Volume 1 (2020)
MediaSpace
DME Journal of Communication

# Manipulation, Public opinion and the Use of Social Media for Political Campaigns

Mitisha Sharma[1] & C. Lalmuansangkimi[2]

## Abstract

Political parties and Silicon Valley have had a long standing quid-pro-quo situation since the beginning of the digital revolution. As millennial generation started flooding their homes with internet-of-things and smartphones became old news, politicians had to reinvent their campaigning strategies. While WhatsApp, Facebook, Twitter and Google helped them redesign, it facilitated this transition by ignoring the red-flags. In this research, an attempt has been made to analyse the different ways in which tech giants can snoop on us. Events like Cambridge Analytica scandal only reinforce the fears that politicians can easily employ help of algorithms to sway the political mood. Using quantitative survey and textual analysis, the results have been built on pre-existing research to prove that media literacy is comparatively low in India. In a stark contrast, technology has surpassed all expectations to deliver results that would have been extremely difficult otherwise. Data analytics is helping politicians target voters based on their likes, dislikes, political affiliation, expectations and caste with remarkable accuracy. When this technology builds a bond with low media literacy, a system of deception is established, creating the danger of distorting the very principles of democracy. Every like, comment, page, profile and link that has your digital footprint is tracked and fed to a system that churns massive amounts of data. This system then spits out highly precise predictions of your behaviour that the commercial industry then uses for revenue generation and political industry uses for voter’s attention. In this interface, consumers are left with little free choice. And the fact that most users cannot differentiate between fake news and real events, only adds to the woes. This research sheds light on such malpractices and its repercussions, demonstrating the need for government to act on it.

***Keywords: Data Analytics, Artificial Intelligence, Media Literacy, Elections, Privacy***

[1] Student, IIMC NER Campus, Aizwal, Mizoram, mitishasharma27@gmail.com
[2] Assistant Professor, IIMC NER Campus, Aizwal, Mizoram, clalmuansangkimi@gmail.com

## 1. Introduction

**"AI is actually a bit like a psychopath. It's adept at manipulating emotions, but underdeveloped morally. They're going through a stage of moral development, and we need to look at how moral development happens in AI." - John Rust, Director of Psychometrics Centre, University of Cambridge**

As gadgets in the 21st century get smaller and lighter, surveillance too has taken a big leap from small scale human eyes to compulsive inescapable computer algorithms. Going off the grid in this world is next to impossible. You wake up to the sound of your alarm, which you occasionally ask your personal Artificial Intelligence (AI) friend Google Assistant to set. The next thing you do is check your phone for important updates on Facebook, WhatsApp, Gmail, Twitter, Instagram, Amazon, Snapchat, Truecaller and Messenger. You then get ready and leave for work. On your way to work you dive into the black-hole of the internet. From catchy yellow journalism websites to serious New York Times (NYT) opinion columns, you hop on the cookie wagon and jump from one host to another. While you were devouring the plethora of information thrown at you from such websites, you were being followed endlessly by carefully crafted algorithms to trace your likes, dislikes, behaviour pattern and gullibility.

To answer a simple question of why they do this? The most presumable reason would be to generate revenue by selling your personal information to advertisers. But there is more to it. When enterprises have access to such a detailed database of citizens involving their financial, commercial and personal information, their ethical standards can be easily influenced by totalitarian regimes and profit-oriented business models. Facebook is already facing ire for its dubious privacy manual. In 2019 alone, there were three odd instances of leaked databases that were unprotected by any password, making them easily accessible by anyone. Phone numbers, location check-ins, comments, IDs and other personal information of hundreds of millions of users were exposed online.

However, Facebook says it's committed to stopping such data breaches with stronger protection mechanisms and allows users significant control over their privacy settings. But what happens when Facebook voluntarily provides access of user information to political parties and their associates during elections? This may sound dystopian but it has already happened.

The Cambridge Analytica scandal sheds light on how personal data can be mined from Facebook to psychologically manipulate voters during elections. While we can argue that this scandal remains an odd nail in the otherwise secure coffin of Facebook atmosphere, there have been multiple studies that highlight how social media troops are hired by political parties to carefully drive voters towards a politician.

India is home to the world's largest democracy with around 900 million eligible voters as of 2019 voters list. In May 2019, these voters geared up to elect their government. As incumbent Narendra Modi made a strong comeback, many researchers found an increase in cyber troop activity on Facebook, just before elections. "Cyber troops" are defined as government or political party actors tasked with manipulating public opinion online (Bradshaw & Howard, 2017). Besides cyber troop activities, increase in fake news and misinformation, disinformation, mal-information, deep fakes, targeted advertisements shared as news, and trolling are also on the rise. But, are we really sure that the state will stop here?

In the age of Internet-of-things, we want smooth interconnectivity between different apps, websites and gadgets. You may not like entering your same Gmail password on your cell phone, laptop and tablet. So, you provide Google access to remembering different passwords for different accounts, making your life simpler but not safer. Every day when you provide access to your contacts, camera, microphone and location, you are allowing the inescapable eye of the algorithm to follow you. In the age of globalization, all these websites and apps share your information to target advertisements catering to your personal needs. But trouble could brew when this lucrative data lands in the hands of an organization with vested interest. For instance, if a Political Party has access to your political opinions, likes and dislikes, it can easily employ the help of automation and AI to manipulate your opinion towards their cause. With sophisticated AI software, they can map and dissect every geographical location to show how many citizens and which communities are in their favour. This can help them target individuals who are against them by analysing their behaviour patterns and political opinions.

This study analyses how political parties can readily mine such data with the help of poor data protection laws, forceful compliance and constant surveillance to manipulate your opinion during elections campaigns. It aims at identifying the methods employed by tech agencies to monitor data and analyses the frequency in which this happens and vulnerability of users to such practices. An attempt is made to establish the level of media literacy among voters in India. It tries to understand and answer why political parties are running elections on the internet and what all they can gain from this media. It also attempts at answering how the commercial and political waves interact on social media while put forward an idea of surveillance and its future.

## 2. Narratives on Rigging of Democratic Game: A Literature Appraisal

2016 was a big year for democracies. Two countries separated by the Atlantic Ocean geared up to change the course of their future. As Americans voted to elect the next US President, Britain voted to leave the EU, kick-starting the Brexit chaos. These two parallel events joined tails in 2018 when whistle-blower Christopher Wylie revealed about Cambridge Analytica.

Christopher Wylie alleged that Cambridge Analytica, a London based elections consultancy firm, harvested personal data of tens of millions of Americans from Facebook. Britain's Channel 4 News came out with an explosive sting operation featuring firm's CEO Alexander Nix. He was caught on camera admitting they use sex workers, misinformation, bribes and manipulation tactics to help political candidates win. But this was not as shocking as what came next. In the run up to the 2016 Presidential elections, Cambridge created psychographic profile of millions of Americans, which it later used to influence voter's sentiments.

Academic Aleksandr Kogan and his company Global Science Research created an app called "thisisyourdigitallife" in 2014. Users were paid to take a psychological test and the app collected the data through Facebook. It also gathered data on a person's Facebook friends, according to the reports (Meredith, 2018). This data was later sold to Cambridge Analytica.

Christopher Wylie revealed to NYT and the Observer in the UK that the firm created a software to influence voters in America. Wylie claimed the data sold to Cambridge Analytica was then used to develop "psychographic" profiles of people and deliver pro-Trump material to them online (Meredith, 2018). Similar tactics were used by the consultancy to deliver pro-Brexit results. Facebook claimed that even though Kogan's app acquired data legitimately, he violated the terms and conditions when he sold it to a third party. 2016 "Brexit" campaign used a Cambridge Analytica contractor to help skirt election spending limits. The story implicated two senior advisers to Prime Minister Theresa May (Confessore, 2018).

The idea behind Aleksandr Kogan's app was not new. As a professor of psychology at University of Cambridge, he was already aware of the research done by David Stillwell and Michal

Kosinski of the Psychometric centre at the University. In 2013, they came out with a study which predicted behaviour of users accurately using just their Facebook likes.

They show that easily accessible digital records of behaviour, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender. The model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases (Michal Konsinski et al., 2013).

*If you want to keep a secret, you must also hide it from yourself*. - George Orwell, 1984

Before revelations made in 2013 by Edward Snowden, an ex-National Security Agency (NSA) Contractor, the term Global Surveillance was not mainstream. His documents exploded in the media like an atomic bomb. The Washington Post and The Guardian became the first to publish the top secret documents in July 2013. These reports revealed how NSA and its international allies had a massive surveillance system in place for US and foreign citizens. They used Boundless Informant to visualize large sets of metadata on the internet and telephony data of millions of citizens.

This highlighted how NSA in compliance with intelligence agencies of the UK, Germany, Netherland, Australia, Denmark, France, Italy, Norway, Spain, Switzerland, Singapore and Israel shared and received data on millions of citizens. The documents showed that in more than one surveillance programs, private entities like Facebook, Google, Apple, Microsoft, Verizon Business, Vodafone cable and British Telecommunications were involved as commercial partners.

While surveillance is the biggest of all threats to privacy, when it comes to manipulating your choice, cyber troops are not far behind. As tech companies are working on sophisticated gadgets and software that track you everywhere - extent of which are still not known - cyber troops are more mainstream and established in the cyber swaying industry. India itself is home to political cyber troop that are deployed before elections with only one goal, spread as much misinformation as possible. Even though there has been a significant rise in the miniscule chunk of intellectuals well-versed with this art and thus, are immune, there are millions of unaware citizens in India that fall prey to such propaganda through social media channels like WhatsApp and Facebook.

In the lead-up to the 2019 general election, cyber troop capacity has grown significantly as compared to 2017 in which only few actors were involved in social media manipulation. In the words of Samantha Bradshaw, "Political parties are now working with a wider-range of actors including private firms, volunteer networks, and social media influencers to shape public opinion over social media". "At the same time, more sophisticated and innovative tools are being used to target, tailor, and refine messaging strategies including data analytics, targeted advertisements, and automation on platforms such as WhatsApp" she added. (Samantha Bradshaw, 2019, p.1).

Samantha Bradshaw further said, "Political parties in India have also been known to work with private firms." Whistle-blower Christopher Wylie also revealed that Cambridge Analytica "worked extensively in India". "The Indian IT firm Silver Touch was responsible for building Modi's NaMo app, and was linked to fake Facebook accounts" said Samantha Bradshaw (Samantha Bradshaw, 2019, p.2).

Besides cyber troops, political parties employ automation, data analytics and trolling to boost their status. Quartz India report pointed out that as a way to better target their messages, political parties are, nowadays, employing data analytics to help them create groups based on demographic and socio-economic factors. (Singh, 2019).

The Quartz India report added how easy it is for analysts to gather a person's detail personal information such as name, age, parents' name, address and voter ID number from publicly made available electoral roll information. "In many large states of India, such as Uttar Pradesh and Bihar, the caste of over 70% of people can be determined simply by analysing their names" the report explained (Singh, 2019). Parties can gather all this information, including phone numbers and socio-economic status through publicly available data like land records, BPL list, NSSO surveys, electricity bills etc.

## 3. The Orwellian State…?

*"Every day those two plus billion people pour into Facebook's servers live documentaries of their lives and the lives of those around them….haring with the company their most intimate and dangerous secrets for it to do as it sees fit"* – Kalev Leetaru (Forbes Journalist for AI and Big Data)

Facial recognition software for surveillance systems across the world is not uncommon. Tech giant Facebook has earlier proposed services to businesses where it can offer an enormous database of pictures from the networking site to facilitate smoother functioning of facial recognition software. Every picture you upload or every time you or your friends tag you in picture, you are making yourself vulnerable to all these software that can recognize you on streets by using an algorithm.

An article titled '*Facebook's Automated Ad Labels Plus Facial Recognition: The Real-Life Minority Report?'* on Forbes.com written by Kalev Leetaru said, "One patent application envisions Facebook selling a commercial service to retail companies to hook into their surveillance camera networks to perform facial recognition on every person walking through their stores, connecting them both to their real name and to every data point Facebook has about their interests." He further added, "The patent further envisions using all of Facebook's information about that user and their friends to assign a "trust" score to each shopper that would be used to determine how they are treated in the store and what security measures might confront them" (Leetaru, 2018).

To explain the competency of Facebook to carry out tracking, Kaley Leetaru used a country where homosexuality warrants death penalty as an example and wrote, "Facebook will hoover up every data point it can acquire about you and watch your every move to guess your sexual orientation and provide that as a label on your account, ready for your government to issue a legal request to Facebook to get your name and arrest you" (Leetaru, 2018).

Distance between the present and such dystopian scenarios is smaller than we can imagine. With access to our name, number, political preference, likes, dislikes and, sexual and mental orientations, it's not hard to imagine a global surveillance and intelligence network that can be dangerous not only for dissent but for mental and physical freedom of an individual as well.

Imagine a situation where you are randomly discussing a French Press coffee maker with your colleagues. At night when you decide to cosy up in your bed and begin an endless swiping exercise on social media, an innocent advertisement pops up. But it's not any ordinary advertisement. It proudly displays the same French Press you were discussing about. However, this advertisement will tell you that you are a lucky customer as it comes at half the store bought price from Amazon. Spooky, isn't it? But we don't have to imagine this situation as we've suffered this invasion multiple times.

When Silicon Valley came up with personal AI assistants like Google, Alexa, Cortana and Siri, consumers were thrilled. It's fun to say Hey Google! wake me up in an hour. What we didn't anticipate was what if turns on by itself and starts listening to our conversations. To use an AI assistant, you have to give away access to your contacts, microphone, location and camera. Hidden away in their terms and conditions, that you agreed to in a jiffy, is a clause that gives them permission to use your voice to train the assistant. Although, how can you be sure that's all the company will do with your voice and thoughts?

Tech companies wanted their products to be flawless. They envisioned a device so smart that it can identify dialects, cultural idiosyncrasies, emotions, mood and cravings. To help build a system this intelligent, they started employing low-paid temps to transcribe voice recordings from Google Home, Echo's Alexa and Siri. "So-called smart devices inarguably depend on thousands of low-paid humans who annotate sound snippets so tech companies can upgrade their electronic ears; our faintest whispers have become one of their most valuable datasets" (Carr et.al, 2019).

Carr et.al explained, "In 2015, the same year Apple Chief Executive Officer Tim Cook called privacy a 'fundamental human right', Apple's machines were processing more than a billion requests a week. By then, users could turn on a feature so they no longer had to push a button on the iPhone to activate the voice assistant; it was always listening." While elucidating on user agreement legalese, the article clarify Apple's intention to record data solely for the purpose of improving Siri, but it did not mention that fellow humans might listen (Carr et.al, 2019). There have been instances where voice recordings were initiated accidently by a kid and his parent private conversations get recorded. Kids reading out credit card numbers, house addresses, phone numbers and other private information can be recorded by your smart speaker. This will eventually be transcribed by a human who can misuse this. But scarier than this is the idea of it landing in the hands of the government.

Unlike Cambridge Analytica's psychoanalysis trick, this is more accurate and efficient in recognizing who favours which political party. When Silicon Valley is listening to everything you say, every confession, thought, preference, allegiance, likes and dislikes can be used against you in mysterious ways. "The risks of inadvertent recording grew along with the use cases" said Mike Bastian, a former principal research scientist on the Siri team who left Apple in 2019. "The Apple Watch's "raise to speak" feature, which automatically activates Siri when it detects a wearer's wrist being lifted, as especially dicey. There was a high false positive rate" the article further said (Carr et.al, 2019).

We know that Google saves our location when we open location on our smartphones to use Maps. But what most of us are unaware of is that it also tracks you wherever you go with your smartphone, whether you use any Google service/apps or not. This setting called 'Location History' is always on by default. On your Google account it is described as, 'Saves where you go with your devices, even when you aren't using a specific Google service, to give you personalized maps, recommendations based on places you've visited, and more'.

This is the reason why you get a pop-up for review when you visit a new place even when the location of your device is off. If you have a curious and conscious mind, a simple search will direct you to forums that can give you information on how to turn the setting off and its repercussions. However, an investigative story by AP news shows how Google continues to store your location data even after you turn location history off.

This deceptive privacy setting is found just above location history on your Google account. It is called 'Web and App activity' and it is described as, "Saves your activity on Google sites and apps, including associated info like location, to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services." Given how it's placed right above location history, many users thought that both are not aware that their location will still be tracked unless both are off. In its defence, Google claims that a disclaimer informs them before pausing location history but as a user, it is hard to find that hidden inference in sugar-coated words of enhancing user experience.

Every new app on the phone brings with it a new set of trackers. Websites track and monitor your every move with the help of cookies. These little bugs know where you've been and what you like. Tech companies rely on them heavily to ease internet browsing experience and improve their targeted advertising strategy. The terms and conditions pop-up that we promptly agree to, entails a wide range of permissions that monitor your phone's battery, your IP address, name, location, camera and microphone. The ambiguity in the text has led to shocking ramifications.

Companies across all sectors now rely on your personal data to boost their profits. This can be sometimes direct and mostly indirect. What if a company wants you to wear a Fitbit and give them your health data so they can analyse your profile? To explain this, Ingraham wrote, "John Hancock Life Insurance Company made a splash…with the news that all its policies would….let the company track your fitness — via either a website or an app, or through the use of a fitness tracker like an Apple Watch or Fitbit." The more active people are, the more their insurance premiums go down (Ingraham, 2018).

Or if cab services start exploiting your battery data to jack up the prices of cab rides right when you desperately need the service? Withnall in his Article 'Uber knows when your Phone is running out of Battery' wrote, "Uber knows when the battery on your phone is running low – and that you are more likely to pay higher "surge" prices for a car as a result." "Uber knows whether a user is on low battery because the app needs to use that information to go into power saving mode" he added. (Withnall, 2016). Amazon's AI Alexa can predict your mood based on what you've ordered for dinner or the songs you play. Company is already working on its social cues to predict your feelings based on your voice and command.

Facial recognition software is now smarter and cheaper (less than $100 on Amazon), making it a delectable technique for surveillance. Using just a simple software and footage from public web cameras, a team from NYT could identify a stranger through his social media profile. The fact that your images on publicly available identifications like, Driver's license, Aadhar card, Pan Card, Facebook and other social media profiles can land you in a bottomless pit of databases for anyone to exploit, is alarming.

When lawmakers and tech companies resonate with each other, no matter how different their goals may be, the scope of truth and free choice is very limited. As we have seen how they exploit our deepest desires to our most desperate needs, all this information is carefully stored in the form of databases and profiles that governments can access to influence your democratic rights. Though tech companies have the right to use this data for advertising, nothing is said about a secondary deal with the government. While Facebook claims Cambridge Analytica scandal was an extraordinary case, with the level of surveillance and the frequency of leaks, their assurance is not very reassuring.

## 4. Critical Appraisal of Research Methodology

Accessing the psychological traits of consumers has become relatively easy for Silicon Valley. In contrast, citizens are yet to fully understand the extent and consequences of this serpentine tracking. To analyse the awareness of voters consuming large swathes of data, a quantitative approach was employed. Poor media literacy is the biggest nail in the coffin of surveillance and manipulation. When citizens are not aware of terms like Filter Bubble and selective targeting, they can easily fall prey to hidden propaganda and illegal data transfers.

Using Google forms, a questionnaire was circulated randomly to people who were eligible to vote by 2019. The form was not demographically restricted and anyone with access to social media and an interest in current affairs was encouraged to participate. Questions were basic and obvious to invite people from different backgrounds as volunteers. Starting with name, age and occupation, questions went on to access their knowledge about terms like propaganda, Filter

Bubble, preferred social media channel, fake news and misinformation. Responses were statistically analysed to provide a general overview of media literacy in eligible voters across India.

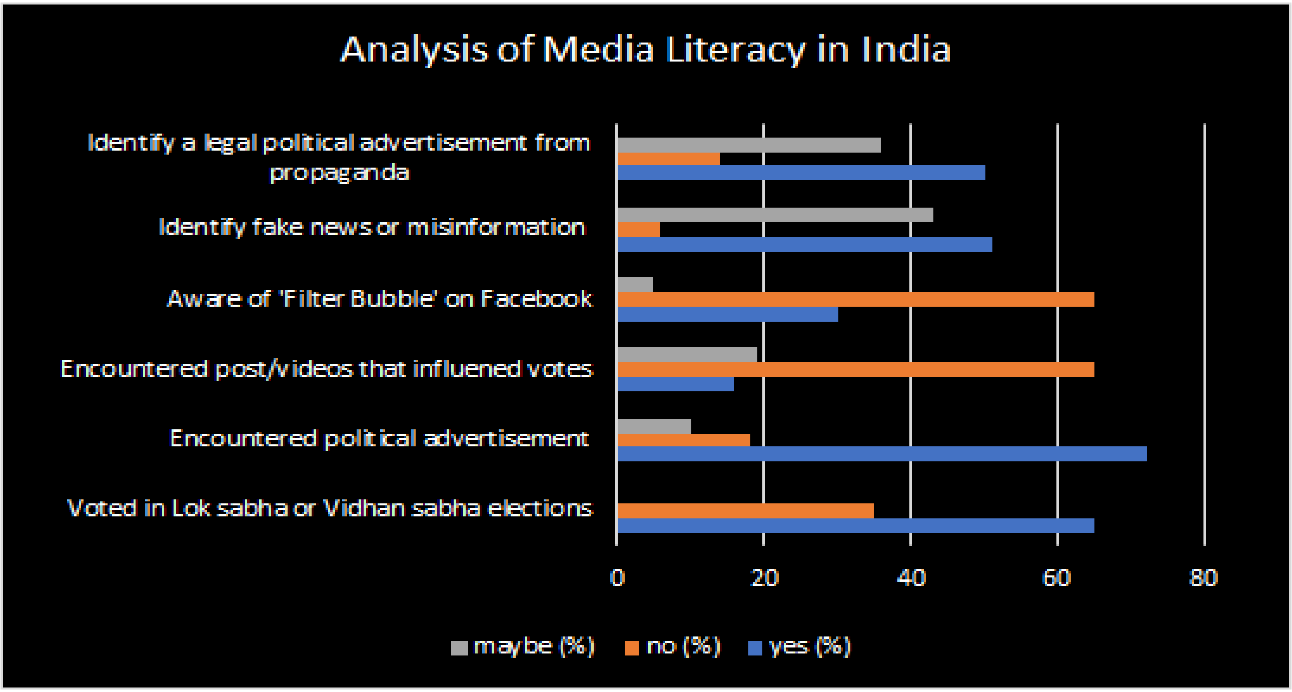
There were no descriptive questions. That increased the chance of concealment on the part of respondents. To tackle that, another option 'maybe' was added next to yes and no. Three similar questions like, 'can you identify a legal advertising message from propaganda?', 'did you encounter post/videos that influenced your vote to a certain extent?' and 'can you differentiate between fake/misinformation and actual news?' were posed to filter out candidates who seemed unsure or lied on any of these.

Besides quantitative questionnaire, qualitative data was drawn from valid discussions and informal interviews for the purpose of analysing some points and establishing relevance. This research is very fluid in its context and tries to report things that have already happened with equal importance and urgency.

## 5. Interpretations

Through a randomized quantitative survey, this study finds that media literacy is poor among eligible voters of India. Voters between age group 18-30 constituted 60% of the survey while only 2% were above 60. Around 50% were students and 60% voted recently in either Assembly or Parliamentary elections. When asked whether they can identify a legal political advertisement from a propaganda message, 50% picked yes, while 14% chose no and 36% maybe. Similar traits were visible for questions related to identification of fake news or misinformation from real news. 51% opted for yes and only 6% said no. However, 43% chose maybe, suggesting that they are not aware of tipping points associated with fake news.

**Figure 1: Media Literacy among eligible voters in India**



**Source: Primary Data**

More than 70% encountered political advertisements but only 16% confessed that they saw posts/videos that influenced their votes. 19% were not sure and 65% said their votes were not influenced by social media posts. These numbers show that media literacy is not bad in our country but the next question proves this wrong. Around 70% of the participants were completely unaware of the concept of Filter Bubble. This concept is responsible for what appears on your wall and thus affects your opinions and ideologies. When consumers claim ignorance against social media strategies, they lose the argument of free choice. If they are not aware of the reason why their Facebook wall appears like an ideological supplement, they might think that their political choice is a free will, although, often it's not.

This survey shows that media literacy in India is still significantly poor. Tech companies are consistently utilising loopholes to gather data on users and help advertisers build profile-oriented ads. There have been cases where governments have used these profiles to infiltrate political affiliations and disseminate propaganda. When nearly half of the participants cannot differentiate between fake news and real news, their free will can be easily steered to any direction preferred by the algorithm.

## 6. Analysis: Elections of the Future

Governments across the world are already purchasing commercially available data for law enforcement activities. Apps on your smartphone can access your location in the background even when you’re not using it. This default setting needs to be changed manually to ‘only when using the app’. When governments have access to your tracks and personal choices, it's easier for them to target your soft spot. These apps collect and share all sorts of data on users. Right from your ovulation cycle to your preferred political party, all your favourite apps are on the same page when it comes to data harvesting. This data is shared and bought by Data Brokers for advertisers, agencies and governments. Silicon Valley claims that data collected by apps on an individual is dismembered and sold separately but experts suggest that when all transactions occur on the same level, it’s easier for an algorithm to reassemble the bits and pieces.

Algorithms on Facebook can make remarkably accurate predictions about your likes, dislikes, nature of relationships with friends, political affiliations, personal quirks and habits based on what you see, post, like and comment while using the app. Now imagine this data ending up with the data analytics team of a political party.

In the words of Vaidhyanathan, “Facebook allowed Donald Trump to target advertisements at voters in select states with remarkable precision. In some cases, Facebook Ads were meant to dissuade potential Clinton voters.” The Trump team also cautiously tailored and tested Facebook Ads to motivate small segments of potential Trump voters so they might show up at the polls. It worked (Vaidhyanathan, 2018, P. 149).

The Cambridge Analytica scandal highlighted the extent to which psychographics can harm the integrity of democracy. But there is no formal law against the practice. How you source the data predicts how legal your analysis is. You can employ a hacker to illegally steal data on millions of users. Or, you can purchase data from data brokers. You can also hire a political data analytics firm like Cambridge to do the dirty job for you. In any scenario, users will be exposed to Ads that can manipulate and exploit their free choice.

### 6.1 Can a law protect our privacy?

It must be noted that there is no guarantee that a law will save consumers from political and commercial surveillance. Indian government’s Personal Data Protection Bill, 2019 tabled in the Indian Parliament has been criticized for possible discrepancies that a bill meant to protect consumer data can only benefit tech giants and governments. While the bill focuses on consent, limits the use of personal data and promotes data localisation, the loopholes in its structure, some said it provides sweeping powers to central government. "Its execution will be tricky and result might be disappointing", they added. Following is an analysis as to why experts are not optimistic with this 'progressive' step in 3 simple points:

a. Much of the complexities concerning the law are left for the Data Protection Authority of India (will be formed after the bill becomes law) to formulate. This includes definition of critical personal data and establishing the lawful, clear and specific purpose for which personal data can be processed. Until instructions and definitions are clarified, the extents to which our data will be protected will remain unknown.
b. Section 35 of the bill grants central government authority to exempt government agencies from its implementation. It also allows them to surpass all safeguards in matters related to security of the state. Governments can process personal data without consent for providing benefits and legal matters.
c. Social media intermediaries will have to abide by its mechanism and ensure explicitly that consent is taken while processing sensitive data. While this seems like a good move, the Intermediaries Guidelines rule issued in 2018 leaves little room for independence from the government. These intermediaries will be obligated to remove any type of content hosted on their portals, if deemed unfit or unlawful by the government, within 24 hours. Besides providing assistance to the state in matters of unlawful content, they need to deploy automated tools for detecting such posts.

Some argue that the bill talks about explicit consent, grievance redressal mechanisms and empowers consumers to edit, remove, track or opt out of data tracking. However, in a country like India, where media and digital literacy is exceptionally low, these mechanisms will bear no fruit. This, if tied to state-sponsored psycho-surveillance, can easily give birth to Cambridge Analytica 2.0.

You can claim that even after such interferences with the mind and social media profiles, one can execute their 'free will' and avoid manipulation but scientists argue that free choice is just a manifestation of our liberal theory. Harari explained the reason why some prefer voting for the Conservatives rather than the Labour party. He said that he did not choose any of these wishes. And, he felt a particular wish welling up within him as "this is the feeling created by the biochemical process in my brain." "In the paddington of my brain, I might be compelled to embark on a particular train of reasoning by deterministic processes, or I might hop on at random. But I don't freely choose to think those thoughts that will make me vote Conservative," she added. (Harari, 2017, p. 330-331).

So, if you like a particular political party and use a smartphone, there can be chances that you prefer that party because of its presence in your life. In the background, that party might be using your likes and dislikes, contacts, personal interests and location data to target pro-party ads while completely alienating you from dissent and opposition.

## 7. Conclusion

Innovations in elections are already troubling the level playing field in India. Political stalwarts are using apps, social media giants and algorithms to rig the liberal game. From Congress leader Bhavya Bishnoi's android app to BJP leader Manoj Tiwari's use of deep fake technology to target multilingual population, campaigns are crossing innovation barriers and privacy barriers to strike deep into the minds of voters. Attacks like using Pegasus snoopware on WhatsApp and Google's disclosure about spying activity by government-backed hackers are growing in numbers. When the richest man's phone can succumb to data theft, we are not left with much hope of safe cyber practices.

Even without such attacks, governments are capable of curating smart tools using commercially available surveillance data, courtesy of Artificial Intelligence. With weaker laws, our love for social media, Silicon Valley's dependence on our interests and growing interest of the government in digital gold, one can expect the political hustle to completely shift on cell phones and laptops. While you connect your smart watch to your smart TV, ask Alexa to share some international news and reorder your favourite coffee, a giant pervasive army of algorithms and state-sponsored infiltration programs are working day and night to map your social-graphs. Why? For advertisers it means more money and for politicians it means more years.

For a coherent and symbiotic relationship, both variables have to move in sync. But, while governments are utilizing the power of technology, consumers are lagging far behind in shielding themselves from its misuse. When one variable takes a giant leap of faith and other continues to undermine its consequences, it is no longer a symbiotic association. For former, it's all jingles and mammoth-sized profits, for latter, it's a deal that makes the Orwellian state sound less shocking.

## References

Bradshaw, Samantha & Philip N., Howard (2017). *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Accessed from https://comprop.oii.ox.ac.uk/ research/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/

Campbell-Smith, Ualan & Bradshaw, Samantha (2019). *Global Cyber Troops Country Profile: India*. Oxford Internet Institute, University of Oxford https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/ 2019/05/India-Profile.pdf

Carr, Austin et.al (2019). *Silicon Valley is listening to your most intimate moments*. Accessed from https://www.bloomberg.com/news/features/2019-12-11/silicon-valley-got-millions-to-let-siri-and-alexa-listen-in

Collins, Keith & Dance JX ,Gabriel (2018). *How Researchers Learned to Use Facebook 'Likes' to Sway Your Thinking*. https://www.nytimes.com/2018/03/20/technology/facebook-cambridge-behavior-model.html

Confessore, Nicholas (2018). *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*. Accessed from https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
Dreyfuss, Emily (2018). *Google Tracks You Even If Location History's Off. Here's How to Stop It*. Accessed from https://www.wired.com/story/google-location-tracking-turn-off/

Flaxman, Seth et.al (2016). *Filter Bubbles, Echo, Chambers, and Online News Consumption.*

Harari, Y. (2017) *Homo Deus - A Brief History of Tomorrow*, (rev. ed) London: Vintage (Penguin Random House)

Hogan,Mél & Shepherd, Tamara (2015). *Information Ownership and Materiality in an Age of Big Data Surveillance*. Journal of Information Policy , 2015, Vol. 5 (2015), pp. 6-31. Published by: Penn State University Press. Stable URL: https://www.jstor.org/stable/10.5325/jinfopoli. 5.2015.0006

Ingraham, Christopher (2018). *An insurance company wants you to hand over your Fitbit data so it can make more money. Should you?*Accessed from https://www.washingtonpost.com/business /2018/09/25/ an-insurance-company-wants-you-hand-over-your-fitbit-data-so-they-can-make-more-money-should-you/

Lapowsky, Issie (2018). *The Man Who Saw the Dangers of Cambridge Analytica Years Ago.* Accessed from https://www.wired.com/story/the-man-who-saw-the-dangers-of-cambridge-analytica/

Leetaru, Kalev (2018). *Facebook's Automated Ad Labels Plus Facial Recognition: The Real-Life Minority Report?* Accessed from https://www.forbes.com/sites/kalevleetaru/2018/07/18/facebooks-automated-ad-labels-plus-facial-recognition-the-real-life-minority-report/#2ab799176808

Leetaru, Kalev (2019). *Global Mass Surveillance And How Facebook's Private Army Is Militarizing Our Data*. Accessed from https://www.forbes.com/sites/kalevleetaru/2019/03 /11/global-mass-surveillance-and-how-facebooks-private-army-is-militarizing-our-data/#31a25cd81786

Levitin, Daniel J. (2016). *Weaponized Lies: How to think critically in the Post-Truth Era.* Dutton, New York

Meredith, Sam (2018) *Here's everything you need to know about the Cambridge Analytica scandal*. Accessed from *l* https://www.cnbc.com/2018/03/21/facebook-cambridge-analytica-scandal-everything-you-need-to-know.html

Michal Konsinski et al. (2013). *Private traits and attributes are predictable from digital records of human behaviour*. https://www.pnas.org/content/pnas/110/15/5802.full.pdf

Orwell, George (Reprint 2018). *1984.* Published by Prakash Books India Pvt. Ltd.

Public Opinion Quarterly, Vol. 80, Special Issue, 2016, pp. 298–320

Singh Shankar, Shivam (2019). *A former BJP data analyst reveals how the party's WhatsApp groups work*. Accessed from https://qz.com/india/1553765/bjps-whatsapp-ops-is-what-cambridge-analytica-can-only-dream-of/?utm_source=facebook&utm_medium=qz-organic

Stephens –Davidowitz, Seth (2017). *Everybody lies: What the internet can tell us about who we really are.* Bloomsbury Publishing, London, UK

Vaidhyanathan, S. (2018) Antisocial Media - How Facebook Disconnects Us and Undermines Democracy, New Delhi: Oxford University Press

Withnall, Adam (2016). *Uber knows when your Phone is running out of Battery*. Accessed from https://www.independent.co.uk/life-style/gadgets-and-tech/news/uber-knows-when-your-phone-is-about-to-run-out-of-battery-a7042416.html