A Study on the Rise of Social Media Surveillance in Modern Times on the Pretext of Combating Fake News

Debarshi Bhattacharyya

Faculty, Department of Journalism & Mass Communication Rani Birla Girls’ College

*Corresponding Author: Debarshi Bhattacharyya, Faculty, Department of Journalism & Mass Communication Rani Birla Girls’ College, India

Abstract: Social Media surveillance is not a new concept to the world. Surveillance activities have been in practice for a long time in different countries of the world. With the growth and rise of different social media platforms, the governments of both democratic and authoritarian countries have invested heavily in deploying tools for tracking the online activities and behaviors of their citizens. This is primarily done to track down hate speech, misinformation, and fake news however there have been numerous instances across the globe which speak otherwise. In the pretext of only combating fake news and false information the governments of different countries of the world track user details by prying on their online presence. In such a process huge metadata of personal information is accumulated without their knowledge and consent. This is not only alarming but also scary as this is a serious breach of not only some of the basic human rights but also fundamental rights.

This academic paper discusses many aspects where both the Union and State governments of India have crossed the line and used social media surveillance tools for collecting personal users’ data for their benefit. Such data would often lead to the identification of users posting strong criticism against government policies which is of course a constructive and healthy practice in a democracy. However alienating from such a healthy discourse, the government used the data in quashing posts that were anti-government citing the pretext of either combating misinformation or defamation caused. However, instances have also been cited objectively as to how the Union and State governments of India have successfully identified false news spreaders and arrested the further spread of misinformation through different social media platforms.

This academic paper also discusses in detail about fake news, how it spreads, and also identifies the elements responsible for it. Motivated mechanisms along with the support of technology often create an environment for such misinformation to spread rapidly and attain virility in a very short time. This paper apart from citing what can be done in such a crucial time also focuses on the thin boundary of government surveillance on social media platforms in the pretext of combating fake news.

Keywords: Surveillance, Social Media Surveillance, Government Surveillance, Privacy, Fake News, Cyber Propaganda

1. INTRODUCTION

Mass media surveillance, especially social media surveillance is a very serious topic that needs to be discussed in the present day scenario. With so many instances of violations of basic freedom on the ‘net’ happening for some years now all over the globe, it calls for a better introspection about the issues at hand. Not just the fundamental rights are at stake but also some of the very basic human rights and the right to express. From authoritarian to democratic countries alike have been engaged in scrutinizing their citizens’online activities and online behaviors.

According to Shahbaz and Funk (2019), there are about 3.8 billion people who have access to the internet. The authors also state that out of the 3.8 billion people, 71% live in countries that have been imprisoned or arrested for posting on social, political, or religious issues. The authors also observed that 65% of the individuals live in countries where they have been attacked or killed for their online activities since June 2018 and 59% live in countries where State authorities have posted pro-government commentators for manipulating online discussions. Shahbaz & Funk also found out that out of 3.8 billion internet users 56% live in countries where religious, social, or political contents were blocked online, 46% of the individuals live in countries where authorities disconnected internet or
mobile networks often for political reasons and 46% of them live in countries where access to social media platforms was permanently or temporarily suspended. From the data cited above, it is evident that freedom on the net is highly infringed across the world. This is not only direct and relevant data that highlights serious violations of basic human rights and the freedom to express but also focuses on why serious concerns must be laid both academically and professionally on these issues.

Recently the social media platforms have come under the scurrilous monitoring mechanism of the elites for it serves as a breeding ground for like-minded opinion assemblages. These platforms serve as the perfect ground to practice free speech and express personal opinions. The veracity attained by constructive discourse must be encouraged ethically. But, the big question is whether such platforms are utilised in the best possible way for meeting vital ends for society as a whole? The role of the elites is very important in this regard. When the elites have control and dominance over different social media platforms, it is quite likely they will try to control speech and expression in different ways. The emerging and growing patterns of media conglomerates strengthen such claims. What is witnessed is the adaptation of different surveillance techniques to monitor and track users’ online content without their knowledge. This might be a useful tool to track sensitive contents that aim to spread dissent, scornful messages, and misinformation among the public which may further disrupt the public order. However, deeper analysis and further studies are needed to understand the serious repercussions of wide-scale surveillance of users’ contents, profiles on social media platforms and even tracking their online activities and device locations.

2. RESEARCH QUESTIONS

The following are the questions that have been focused on finding appropriate answers in this research work.

- What happens to all the data collected online?
- Are these data utilised for political purposes?
- Are these data stored for a long time and what if these data get hacked?
- What about our online security and why should we be worried about our security if our personal information gets breached online?
- Do the modern elites still dominate the information flow and use the latest technologies of surveillance to dictate the lives of the general public?
- Is the fake news served strategically with a definite goal and is this the return of Propaganda?
- What would be the effective strategy to fight such misinformation?

3. AIMS

The Following are The Aims of this Research:

- This research aims to discuss the many ways social media surveillance has become a reality today and how countries across the globe have made use of the latest surveillance technologies to keep an eye on their citizens over their online presence.
- Through this research, an attempt has been made to discuss the use of social media surveillance mechanisms by the government in times of increasing fake news citing how such fake posts can disturb communal harmony and societal balance and whether the government (an elite) has been instrumental in using surveillance tools over online and digital platforms in combating problems relating to the rise of fake news, misinformation, hate messages and thereby taking a step towards maintaining the integrity of the nation and securing the public order?
- This research then addresses a plethora of the news reports and articles that appeared in Indian newspapers where the government took steps to monitor social media posts and how social media surveillance is a threat to privacy which ultimately hampers the democratic rights of the citizens.
This research further aims to assess what happens to the data collected online through the latest surveillance technologies and also attempts to find answers over the serious repercussions it brings when personal data is breached online.

3.1. Research Methodology

This Research Relies Heavily on the Followings:

- Discussions on various instances across the world and specifically India as reported in Indian newspapers, magazines, and websites on the infringement of Freedom of Speech and Expression on the internet by the international and national elites. This is a necessary inclusion as this has helped in framing ideas and constructive knowledge about the relationship between the binary factors - the elites and their role in surveillance activities.
- Constructive analysis through discourses about relevant theories has been discussed for interpreting why fake news is still shared by users, whether this massive orchestration used for spreading and breeding false information is deliberate, or are these the results of misinterpretation of social media texts?
- Subjective representation of facts has been focussed thereby giving prominence to the necessity of personal opinions and expressions based on extensive reading of relevant texts. Myriad relevant phenomena have been analytically broken down for accurately predicting and assessing important evaluations related to the noted research questions and aims of this research.

3.2. Understanding Surveillance and Social Media Surveillance

The word surveillance comes from a French word meaning to oversee or watch over, carried out by observers and watchers thereby implying social hierarchy (Fuchs, 2011). Human beings constantly remain aware of their surroundings either consciously or less consciously by taking note of the behaviour and appearances of the people nearby. Such activities are dominant in every social system like between friends, managers, co-workers, and the bureaucrats (Marx, 2012). This also includes keeping a close eye on the activities of people on Facebook, Twitter, Instagram, and YouTube, etc. (Brown, 2014). According to Shabbaz and Funk (2019), “Social media surveillance refers to the collection and processing of personal data pulled from digital communication platforms, often through automated technology that allows for real-time aggregation, organization, and analysis of large amounts of metadata and content” (p. 12). This idea also echoes in the words of Lyon, Haggerty & Ball (2012) where they say that such a process is typically distributed across interlinked systems, social connections, and bureaucracies thereby converging into “surveillant assemblages” and therefore remain rooted within everyday life. According to Brown (2014), these social media sites are increasingly resembling such assemblages by tracking the users’ activity and gathering data from the internet via cookies, different tracking mechanisms, loyalty cards, smartphone location traces, and customer surveys. Thus, whatever we share online is always public. There are multiple websites and especially social media platforms from where data breaches have been reported in recent times. Facebook is one such platform that came under scrutiny for a data breach of over half a million Indian Facebook users. (“Over Half a Million”, 2018). The data gathered through social media surveillance becomes valuable intelligence to others who can further monitor and manipulate. Thus, whatever content we post on social media can be accessed, checked, and carefully monitored without our knowledge. Not only content on social media but also almost every activity we put on the internet can be regularly checked and monitored.

This is particularly dangerous as it curbs the very right to privacy. The social media we rely on for information, news, and entertainment can be scurrilously checked by third parties in gathering huge amounts of digital personal data. Social media surveillance is however not new. According to Brown (2014), the concept of surveillance is not new but attained a new meaning in the late twentieth century where it became a central organising societal practice affecting the power dynamics, institutional practices, and interpersonal relationships. With the development of technology, this transformation was driven by instances and factors of increasing managerialism, greater public perception of risk, and political convenience (Lyon et al., 2012). In both democratic and authoritarian regimes, the extent and intensity of surveillance practices in modern politics have been labelled as surveillance societies.
A Study on the Rise of Social Media Surveillance in Modern Times on the Pretext of Combating Fake News

(Marx, 2012). According to Hasse (2013), surveillance is, looking at the lives of other people and their behaviours, appearances, and social relationships in a natural social process. There have been numerous instances when the personal information put up by the social media users has become public and that too without their consent. Thus, the question of privacy becomes very important in this respect.

According to “Current practices in electronic surveillance” (2009), “Surveillance is the collection or monitoring of information about a person or persons through the use of technology” (p. 5). As explained by Odoemelam (2015) surveillance incorporates a plethora of technologies and practices aimed to constantly monitor the activities of people without their knowledge and permission. For instance, there is audio surveillance- which includes phone tapping and installing listening devices, visual surveillance like CCTV- closed-circuit television camera, tracking surveillance like GPS-global positioning system and mobile phones and data surveillance- which includes the computer, keystroke and the internet monitoring. The majority of the devices we use every day that makes our life easy and has become a very important aspect of our lives are constantly being used by the government or some other third parties to monitor people without their prior permission and knowledge. Thus, surveillance is an instrument or aid used by the authorities or the government for managing and monitoring the activities of the citizens. This is clear in the words of Lyon (2007) as any focussed, systematic and routine attention to personal details for influence, management, protection, or direction. To achieve this the nations often use technological surveillance methods like wiretapping telephone conversations, using infrared cameras, and tracking people with biometric data. In a similar fashion marketing companies, these days often use social media platforms like Facebook, Twitter, instant messaging services, and even blogs to collect user’s data and often end up violating the privacy of the users (Odoemelam, 2015).

3.3. Social Media Surveillance, Technology and how the Governments use it?

Surveillance and even social media surveillance are not new to the western world. The governments of the developed nations have been using electronic surveillance to keep a watchful eye on their citizens for any dissidents or in keeping a check and in solving criminal activities. The prominence of surveillance heightened in the United States after the September 11, 2001, terrorist attack. This incident escalated the urgency and need for surveillance for keeping the nations safe and secure from further terrorist activities. In this regard, many nations have deployed huge amounts of money in developing technology and software aimed to detect and collect personal information of people from within and outside the borders. In the words of Odoemelam (2015), “Electronic surveillance is a common phenomenon these days with invisible, visible, semi-concealed cameras and sensors embedded everywhere in all corners of society” (p. 1). The author also mentions that surveillance is also used in homes, public spaces, and even in homes. Surveillance has become a model of deploying control of parents over their children, community members over their neighbours, managers over their employees, and the government over its citizens.

The modern generation is witnessing high growth of software used in almost every area of the profession. According to epic.org (2018), social media monitoring software (SMMS) has dilated over the past several years. Now, Fortune 500 companies, law enforcement, politicians, federal agencies, defense contractors, and even the military are purchasing SMMS products like MediaSonar, XI Social Discovery, Geofeedia, Dataminr, Duann, and SocioSpyder, etc. (McCullough, 2016). Even the Central International Agency or CIA has a venture fund named In-Q-Tel, that invests in SMMS technology (Fank, 2016). In the words of Scott (2017), the software is not just used to look for keywords but is also used to track down the location minutely as from which social media the posts are coming, identify relationships between people, scan events, and sway an individual’s potential for violence. Also in India, the government is planning to develop social media surveillance tools that are aimed to track overall social media trends and also monitor individual social media users. The tools would be able to gather private as well as paid social media data, track sentiments, and even would be able to analyse trends relevant to government-related activities which might harm the social and socio-economic fabric of the society (Barik, 2020).

Technological growth and advancement certainly have made our lives easy and comfortable but standing in the present time, we must focus on its flip side. The question of negative influence
however echoes the voice of the scholars of mass society perspective; important and uncomfortable questions need to be addressed. Starting with Thorstein Veblen’s technological determinism, it is important to remember here Marshal McLuhan’s optimism about the cultural consequences of capitalist-dominated media. McLuhan was “fascinated by the implications of Innis’ arguments concerning the transformative power of media technology. He didn’t fear the ways this power might be exercised by the elites. (Baran & Davis, 2011, p. 231). McLuhan’s over-optimistic approach comes under a strong challenge from the modern elites- the government. News reports from across the world throw light on how the governments of democratic and authoritarian regimes have deployed automated surveillance tools to check the online presence and activities of their people (Shahbaz & Funk, 2019). McLuhan, while arguing, stated that there is nothing to fear from the elites if the technologies can determine how these would be used (Baran & Davis, 2011.). We see just the opposite to such a prophecy. Elites have played a crucial role in this regard. Their pivotal dominance in checking what people post, comment, or share on social media platforms has become an important course of study in recent times. According to Foucult (1977), surveillance is a “shameful act” of overserving and imposing control on a subject through a “hierarchized system of policing”. Thus he meant that surveillance acts as a tool of control for the political and economic elites (Odoemelam, 2015).

Multiple instances have been reported where some major authoritarian powers as well as poorer countries invested heavily in purchasing sophisticated technology for tracking dissidents and persecuted minorities (Shahbaz & Funk, 2019). The question that arises now is why the governments are worried about the online activities of their citizens? Freedom of media has resonated in a vivid dimension in not only texts but also speeches of politicians. Media gives us the power and opportunity to participate- particularly social media. The freedom to create our meanings and availability of technologies to recreate, investigate, and spread that meaning speaks volumes of evidence which firms the belief that we are now living in an era of meaning-making perspective of mass communication theory (Baran & Davis, 2011). This became clearer and convincing when Times acknowledged this reality and named “YOU” which means us- the people as the person of the year in 2007. This content creator role of individuals is a direct participatory approach. Individuals now don’t have to depend on any traditional media but create their content and disseminate it to their targets. These powerful instances are often well reflected in strong posts, comments, and criticisms on Facebook, Twitter, Instagram, etc. The government and the law enforcement departments can examine posts on social media like Facebook, Twitter, Instagram, and YouTube for information on potential threats, breaking news, protests, etc. (epic.org, 2018). Such posts often reach wide popularity and are vastly shared and liked by many. What can be witnessed here is the idea of ideal democracy where people enjoy the basic human right- and that is to express themselves freely. A country thrives when its citizens are made aware in the truest sense; when the citizens are made aware and provided with an opportunity not just to comment but actively express their opinion- the society and the country as a whole reach a new height of development. The role of media becomes more prominent in this regard.

According to Kumar (2016, para. 1), “Media constitute the fourth pillar of democracy. The role of the media is vital in generating a democratic culture that extends beyond the political system and becomes engrained in the public consciousness over time”. Such watchdog roles of media have been widely discussed in many texts but what about instances when this watchdog role is being restricted and in some instances suspended? For a country to progress it should provide “transparency on many levels including for access to information; accountability and legitimacy of individuals; institutions and processes themselves; and for rightful participation and public debate” (ace, nd, para. 4). However such ideal situations are seldom found as according to Shahbaz and Funk (2019), “the governments have long employed people to monitor speech on social media, including by creating fraudulent accounts to connect with real-life users and gain access to networks” (para. 2). The authors also state that Iran has deployed an army of 42,000 volunteers who check online speech. Any citizen of Iran can report for duty on the website of cyber police, commonly known as FATA. In China, the Communist Party recruited many individuals to examine the internet and report problematic contents and accounts to the authorities.
In addition to this, advancement in artificial intelligence (AI) also has been a key weapon in putting a check on people over their online activities. These technologies can easily map user’s relationships through link analysis, located precisely from where they are accessing their social media accounts. Machine monitored surveillance activities are way advanced and integrated than keeping an eye on manually. What might remain invisible to human eyes are scrutinised through deep neural networks-which opens up further avenues for deeper investigations. Such activities can have serious consequences as machines might reach faulty conclusions about an individual’s posts on social media, which might lead to banning, restricting, or suspension of social media accounts and even arrests. As Shahbaz and Funk (2019) put it, “Whether accurate or inaccurate, the conclusions made about an individual can have serious repercussions, particularly in countries where one’s political views, social interactions, sexual orientation, or religious faith can lead to closer scrutiny and outright punishment” (p. 12, para. 4).

A balance must be maintained by the government as to what to keep under check and how to monitor the activities of the citizens? Having said so and discussed already that electronic surveillance has proven to be highly effective in the detection of crimes and preventing criminal activities, it should also be remembered that certain lines should never be crossed. It shall be the primary duty of the government not to malign and infringe the basic fundamental rights of people but strike the perfect balance by which the technologies deployed heavily can be used for societal good as a whole.

### 3.4. Social Media Surveillance and Privacy

There is no denying the fact that despite using social media for our benefits it has eroded our privacy to a great extent. For instance, when we log in to social media platforms we reveal our personal information and data and such information gets public almost instantly. These data might be used by governments or even marketing firms in knowing our behavioural and attitudinal patterns. What is more worrying is that often these data are being sold to marketing firms by social media companies like Facebook, Four Square, and even Google. According to Hoofnagle (2019), the social media firms claim that they do not sell users’ data but some shreds of evidence confirm Facebook and Google to have paid developers with users’ data. This selling of the users’ data is central to “platform economics”. It is very important to address a primary area here, which is to make the users aware and educated about such issues. The people accessing social media or any websites must be enlightened about the scopes of data breaches and how they might have negative consequences in their lives. The users therefore must examine and re-examine the privacy issues before putting personal data on any social media platforms or websites especially in the era of digital technology (Odoemelam, 2015).

To define privacy, according to Woo Jisuk (2005), as to how one’s personal data and personal information are handled in social contexts, and particularly more in public settings. The “private” is that which is shared only with close, trusted, and face-to-face relations. Thus, privacy concerns the protection of sensitive data and information, financial and medical records from unauthorized access or view. Social media posts and comments that are being made public make privacy issues more complicated (Odoemelam, 2005). The question of privacy when users openly and intentionally decide what to post and when to post needs further discussion.

What users post or comment on social media is done with certain objectives. It can be to voice their support or speak strongly against any local, national, or international issues. Sometimes social media posts are even benign and casual. But in every instance, the posts are meant to reach somewhere (not physically) and to be read by someone, even by whom the users don’t know personally. Users tend to use social media as means of expression because these media are easily viable, cheap, user friendly, and interactive. Benevolent expressions though seem harmless but have their other uncomfortable sides as well. All Facebook friends or Twitter followers might not be trustworthy and the personal details of users get breached too often. There have been numerous instances when users’ personal photographs have been downloaded and used for creating fake profiles or accounts without the users’ prior permission and knowledge. For instance, a news article published in The Times of India where an engineer named Ajay Galar created a fake profile and duped a Delhi law student of ₹30 lakhs after befriending her (Mishra, 2020). Again, another news that appeared in The Times of India where a 37-year-old labourer of an automobile factory was arrested by the cyber cell for creating fake accounts of girls and morphing their faces with obscene pictures (“37-year-old posts morphed pics”, 2018).
Another such incident was reported from Gurgaon and published in India.com where a man had multiple fake accounts of women on Facebook and Instagram and he used those accounts for making profitable businesses (“Gurgaon: Man arrested for running Profitable Scam”, 2018).

It is important to address the discourse of privacy in public as this is essential in a well-functioning democracy (Scott, 2017). Privacy in public allows for associational rights, self-realization, supports freedom of thought, prevents similarity of thought, and prevents suppression of free speech (Reiman, 1976). This is vital in a democracy as it further protects the “free market of ideas” (Scott, 2017). The author also stated that traditionally privacy in public was protected by economic and technological limitations and this made public information largely obscure. Most of the traditional theories of privacy were concerned with the protection of the intimate and personal sphere but with the rise of information technology and databases, there arises a threat to privacy in public (Nissenbaum, 1997). It is because the more we get dependent on social media for our activities and basic communication— even if it is casual we are exposing ourselves to the wide range of surveillance technologies that can keep a constant check on our online presence. It is important to maintain privacy even in the public sphere because what the users choose for public access depends on their will and conscious deliberations. However, the context becomes more complicated when unauthorized views loom over the posts that users don’t intend to share with.

Gathering public information is an easy task now with so much software and technologies to scan our online profiles; careful observations must be cited in this regard. In the absence of technology gathering, public information was obscurity but absence of obscurity has paved the way for indiscriminate mass surveillance of everyday occurrence (Scott, 2017). The context of this obscurity can be applied to the online realm as well. With the decrease in obscurity there arises the increasing threat to online surveillance activity. This inversely proportional relationship echoes in the work of Hartzog and Stutzman (2013) where they proposed determining online obscurity based on four factors- search visibility, unprotected access, identification, and clarity. Obscurity can be further understood in reference to the work of Reidenberg (2014) where the loss of practical obscurity has been explained in three stages- obscurity, accessibility, and transparency.

On August 24, 2017, the nine-judge bench of the Supreme Court of India headed by the then Chief Justice KS Khelar ruled that right to privacy is a fundamental right for Indian citizens guaranteed by the Constitution of India. Thus, no legislation passed by the government can unduly violate it (“Right to Privacy a Fundamental Right”, 2017). However, in December 2018 the Ministry of Home Affairs granted surveillance rights to ten central agencies including the Central Bureau of Investigation (CBI), Delhi Commissioner of Police, and the Directorate of Revenue Intelligence to name a few for monitoring individual computers, their receipts, and transmissions under powers conferred on it by the sub-section 1 of section 69 of Information Technology Act. It has authorized these security agencies to intercept, monitor, and decrypt any information generated, received, transmitted, or even stored in any computers (“10 central agencies can now snoop”, 2018). “Facebook trouble: 10 cases of arrests,” (2015) a Hindustan Times report cites instances when arrests were made for violating section 66A of the Information Technology Act and the vociferous opposition to it. It is also worth mentioning that another news report published in The Tribune state where the Supreme Court of India ruled that no arrests can be made under 66 A of the Information Technology Act, 2000 for social media posts. Pronouncing the verdict on a PIL filed against a section, which empowers police to arrest a person for allegedly posting offensive materials on social networking sites, the court said it is illegal because it breaches the fundamental right to freedom of speech and expression (“No arrests under 66-A”, 2015).

The question in context is how far is it justified? Can the government go on policing social media posts and profiles just because it might incite tension or escalate criminal activities? Article 19 (2) of the Indian Constitution clearly states such restrictions. Better known as reasonable restrictions, it has been mentioned that the fundamental right of freedom of speech and expression remains suspended if such expressions are against the “interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court, defamation or incitement to an offence” (Indian Kanoon, n.d., para. 2).

In 2016 a news surfaced in The Wire where a 19-year-old student, Abhishek Mishra was arrested by Madhya Pradesh police over social media posts that attacked the prime minister, Narendra Modi, and
A Study on the Rise of Social Media Surveillance in Modern Times on the Pretext of Combating Fake News

the chief minister of the State, Shivraj Singh Chouhan on the issue of demonetisation. Mishra claimed to be aware of people through his social media posts. An FIR was filed against him under section 469 of the Indian Penal Code and 66C of the Information Technology Act, 2000. A cyber cell official said Mishra was arrested because of posting abusive comments against the chief minister of the State and other dignitaries. Mishra’s posts were deleted from his Facebook account and the website he ran was also blocked by the Madhya Pradesh police. He was later released on bail. (“Social Media Post Against Demonetisation”, 2016). In another such incident reported in The Times of India, the Crime Investigation Department (CID) arrested four persons from different parts of Andhra Pradesh on the charge of posting objectionable and offensive posts on social media and sharing them with others. CID registered cases under “sections 505 (b) and 120 b of the IPC” (G. 2020). In another incident reported in ndtv.com, 124 people were arrested by the Uttar Pradesh police for inciting content and 19,000 social media accounts were reported. The crackdown by the police came at a time “when the State was on the edge after violent protests in many parts over the new citizenship law” (Pandey, 2019, para. 1). In June 2019 eight people were arrested over social media posts in four states of Uttar Pradesh, Assam, Chhattisgarh, and Tripura. In this context, the arrests of three journalists by the Uttar Pradesh police received a lot of media attention as police claimed the social media post defamed the chief minister, Yogi Adityanath. The action was also taken against the people in Assam, Tripura, and Chhattisgarh (“Eight people have been arrested”, 2019). In Kerala for offensive posts on social media an ordinance to allow three years imprisonment has been signed by the governor (“Kerala governor signs ordinance”, 2020). When arrests were being made in Uttar Pradesh for making objectionable comments and defaming the chief minister of the State; people were also booked in Kerala for abusing the chief minister of the State, Pinarayi Vijayan on online platforms. On October 29, 2020, a news report published in Scroll.in published news where the Supreme Court warned West Bengal police on harassment against social media posts. The top court was hearing a challenge against summons issued to a Delhi resident by West Bengal police over her Facebook posts (“Let India remain a free country”, 2020). In another incident reported in ndtv.com, the Calcutta High Court ordered the Mamata Banerjee government to give Professor Ambarish Mahapatra the compensation laid down by the State Human Rights Commission and an additional ₹ 25,000 for legal expenses. Professor Mahapatra was arrested in 2012 for forwarding to his friends a cartoon mocking Mamata Banerjee (Banerjie, 2015). On October 18, 2019, West Bengal police arrested a Congress Bengal spokesperson over social media posts from his home “for circulating posts critical of the TMC government.” (“Congress Says Its Bengal Spokesperson”, 2019). A similar news report in Outlook was published on 4th November 2020 about the arrest of a journalist for Facebook posts “on charges of inciting enmity between the two communities” (Gani, 2020, para. 2). The same journalist Kishorechandra Wangkhem was arrested in 2018 for writing inflammatory posts on social media (“Journalist arrested in Manipur”, 2018). However, in April 2019 the Manipur High Court quashed all allegations against him and released him from jail (“Manipur Scribe Held Again for Sedition”, 2020).

Thus, from the instances discussed above it becomes clear that in most cases people were arrested and social media posts were deleted by the police for writing indecent, objectionable, inflammatory posts and wrongfully maligning the reputation of politicians. However, the justification of arrests made over social media posts remains an unanswered question especially in reference to the rulings of the court of law.

3.5. Fake News in Social Media and Argument Over Necessity and Justification for Social Media Surveillance

The advent of digital technology and the rise of social media have been the hotbed of fake news. Fake news by its definition breaches the primary condition of news, i.e, it not only lacks objectivity but also contains false information. The domain of fake news is much wider than what it seems to be associated with implausible, fantastic stories with catchy and exaggerated headlines coming as constant feeds on the social media platforms (“Fake News and Cyber Propaganda”, 2017). The context of study needs further microscopic analysis as to why social media have become the favourable breeding platform for the spread of such news?

Fake news has proven to be a new concern in modern times. Though social media platforms are normally attributed to the virality of fake news, social media associated with several other factors can
be cited to be responsible for causing fake news to spread to millions of people in the shortest possible time. According to an article published in *Trend Micro*, “Fake News and Cyber Propaganda: The Use and Abuse of Social Media” (2017), fake news needs “three different items to succeed”. These items collectively make a fake news triangle. These factors enable fake news to reach its potential targets. These are tools and services, social networks, and motivation. Tools and services can be very simple and also can include paid services to increase likes and shares whereas, some services can be unusual—that “promise to stuff online polls, while some force site owners to take down stories” (para. 4). Such paid and non-paid tools are widely available nowadays. Social networking sites are where such tools and services are applied. The fake news thus gets the platform or medium to attain virality and ultimately motivation catalyses its spread. People or organizations that spread fake news try to lure people who spend quality time on various social media platforms thereby enabling its wider reach. Often such news or pieces of information come up with catchy headlines and fabricated truth. Thus, it can be rightly categorised as propaganda- where reality is deliberately manipulated. The only change is in the platforms used as propaganda has been in existence for around centuries.

The term Propaganda originated with Roman Catholic Congregatio de Propaganda Fide, meaning Committee for the Propagation of the Faith. It was an order of the church “established by a papal bull in 1622”. It was originally founded to suppress the Protestant Reformation. The term refers to a certain type of communication strategy which involves “no-holds-barred use of communication to propagate beliefs and expectations” (Baran and Davis, 2011, p. 76). Propaganda, misinformation, and fake news have overlapping meanings. These are often associated with causing harm by sharing information either intentionally or unintentionally concerning the promotion of a moral or political cause or point of view. Propaganda, misinformation, and fake news have the power and ability to polarize public opinion, nurture vicious extremism and hate speech which ultimately undermines trust in democracies and democratic processes (*COUNCIL OF EUROPE, n.d.*). According to Fritz Hippler, the head of the film propaganda division of Nazi Germany said the secret to effective propaganda is to simplify a complex message and repeat the simplification over and over again (*World War II*, 1982). We often see such reflection in online news portals and social media platforms. One such misinformation that spread across WhatsApp and Facebook in recent times spoke about the discovery of homemade remedies for COVID-19 by a boy named Ramu from Pondicherry University, India, and has been accepted by the World Health Organization (WHO). The misinformation almost attained virality and was a dominant post across manifold social media platforms. The remedies cited in the message were mainly the homemade remedies Indians apply for treating the common cold (Press Club Media Project, 2020). It was oversimplified because COVID-19 is not a simple common cold disease-causing virus. To date, there has been no official drug to cure the disease and the vaccine candidates are still in the phase of dry run in India and other countries across the world. In such a scenario the virality that this misinformation has attained is scary and immediate attention is required. If people fall into the trap of such misinformation and thereby believe that COVID-19 remedy has been discovered and is easily available they might simply decide not to follow the COVID-19 protocol approved by the WHO, i.e, wearing a mask in public places, washing hands with soap or alcohol-based sanitizer for at least 20 seconds and maintaining social distancing. The fact is that such misinformation has no valid source and the authenticity cannot be traced but still people fall prey to such false claims. In another incident reported in news18 world that in Iran over 300 hundred people died after drinking methanol to save themselves from coronavirus. The information came as fake remedies spread across social media where claims were made that a British teacher and others successfully cured themselves of the coronavirus by consuming whiskey and honey. People wrongly interpreted the message where alcohol-based hand sanitizer was advised and some consumed high-proof alcohol believing it to kill the virus inside their bodies (“Over 300 Killed in Iran”, 2020).

Another aspect that aids the spread of fake news is the strategic and extensive usage of media. In recent times due to the availability of numerous digital and social media platforms, the spread of fake news has become easy and widespread. As Sproule (1994) argues that “effective propaganda is not openly acknowledged as it persuades people without seeming to do so” (p. 3); involves “massive orchestration of communication” (p. 4), and “uses tricky language to discourage reflective thought” (p. 5). According to Baran and Davis (2011), propagandists believe that “end justifies the means” and thus, according to them, it is not only right to tell the half-truths but also outright lies if necessary so
that people believe in what the propagandists want them to believe in. The authors also state that the propagandists rely on “disinformation to discredit their opposition”. They often spread false information about the opposition groups and often lie about their objectives. The source of their claims is mostly hidden and unclear so that “it can’t be traced to the propagandist” (p. 76).

The context to be addressed here is why do people fall prey to misinformation and end up sharing fake news on social media? This is because people have the tendency to believe in the wisdom of the crowd and they are likely to associate themselves with like-minded people. Social networking sites provide us with the opportunity to extend this tendency as people can add, follow and unfollow people according to their preferences and choice. This tendency is known as the echo chamber effect, it is because people only want to assess and consume similar opinions that are echoed with their pre-existing beliefs; any dissimilar opinions are churned out. This is typically dangerous as it narrows down the probability of verifying information sources and strengthens the belief in the wisdom of the crowd. People confuse quality with popularity and thereby end in believing posts that are shared and liked by many. Such social herding is also one of the many reasons why people end up sharing false news (Menczer & Hills, 2020). The authors apart from citing confirmation bias also state information overload to be one of the many reasons why people find difficulty in consuming the bombardment of information people receive every day. Such huge data that people are exposed to every day, they end up believing what their peers, family, and communities share and believe.

Information processing theory can also be attributed in this regard. When people are exposed to manifold and paradoxical information, they often fail to assess all the information coming in their way because of limited cognitive resources. Thus, naturally, people select information based on their preferences so that their cognitive resources can be concentrated to interpret specific information. Some cognitive psychologists argue that human beings must have developed skills to process screening in and screening out information for surviving in the hostile physical environment (Wood & McBride, 1997). Baran and Davis (2011) argued that the modern college generation has pushed their cognitive resources to the limits for constant multitasking they are engaged in and thus are more susceptible to make mistakes and learn what they intend. No wonder this is why after repeated awareness campaigns people fail to identify the fake news and end up sharing what their selected community assumes to be true. The only way to end the cycle of fake news is to make sure that people check, recheck and verify the sources from which the information is coming and this will be only achieved when people are informed, guided and properly educated so that they don’t rely on such arbitrary and unscientific factors.

The above paragraphs dealt with extensive discourses on what makes fake news attain virality and also addressed the core reasons why people tend to fall prey to the looming propagandists targeting people in social networking sites, however further deliberations are necessary to see whether surveillance is the need of the day in such a time when the vulnerability of social media is directly in question.

In a news article published in the Hindustan Times on 6th April, the Assam government arrested 7 people and lodged complaints against 12 more for sharing fake news on social media and further airing and publishing such news about COVID-19 without verifying its authenticity. The government’s information and public relations department filed an FIR against Jugasantra, a vernacular daily published from Silchar for publishing false news reports against the state’s first COVID-19 patient. While the patient was still admitted at the Silchar Medical College Hospital, the newspaper reported that the patient was cured of the disease as the second report came out to be negative. The doctors treating the patient later confirmed the misinformation being spread. A case was lodged against the reporter who filed the story and the publisher of the newspaper under section 188 IPC and provisions of Assam COVID-19 regulation, 2020. The information department of the government further took to Twitter to squash all claims of fake news and also named an English daily, The Eastern Chronicle and Pratidin Time, an Assamese news channel for sharing unauthentic news about COVID-19 patients (“Covid-19: Assam cracks down against fake news”, 2020). Such an initiative taken by the government is praiseworthy. As discussed, the only way the cycle of fake news can be completely stopped is by awaring, informing, and educating the people. People must be exposed to the authentic information as much as possible and any such false claims must be immediately addressed before it attains virality.
Again, in another news article published in *The Hindu*, six people were arrested from the Godavari station coal belt on charges of spreading fake news of two people having been infected with COVID-19 in the region. The fake news shared by them created panic among the people of the region. The police registered cases against them under IPC and section 54 of the Disaster Management Act and section 2 of the Epidemic Disease Act of 1897 (“Six arrested for fake news”, 2020). In a similar vein one news article published in *India Today*, a 32-year-old man was arrested for posting fake news about a Kerala return person having been tested positive for coronavirus and was under treatment in Odisha. The person when questioned revealed that he got the information on the WhatsApp group. However, later investigations by the police confirmed the news to be completely false (“Odisha: 32-year-old held”, 2020).

According to a news report published in *The Indian Express*, a 29-year-old woman was arrested in West Bengal for posting fake news about a doctor being infected with COVID-19 while treating patients afflicted with the disease. The woman was booked under the IT Act (“COVID-19: Woman arrested in Bengal”, 2020). In a PTI story published in *Business Insider*, a Rajasthan health worker was arrested for spreading false information on social media about the number of COVID-19 patients and the number of isolation wards being set up to treat the patients. The person was arrested “for his statement conducting to public mischief” and later terminated for spreading rumors on social media (“Rajasthan health worker arrested”, 2020).

Outright fear due to the fast-spreading COVID-19 crippled the sense of many with such misguided and unverified fake news. Doctors, nurses, health workers were ill-treated, beaten, and even abused both physically and mentally on social media. In one such news report published in *Aljazeera*, a 36-year-old woman doctor was accosted while she returned home after treating COVID-19 patients. She was not only treated as untouchable but also was blocked at the entrance to her apartment and was threatened to face consequences if she continued her work. This came at a time when the government urged people to stop falling prey to false information and treat the health workers as Gods- because they risked their lives to save humanity from dying (“Stigmatised: India’s coronavirus heroes”, 2020).

Health workers were also doxed and received death threats apart from being a subject to online bullying (Arora, Pendergrast & Jain, 2021). Another disturbing incident of similar nature was reported in *The Wire* in Indore where fake videos of healthy Muslims being taken away and injected with the virus made rounds and soon became viral. A team of doctors, revenue officials, and ASHA workers were attacked by the residents due to the panic spread by the fake news. Four people were booked under the National Security Act (“Fake WhatsApp Videos Behind Attack”, 2020). Another news story surfaced in the *BBC* where women doctors and nurses came under attack in Madhya Pradesh where they were not only verbally abused but also stones were pelted towards them (Pandey, 2020). There have been numerous such incidents reported in Indian newspapers of a similar vein and all can be attributed to the sole concern of individual and community fear. Social media escalated such fears to such a height that people took to violence to ‘save’ themselves from the clutches of the pandemic; however little effort was laid in finding out the truth of the stories and believing in any messages that came in their way. As rightly being said in an article published in the magazine, *The Week* that amidst the pandemic the infodemic of fake news has also set its root quite firmly in our consciousness (“Amid the coronavirus pandemic”, 2020).

In critical times when rumour and panic spread faster than news, many important questions need to be asked in this context. However, it should be remembered that though in the year 2020 there has been an exponential rise in the spread of fake news, it is not new and has always been there. Social media were used extensively and as prominent channels for spreading such misleading information. Arrests were made, regulations were imposed but still, such news continued to be spread across multiple platforms going unchecked and unregulated. According to Ahmed (2019), ever since the revelations of the use and abuse of Facebook stemmed out from the 2016 US elections, the social media giant has worked on making things difficult for the foreign actors to manipulate the users with their “advanced ad targeting”. To limit the number of fake stories being shared, Facebook has added third-party fact-checking on viral news stories, added related post listings which appear alongside the highly shared stories, launched page information to check who is behind the post, and published tips and tools to detect and report fake news stories. According to Silverman and Pham (2018) despite all the efforts by Facebook to limit the number of fake stories being spread, 50 of the biggest fake news in the year
2018 garnered around 22 million shares, reactions, and comments on the social media platform. According to the authors, it was only 7% fewer engagements than the 23.5 million engagements generated by the top 50 fake news of 2017, and only a little more than the top 50 fake news identified by BuzzFeed news in 2016, where those links generated a staggering 21.5 million engagements. The answer to why such a trend is still prevalent can be attributed to the article by Silverman (2018) where he said that publishers have changed their domain names to try and stay ahead of the algorithmic changes made by Facebook. Such a tactic blunts the “impact of Facebook’s recent News Feed algorithm changes” (para. 3). Frequent domain hopping also keeps the publishers at bay from blacklisting their websites by the advertisers. People usually don’t notice the Uniform Resource Locator (URL) attached to the news stories that are being shared on Facebook and thus publishers cycle fake news with different domains every time; thereby escalating its further penetration. Thus, even if a website is identified to be sharing fake news and misleading information; it becomes difficult to restrict and blacklist it if the domain remains unknown or changes constantly with time.

In May 2020, BECIL floated an expression of interest document, seeking to appoint an agency that would provide solutions and services, scrutinize information, detect disinformation and verify facts across various social media platforms. This move by the Government of India of building the nation into a social media hub however was jolted after the Supreme Court of India likened it to a move towards a surveillance state (Barik, 2020). However, the Indian government using tools to monitor social media activities and scan data are not new as it has been in practice since 2016 (Shrivastava, 2018). The Ministry of Information and Broadcasting through Broadcast Engineering Consultants India Limited (BECIL) moved an expression of interest for enlisting an entity for the creation of such surveillance tools. The proposed surveillance tools will act as a search engine and would function as both web crawlers and social media crawlers, thereby identifying various hashtags and keywords across eclectic social media platforms. This would further enable the social media surveillance tools to track, monitor, and analyse various trends on different social media platforms (Barik, 2020).

Around 2013-2014 a software named Advanced Applications for Social Media Analytics (AASMA) was developed by Poonurangam Kumaraguru at the Indraprastha Institute of Information and Technology, a Delhi government University funded by the Union Ministry of Electronics and Information Technology which works in a similar vein in monitoring social media posts of individuals, tracking users’ locations and network of connections. The software performs behaviour analysis and even sentiment analysis to determine the nature of posts and tag them accordingly as positive and negative. The alarming fact is that AASMA has been used by at least 40 state and central government departments and agencies for the past 7-8 years (Shrivastava, 2018). That means the social media data individuals put up are under the watchful eyes of the government agencies. This is a chilling fact, especially in parlance to free speech. In a news article published in The Indian Express in the year 2016, the National Security Council Secretariat proposed to establish a National Media Analytics Centre based on media and social media monitoring software. The software would collect background data, analyse past and present social media posts of users, track devices and locations, analyze the users’ preferences and monitor the most visited websites to categorize the contents as potentially troublesome and also if the contents are meant for radicalization. Since then, any information about the National Media Analytics Centre has remained unknown from the public domain. The Unique Identification Authority of India (UIAI)- the agency that looks after Aadhar data floated a tender to hire organizations to monitor social media platforms and posts that were aimed specifically against the agency so that such posts with dissent can be neutralized (Shrivastava, 2016).

However, in 2019 the Centre informed the Supreme Court of India that the UIAI’s plan of hiring agencies to monitor social media platforms has been shelved. (“UIAI’s proposal for social media agency”, 2019). Law enforcement monitoring criminal activities or people who are suspects however can be justified on the ground of maintaining public order and security but monitoring and storing of public data on social media seems unreasonable and can have a devastating influence on freedom of speech and expression as guaranteed in the Indian Constitution.

4. CONCLUSION

Surveillance becomes a cause of concern when democratic institutions are targeted. Activities aimed to monitor the work of journalists and the press can wash the basic fabric of a democratic setup. The right to know and get informed receives a set back when the government uses technology to know
what ‘others’ are doing without their consent and knowledge. There have been numerous incidents of such degree reported from different parts of the globe for quite a time now but, the news of Pegasus-an Israeli spy software aimed to track the cellular activities of Indian union ministers, journalists and opposition leaders have opened up gates of controversy rather than debate; though all such claims have been strongly refuted by the government of India (Bhardwaj, 2021). Constructive discourse and debate regarding its drastic consequences need further scholarly deliberations in full scale.

The world has seen multiple instances where the privacy of the people on the internet has been regularly compromised on different occasions. For instance countries like Ethiopia, Nigeria, Brazil, and China have fallen in Freedom on the net index (Shahbaz & Funk, 2019). The very reason why social media became immensely popular in a very short period is because of its interactivity and flexibility. If the governments continue attacks like this, the very essence of freedom is likely to be lost. Their freedom to express must be retained and reinforced at all costs. Progressive and insightful conclusions always emerge from healthy discourse. Social media posts, even if they are anti-government must be considered by the government as a serious feedback loop. It makes the government know and aware of why their stands have not been accepted and what changes the people want. After all, the government is for the people and not vice versa.

Recently one news surfaced in many Indian newspapers and television news channels where the Ministry of Electronics and IT asked to share details of the social media platforms operating in India as per the new IT guidelines. The new IT rules make it compulsory for the social media platforms operating in India like Facebook, WhatsApp, Instagram, Twitter, Telegram, Koo, etc. to identify from where unlawful messages have originated, identifying and deleting such messages within a stipulated time, setting up a grievance redressal mechanism and assisting the government in the investigation (Bhargava, 2021). Different social media platforms like Facebook, WhatsApp, Instagram, Koo, and Telegram complied with the new guidelines; the only exception was Twitter that raised concerns over the misuse of the new IT rules as they feared it would make way for motivated monitoring of the users (Bhargava, 2021). The standoff escalated between the Indian government and Twitter after the technology minister accused the microblogging giant of not complying with the local laws (“India accuses Twitter”, 2021). Further, failing to comply with the new IT rules beyond the deadline, the social media giant lost its intermediary status in India. This means instead of considering Twitter just as a platform to host various users’ content, it would be directly and editorially responsible for posts published on its platform (Ghosh, 2021). This initiative by the government for combating the rise and spread of fake news, misinformation, and hate posts is praiseworthy but concerns loom over the lack of robust guidelines and transparency which might affect the privacy of the users. It is important to note here that the ripple effects of the provisions imposed due to the new IT rules might have a devastating impact on privacy, security, and freedom of speech and expression (Xavier, 2021).

Social media surveillance has become a reality today. There is no denying the fact that the government employs sophisticated tools to monitor the social media activities of the respondents. Evidence proves that people fall prey to fake news that is spread with predetermined goals. The virality these fake news attain often misleads the population with devastating consequences. It is important to remember that the problem lies not in using the social media platforms but in enlightening the users as to how to select messages amidst a wide array of misleading information. In this regard, it is important to mention John Dewey’s arguments on Pragmatism. He argued that people would learn to defend themselves if they are taught the correct defenses. (Baran & Davis, p. 86). The government must focus on educating people through strategic information campaigns and train them with the defenses to identify fake news rather than prying on the online activities of the users on the pretext of combating fake news.

REFERENCES


[22] Hoofnagle, C. (2019). Facebook and Google Are the New Data Brokers. DLJ@CORNELL TECH. dltech.cornell.edu/post/facebook-and-google-are-the-new-data-brokers


A Study on the Rise of Social Media Surveillance in Modern Times on the Pretext of Combating Fake News


[27] Over half a million Indian Facebook users may have been affected in data breach (2018). The Times of India. Retrieved from timesofindia.indiatimes.com/india/over-half-a-million-indian-facebook-users-may-have-been-affected-in-data-breach/articleshow/63625675.cms


[35] Eight people have been arrested in four states over social media posts in India this week (2019). Scroll.in. Retrieved from scroll.in/latest/977004/in-india-this-week-at-least-eight-people-have-been-arrested-in-four-states-over-social-media-posts


A Study on the Rise of Social Media Surveillance in Modern Times on the Pretext of Combating Fake News


A Study on the Rise of Social Media Surveillance in Modern Times on the Pretext of Combating Fake News


Citation: Debarshi Bhattacharyya. “A study on the rise of social media surveillance in modern times on the pretext of combating fake news” International Journal of Sports and Physical Education (IJSPE), vol 8, no.1, 2022, pp. 25-41. doi: https://doi.org/10.20431/2454-9452.0801003.

Copyright: © 2022 Authors. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.