforms and political parties must also have a dedicated mechanism to report violations of the Code by digital platforms to the ECI. Users must be made aware of such reporting mechanisms. Reports of violations and actions taken on them must be publicly documented in the interest of transparency and accountability. The ECI must develop the capacity to deal with such complaints in a timely manner.

2. **Disclosure by Political Parties on their digital activity:**

- a. The ECI must make it mandatory for all political parties and candidates to publicly disclose:

²⁷ 'Guidelines for the Development of a Social Media Code of Conduct for Elections' (November 2015)[Guidelines for the Development of a Social Media Code of Conduct for Elections | International IDEA](#)

²⁸Tejasi Panjiar and Disha Verma 'Read our Open Letter to Electoral Candidates & Parliamentary Representatives on the Impact of Deepfakes on Electoral Outcomes' (IFF, 26th February 2023)[Read our Open Letter to Electoral Candidates & Parliamentary Representatives on the Impact of Deepfakes on Electoral Outcomes](#)

- i. Official political party/candidate handle on all major digital platforms such as Facebook, Twitter as well as lesser-known platforms such as WeChat, Sharechat, TikTok, etc.
 - ii. The names of companies, paid consultants, and third party agencies looking after their social media accounts, public facing communication, and digital campaigning in relation to electoral matters.
 - iii. Details of all digital spending during the election campaign process.
 - iv. All third-party vendors on contract to provide digital services for them.
- b. The ECI must make political parties/ candidates, their IT cells, and their third party contractors aware of the MCC, the Media Certification and Monitoring Committee (“MCMC”) guidelines, policies and guidelines of digital platforms, and other election laws.
- c. The ECI must put in place curbs on data brokers which collect large volumes of data and sell it to political parties ahead of the elections. Political parties must be asked to report any such transactions.

3. Monitoring Expenditure and Targeting of Political Advertisements on Digital Platforms:

- a. The ECI should closely monitor the online spending of political parties and candidates for election campaigns. The spending declared by political parties must be corroborated by digital platforms.
- b. The ECI should arrive at a clear definition for “surrogate advertising” and establish enforcement guidelines as well as strict limitations for political parties on their advertising spending on digital platforms.
- c. The ECI must direct digital platforms to aggregate and publicly provide details regarding electoral ad/promotion spend during the election period, such as the name and address of the publisher, information on expenditures for ads/promotions by political parties and their listed IT cells and social media promoters, as well as the content of publication /advertisement.
- d. Direct digital platforms to track the monetisation of posts (the practice of paying money to boost the visibility of posts) on social media platforms by political parties, as well as by individuals representing these parties. The digital platforms should also disclose the specific demographics being targeted. The amounts spent on monetised posts and the identities of their target groups should be made public.

4. Build institutional capacity:

- a. Call for an iterative, open, consultative meeting with experts and independent actors working on electoral integrity and combating disinformation, besides discussions with digital platforms, government departments, and political parties.
- b. Engage with news organisations, civil society, and other independent groups seeking to combat disinformation, hate news circulation, and improve fact-checking during the poll process.

5. **Efforts surrounding the spread of disinformation and deceptive media:** The ECI must introduce measures to increase the accountability of political actors using manipulated media to influence voter perceptions.
 - a. The ECI must ask political candidates and affiliated organisations to publicly commit not to use deepfakes technology to create deceptive or misleading synthetic content in the run-up to and during the 2024 general elections.
6. **Protection from voter surveillance:** The ECI should conduct an outreach programme, educating digital platform users on ways to report violations of electoral norms. Some specific steps include:
 - a. The ECI must disallow the use of any surveillance technologies, such as drones, CCTVs, and FRT, at polling stations during the election period to avoid unauthorised profiling of individuals.

Signatories

1. Article 21 Trust
2. Association for Democratic Reforms
3. Campaign Against Hate Speech
4. Common Cause, India
5. Internet Freedom Foundation
6. LibTech India
7. Maadhyam
8. Mazdoor Kisan Shakti Sangathan
9. National Alliance of People's Movements
10. Rajasthan Asangathit Mazdoor Union
11. Software Freedom Law Center, India