MODERATING SOCIAL MEDIA

“Propaganda and disinformation are not new, but what’s different with internet is that you can tailor the story to particular individuals, because you know the prejudice of this particular individual” – Yuval N. Harari

Source
Introduction

Last month, Dictionary.com, an online dictionary portal declared “misinformation” as the annual word of the year. The site spelt out the meaning of the term as “false information that is spread, regardless of whether there is intent to mislead”. Misinformation joins a slew of words like ‘Orwellian’, ‘post-truth’, ‘fake news’ whose usage have spiked up in the recent times (Italie, 2018). This trend is emblematic of the information disorder caused by emergence of social media giants that has impacted countries across the world in the recent times. Information disorder is an umbrella term used by Claire Wardle (Research Fellow at Shorenstein Centre on Media, Politics and Public Policy) to describe different types of information problems (Wardle, 2018).

Social media platforms role in disseminating false information, hate speech and propaganda have been well documented. Stretching beyond US and UK, Facebook has been held responsible for communal and ethnic violence in number of countries including Myanmar, Sri Lanka (Ingram, 2018), Germany (Taub, 2018) and Mexico (Popken, 2018). This however forms only a part of how social media has become a tool threatening to undermine democracies around the world.
Data management, targeted advertisement and false information facilitated by social media are being used for political gains. Starting with involvement of Russian agencies in 2016 USA Presidential elections, the influence of social media to shape the political discourse during elections have taken different shapes in multiple countries with Brazil (Belli, 2018) being the latest example. Justifiably, the optimism that accompanied spread of social networking websites in their initial years across the world has now paved way for skepticism.

India, as expected, has been confronted with same set of challenges as well owing to tremendous growth of social media users. Till March this year, Whatsapp (a messaging service owned by Facebook) had more than 200 million (1.5 billion worldwide) users in India while Facebook, Twitter and YouTube respective users count in India stood at 194 million (2.19 million worldwide), 26 million (330 million worldwide) and 42 million (1 billion)\(^1\). The figures in themselves are testament of India’s prominence in the global social media network. Fuelled by cheaper smart phones and lowering rates of internet data plans, the proliferation in social media usage has come at a cost. As highlighted in a previous brief\(^2\), social media platforms have become a prominent source of misinformation and are being exploited by political parties to spread false information for their political ends. Subsequently, we analysed the need for a new data protection law to deal with challenges thrown by proliferation of the digital medium (PW, Vol. 6, Issue 28). We also covered the implications of the proposed social media hub by the union government which was later withdrawn owing to criticism from different corners including the Supreme Court (PW, Vol. 6, Issue 38). Adding onto our past coverage, in this issue of policy watch we will look into how the problem of information disorder is being framed and addressed in India as well as other parts of the world. Through this we will look at the broad approaches that are being put forward to tackle the problem. But before moving onto these, for the convenience of our readers, we would like to elaborate on conceptual difference between the terms that are often used interchangeably and also why information online is different from the false information cases that existed in the past and therefore more difficult to encounter.

Wardle uses three different words to distinguish the false information online. These are

- Dis-information
- Mis-information
- Mal-information

---

1. [http://164.100.47.5/newdebate/246/26072018/Fullday.pdf](http://164.100.47.5/newdebate/246/26072018/Fullday.pdf)
Identifying the problem

The technological aspect of online networking platforms offers a new set of challenges wherein the identification of the problem is itself a contested zone. While there is no doubt that internet has been misused to disseminate disinformation, experts argue that we need to be cautious while attempting to deal with the issue. They argue that legislations that give more power to state authorities could lead to censoring dissenting voices or self-censorship. Thus depriving us of the advantages that internet offers over other traditional mediums like print and broadcasting. On the other hand governments in a number of countries are introducing regulations and legislations invoking public interest as they argue that free-flow communication aided by social media platforms are threatening their national security. The case of regulation and control gains legitimacy with unfolding of every new online disinformation campaign that comes in public knowledge. The complexity of the issue gets furthered by debates around the role and responsibilities of the social media platforms themselves. How much onus can we put on them for allowing the fraudulent content on their platforms? Or can they be given the mandate to moderate the online content themselves?

In next section, we will look at some of the recent initiatives from other parts of the world and their framework to counter the disinformation problem. We will also look into some of the policy interventions made by
different governments and their limitations. This will be followed by looking at the recent developments in India in this context.

**EU Commission report**

In January this year European commission set up a 39 member (Experts appointed to the High-Level Group on Fake News and online disinformation, 2018) body to advice on policy initiatives to counter the disinformation and fake news on online platform for European countries. The body had representatives from technology companies, journalists, fact-checkers, academics and representatives from civil society as its members from countries of the European Commission. The high level expert group released a 44 page report in March 2018, titled ‘A multi-dimensional approach to disinformation’ laying out a series of suggestions and recommendations most of which were ‘non-regulatory’ in character. The report categorically advised against any concrete intervention from the government without clear evaluation except for support for educational initiatives and additional research on the subject. Some of its major suggestions are as follows:

1. **Disinformation not ‘fake news’** – The expert group in its report rejected the usage of the term ‘fake news’ which they considered inadequate in explaining the complexity of the situation. They identified the problem with the word ‘disinformation’ which they argued is a multifaceted problem which involves political actors, news media as well as civil society and therefore does not have a single solution. According to the experts, disinformation included forms of speech that are harmful excluding the already illegal forms of speech namely: hate speech, incitement to violence, defamation etc. The problem included actors such as – state or non-state political actor, for-profit actors, citizens individually or in groups – as well as infrastructure of circulation and amplification through news media, platforms and underlying networks, protocols and algorithms. It may also include communication via private messaging applications, chat bots, and voice-operated systems as well as augmented reality and virtual reality and content generated and manipulated by Artificial Intelligence.

2. **Financial support**: The expert group was in support of independent news media, fact-checking, source-checking and media and information literacy through public financing. The body emphasized on these initiatives to be free from potential interference of public authorities as well as technology companies as they can be used as public relations exercise by these actors.

3. **Sharing data** - The report repeatedly calls for internet giants to share data with researchers to assess the impact of disinformation as well as the initiatives like Google fact-check tags, Facebook
use of fact-checks. The significance of the report can be measured by the fact that it was signed by the Google, Facebook and Twitter representatives.

4. **Role of public institutions** - To increase the accuracy of the information system, public authorities across the European Union were recommended to share data promptly with fact-checking organizations.

5. **Investing in research** - Creation of a network of research centers across EU focusing on disinformation. The expert group pointed out the lack of knowledge on the subject.

6. **Collaborative approach** - The report asked for a collaborative approach involving all the relevant stakeholders with a structured process which will document the progress and reveal if any stakeholders is failing in their fulfilling their role.

Another major report came out in October on issues related to disinformation by department of Media and Communications of London School of Economics. The commission working on the report was called, *Truth, Trust and Technology commission*. It set out to outline the contours of the information crises and its harmful implications.

**LSE - Truth, Trust and Technology Commission (T3 commission)**

The T3 commission involved stakeholders ranging from journalists, academics, civil society groups as well as government representatives in UK. While the report deals primarily with policy framework in United Kingdom, its observations and recommendations offer a nuanced understanding of the issue that can be applied in other democratic countries as well including India. The commission in its report clearly states that it is firmly against any regulator that is formally linked to government or which has its goal, active regulation of ‘truth’.

The commission identifies five ‘evils’ responsible for the disinformation crises. These are

1. **Confusion** – The abundance of sources for the same information is leading to confusion in the minds of the citizens. As they come across different narratives about the same event, they are unsure about which sources to prefer over others.
2. **Cynicism** – People are losing trust in traditional news sources, this commission argues, is a global trend.

3. **Fragmentation** – Conflicting narratives of the same event is dividing people into ‘truth publics’. This means set of ‘agreeable facts’ of people is reducing i.e. disagreement is not only on the basis of opinion but also on ‘facts’ about any situation.

4. **Irresponsibility** – Absence of accountability in sharing information is leading to irresponsibility. In internet era, organizations disseminating information are neither accountable nor transparent.

5. **Apathy** – The continuous exposure to misinformation is impacting the morale of the citizenry.

The commission recommends a series of measures that could be adopted to counter the information crises:

➢ **Establish an Independent Platform agency (IPA)** - The government should introduce a new levy on social media platform’s advertising revenue, a proportion of which would be used to fund a new independent platform agency. The agency should be independent of government but report to parliament. Its purpose, initially, will not be direct regulation, but rather an ‘observatory and policy advice’ function, and a permanent institutional presence to encourage the various initiatives attempting to address the problems of information.

➢ **Media Literacy** - Government should mobilize and coordinate an integrated
law programme in media literacy.

➢ **Political advertising** - Legislative changes to regulate political advertising online.

The report clearly establishes the set of principles on which any policy framework should be premised on. These are:

- **Freedom of expression** – The right to impart and receive ideas without interference should be preserved. Restrictions should be proportionate, legitimate and prescribed by law.

- **Subsidiarity** – Decisions about content standards should be taken as close as possible to those that are affected.

- **Transparency** – Opaqueness in procedures for filtering content online could lead to self-censorship. The cases of filtration should be consistent with established principles and should be made public.

- **Evidence** – Access to improved data for regulators and the public.

- **Role of Civil Society** - Civil society should be involved in different capacities from providing resources as well as expertise.

- **Independence** – The functioning of IPA including the appointments and finances should be structurally independent from government’s working. The commission report can be read [here](#) in its entirety.
Network enforcement Act (NetzDG) – Germany

Network enforcement Act\(^3\) also called as NetzDG was enacted in January this year in Germany to counter the growing threat of disinformation online. The law does not define ‘fake news’. The legislation requires social media platforms such as Facebook, Instagram, and Youtube to promptly remove ‘illegal’ content as defined in the provisions of the criminal code of the country. It makes a distinction between “obviously illegal” content and “illegal content”. The time limit of removing the former is 24 hours and latter is 7 days. Platforms could face fine upto 50 million Euros if they fail to remove the content. Platforms are also expected to name an official grievance person for the country. Social networks receiving more than 100 complaints per calendar year are expected to produce half-yearly German language reports of the handling of complaints. The responsible authority for any dispute from social platforms is Federal office of Justice. The law does not offer users the chance to challenge the decisions by the platforms.

Criticism of the Act

Experts argue that the act violates freedom of speech on multiple grounds. Human Rights Watch, NGO working on Human rights issues globally, point out that the onus of determining whether any content is illegal or not lie with the platforms, a task which even court find challenging (Germany: Flawed Social Media Law, 2018). Secondly, considering the time limit as well the monetary fine, the act incentivizes blocking of content. Social media platforms will prefer deleting the content to save themselves from the fine. Moreover, the involvement of federal office of justice is a clear cut state interference and might lead to curbing of dissenting views.

The act has gained further prominence as it has been cited by governments in Russia, Singapore, Philippines and Venezuela, countries which are known for their strict media control.

---

France enacts law against fake news

The French parliament passed the fake news law on 20th November 2018. Unlike the NetsDG, the law provides a proper definition of fake news as “inexact allegations or imputations, or news that falsely reports facts, with the aim of changing the sincerity of vote”. The law is essentially designed for the election period, specifically three months before voting (Ricci, 2018). If any false information is being spread online, it can be reported by political groups, public authorities or individuals to the judge. The judge is authorized to act “proportionally” but “with any means” to halt the dissemination within 48 hours from the notification. Second important aspect of the law is the “duty of cooperation”. This requires each social media platform to establish a tool for users to flag disinformation. According to the legislation, social media platforms are required:

➢ To be transparent about their algorithm function
➢ To promote content from mainstream press agencies
➢ To remove fake accounts that “propagate massive misinformation”
➢ To disclose key information relative to sponsored content and the “identity of individuals or organizations that promoted them”.
➢ To undertake media literacy initiatives

The platforms are also expected to designate staff members to facilitate dialogue with public authorities. The broadcasting regulator Higher Audiovisual Council has been mandated with the responsibility of ensuring that platforms abide by the law. Violation of the law could lead to fine of 75, 000 Euros or one year in prison.

The bill was rejected twice in the parliament before getting passed last month. Even now, it has been challenged in court by the opposition parties. As for the provision it has received mix responses from the experts. Those opposing the bill argue that authority assigned to HAC is an overreach.

It is important to notify here that these two are not the only two legislations that have been introduced in the recent times. A number of countries have come up with initiatives to counter disinformation. For example: the president of Kenya in May this year passed a bill called Computer and Cybercrimes Bill, 2017 which criminalises 17 cybercrimes, misinformation being one of them. According to the law, anyone who knowingly shares false or misleading information can be fined upto 5 million shilling or imprisoned for two years (Schwartz, 2018). This includes information that is “likely to discredit the reputation of a person”. Critics argue that the bill criminalizes free speech and violates the right to media freedom. The legislations and commission reports discussed above give us an idea of complexity of the issue. Now let us look at some of the recent developments in India in the recent times.
Recent Developments in India

In last six months, Ministry of Electronics and Information Technology (IT ministry from herein) has notified social media giants on multiple occasions to prevent their platforms from being used to spread misinformation and hate-speech. It first issued a public notice on 3rd July in which it held Whatsapp responsible for fuelling violence across the country (Dey, 2018) and warned it to take immediate steps to ensure that the platform is not used for spreading deadly rumours. This was after Whatsapp was pointed out as the common thread in cases of public lynchings where it was being used as the source to spread provocative messages eventually leading to violence. Weeks after this notice, IT minister Ravi Shankar Prasad addressed the Upper House on the issue of rising cases of violence due to misuse of social media. Assuring the parliament of taking the necessary steps, the minister read out a series of steps for the social media platforms like Facebook, Twitter and Whatsapp. These were:

➢ Asking platforms to have their physical presence in India.

➢ Ensuring sources of malicious messages can be traced.

➢ Appointing a grievance officer to coordinate with the users as well as the law enforcement agencies.

➢ Come up with technological solutions that can filter out fake news and provocative messages from their platforms.

The suggestions of appointing a grievance officer and coming up with technological solutions to trace the source of the message were re-emphasized by the government in later interactions with social media platforms.

The implications of disinformation on political processes, especially elections have not received any major attention from the union government. Election commission, although, has publicly acknowledged influence of social media on elections (Ramachandran, 2018), there has not been much clarity on how the commission has dealt with unique challenges that digital medium has on offer. EC has proposed to bring political advertising on social media platforms under the ambit of paid news. EC also conducted a workshop with Facebook employees and monitors social media through media certification and monitoring committee. There have been no updates on implementation and efficacy of these initiatives.

Before moving onto the responses from the social media platforms themselves, let us briefly look at the existing legal provisions that exist to moderate and regulate online content.

Existing Mechanism

As far as the legal provisions are concerned, websites and intermediaries (Social media
sites) are governed by provisions under section 79 of IT Act, 2000 which provides immunity to social media platforms from any liability under all laws provided they have not conspired or abetted or aided or induced in commission of any unlawful act and have observed ‘due diligence’ while discharging their duties under the act. Interestingly the provision 79 3(b) of the section was read down by the Supreme Court in the infamous Shreya Singhal case in 2015 which struck down the section 66A. The provision required intermediaries to take down posts once notified by any government authority or any other user within 36 hours. The court in its judgement stated a court order is required to take down the content. It was believed that social media platforms would receive million of complaints to take down content and this would lead to over-censorship of the medium. This meant any platform reserves the right to refuse to take down content unless advised by the court.

**Initiatives by platforms in response to government’s suggestion**

Whatsapp on 10\(^{th}\) July this year released full page advertisement in major English and Hindi Dailies. Titled “Together we can fight false information” the advertisement containing a total of 10 steps intended to create awareness amongst its users on how to spot false information (Deep, 2018). It urged the users to be more careful while forwarding messages which seemed ‘unbelievable’ cautioning that ‘fake news’ has more chances to go viral. This multilingual advertisement was part of education/literacy campaign initiated by Whatsapp.

Acting on government’s demands, Whatsapp appointed Komal Lahiri as its grievance officer in September. Similarly, Facebook hired Trushar Barot, a former BBC Journalist to lead their ‘integrity initiatives’ which involves ‘combating fake news and digital misinformation, developing digital literacy’ (Thaker, 2018). Google on their part are training 8000 journalists across the country in six Indian languages to fight detect and combat false news online.

Whatsapp earlier this year rolled out a series of features for users in India in its attempt to curb rumour-mongering on the app. This included capping the number of forwards to five to curb mass spamming, the quick forward button next to media messages was disabled and “forwarded” label was introduced. Other than the newspaper advertisement mentioned above, Whatsapp as part of its user-education campaign has partnered with NGOs to organize user awareness programs across the country. It has also started radio ads as part of the campaign.

While tracing the message may not be the major concern for platforms like Youtube, Twitter and Facebook, this would require Whatsapp to de-encrypt the users’ messages which the company argues would undermine users’ privacy. Nowe we will look at the steps proposed by government and their possible implications.
Analysis

➢ Appointment of grievance officer

Government expects social media platforms to have physical presence and appoint grievance officer in India. This, although might seem like a reasonable demand but is not enforceable for a free internet argues, Nikhil Pahwa, Founder medianama.com. He says that this will deprive the users in India from using latest social media apps since most of them are based outside India and do not have any physical presence in India. While big social media platforms have the resources to do so, comparatively smaller websites would not necessarily have the same resources and hence this would further tilt the balance in big giants favour (Pahwa, 2018).

➢ Tracing the source of message: the privacy issue

Government, on its stance of asking Whatsapp to trace the source of message, has been at the loggerheads with the social media platform. Messages on Whatsapp are encrypted end-to-end to ensure privacy, this means no third party can de-crypt the message, only the receiver and the sender know the content of the message. Government wants to trace the source of the message arguing that it will help them in combating misinformation online, on the other hand Whatsapp feels doing away with encryption will have a global implication for their platform and will weaken the privacy net the platform offers to its users. Experts offer some other alternatives in this regard. Nikhil Pahwa feels Whatsapp can give the users the option of making a message private or public, each with different colour. This means that the receiver will be able to identify whether a message is public or private by looking at the colour. Only public messages should be allowed to be shared. The original sender of the message should decide whether a message can be forwarded or not. Every public message should have unique Id and if reported for misinformation, Whatsapp can either disable the message from being spread further or block the user who sent the message (Pahwa, Addressing WhatsApp's Fake News problems, 2018). A paper by Himanshu Gupta, former employee of We chat and Harsh Taneja from University of Illinios Urbana-Champaign suggested that Whatsapp can keep copies of most commonly transferred data on its servers and if any of it is reported, can that content fact-checked (Gupta, 2018).
Legal context: Time to look at Intermediary liability?

Prashant Reddy, assistant professor, NALSAR, believes that government needs to restore the original version of section 79 before it was read down by the Supreme Court in 2015 for all the social media platforms except Whatsapp. He also calls for removal of subjective terms like ‘due diligence’ as there is no clear definition of the term. He says the concern of over-censorship can be handled by hiring well-trained region specific content moderators who are conversant with the politics, language and sociology of country like India (Reddy, 2018).

He argues for even more firm step for Whatsapp due to its encryption feature asking it to be removed from the immunities provided by section 79. This would mean removing the safe harbor provided to the intermediaries. Giving primacy to public order argument over privacy, Reddy argues that this would either propel the platform to reconsider its stance on de-encryption (Reddy, If WhatsApp Doesn’t Regulate Itself, Parliament May Have to Step In, 2018).

There seems to be some development on this front going by IT minister’s speech on 26th July stating that the provisions in the IT act 2000 need to be revised and reinforced so that they can respond to the emerging challenging. He added “if platforms fail to take adequate steps and prompt action, then the law of abetment also applies to them.” While no intervention has been made in this regard, these statements if taken together mean that the exception in section 79 could now include platforms failure to take the necessary steps to prevent spreading of viral messages. This means failure of Whatsapp or any other social media to put in the necessary mechanism to stop hate speech on their platform would be considered abetment. If announced, these instruments could transform how social media platforms operate in India.

Framing a wrong narrative: are social media platforms being made scapegoats?

While there is no doubt that social media has allowed proliferation, few experts argue that it is being made a scapegoat distracting us from important issues. Apar Gupta argues

‘Safe harbour’ and Intermediary liability - Intermediary liability is a legal concept that governs social media platform’s responsibility for content that is generated by the user of their services. According to Vinay Kesari, ‘safe harbour’ protections that are part of intermediary laws allow search engines, web hosts, blogging platforms, social media companies, video sharing sites and messaging apps to upload content without pre-screening it (Kesari, 2018). This has been one of the chief reasons behind the tremendous growth of internet platforms. A luxury not shared by the print and broadcast media.
that government has never kept a record of public data on lynchings in the past and therefore no comparison can be made if cases of lynching have increased post social media. He argues that rising influence Gau Rakshak dal across different states have considerably increased incidents of lynching which are often attributed to Whatsapp (Gupta A., 2018). Putting the onus on Whatsapp for the issues is allowing public officials and police departments to escape accountability. Therefore instead of focusing on the structural reforms necessary to restore law and order, we are trying to look for quick fixes.

**Conclusion**

While digital media removed the traditional gatekeepers that existed in print and broadcasting medium, the free-flow of communication has now become a cause of concern. In India, the debate around the social media led disinformation campaign has been dominated by the hate speech on Whatsapp. In doing so, disinformation for political gains has not received adequate attention, especially from policy vantage points. Experts argue that looking at how social media platforms were used to manipulate elections in number of countries including Brazil, India should be proactive in its approach. While the European commission as well as the T-3 commission stress against regulation it is important for us to look at the challenges that await us in short term. India will witness the biggest elections in the world in few months time and urgency of the situation demands intervention that could minimize the impact of disinformation campaign. In this regard, the French legislation to control false information campaign online during the elections could be a good starting point. To tackle the problem in the longer run, both the expert group of EU and the T 3 commission provide a framework that could be useful for policymakers in India. Giving the government the sole authority to control content social media platform would antithetical to the idea of free internet. The idea of introducing special levy on social media platforms’ revenues and using that fund to invest in financing literacy programs and research can be tried. Similarly the authority to screen content should not rest either with the social media platforms or government. Moderation should be collaborative effort with involvement of local civil society groups. Furthermore it has been observed that social media platforms have largely been reactive instead of being proactive when it comes to their policies. For example, global giants like Facebook, Twitter, Google tend to enact new initiatives depending on the pressure by the government authorities in any country. One such instance was in Brazil, where Whatsapp refused to roll out features that it did in India. But as the reports of Whatsapp’s involvement in cases of disinformation came out post elections, it chose to introduce the features. The role of political will therefore cannot be emphasized enough.
References


