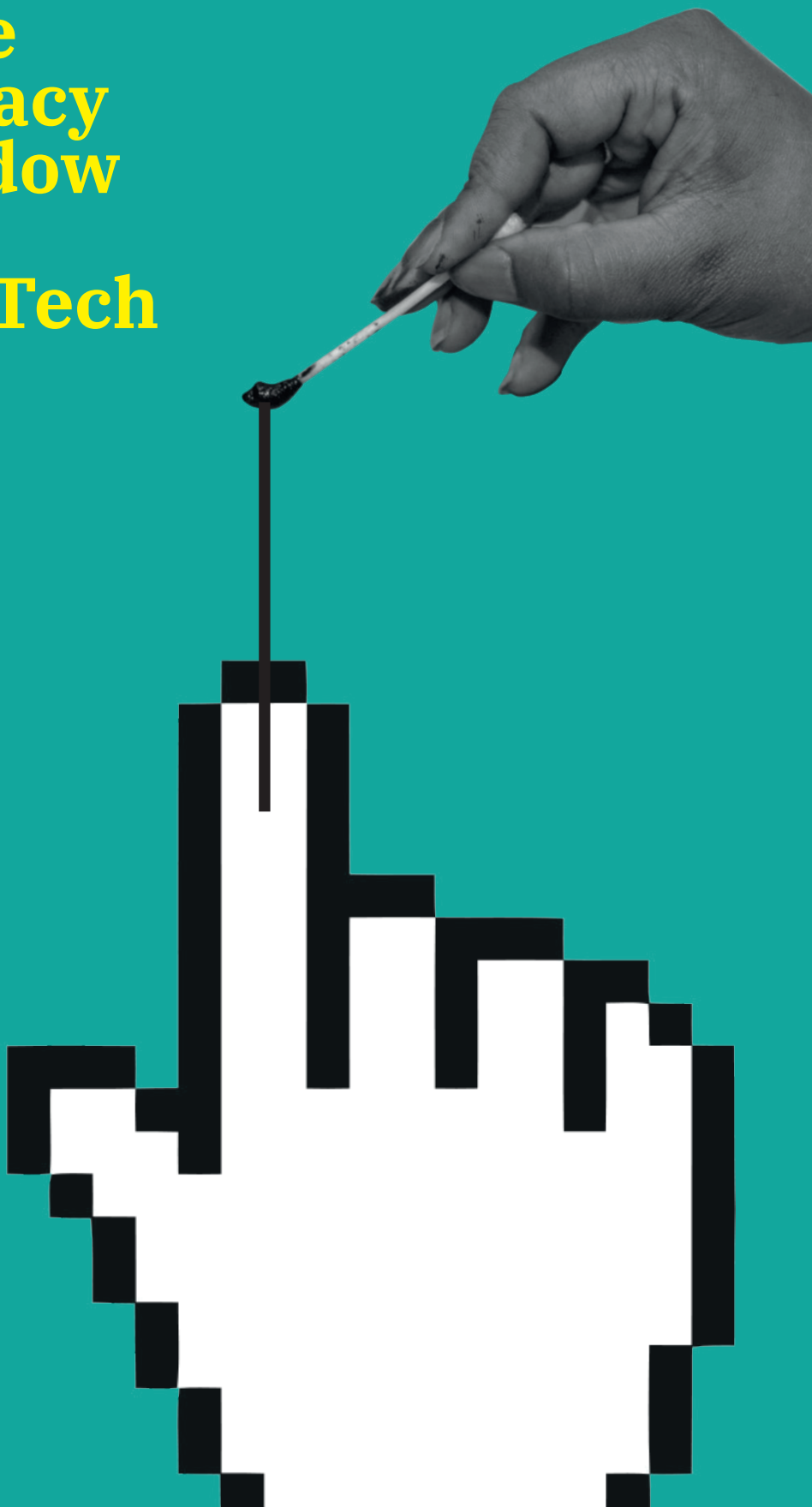
The Future of Democracy in the Shadow of Big and Emerging Tech



Centre for Communication Governance,
with support from the
Friedrich Naumann Foundation for Freedom (FNF)

Published *by* National Law University Delhi Press, Sector 14, Dwarka. New Delhi 110 078

ISBN: 978-9384272-28-9

Design *by* Ram | ramanaya.net

Supported *by*
Friedrich Naumann Foundation

We thank Smita K. Prasad for conceptualising and helping curate the essays for this publication.

Edited *by* Kritika Bhardwaj, Sangh Rakshita and Shrutanjaya Bhardwaj

Editorial Assistance provided *by* Aanchal Khandelwal, Karthik Rai and Mustafa Rajkotwala

Contents

Introduction

Technological invasion of law and society has invited significant criticism. This includes conversations on the dangers posed by 'Big Tech' to democracy generally and civil rights specifically. The Centre for Communication Governance, National Law University Delhi brings to you this series of essays—written by experts in the domain—in an attempt to collate contemporary scholarly thought on some of the narrower sub-issues that arise in this context.

Our first essay addresses the basic but critical question: What *is* 'Big Tech'? Urvashi Aneja & Angelina Chamuah present a conceptual understanding of the phrase. While 'Big Tech' refers to a set of companies, it is certainly not a *fixed* set; companies become part of this set by exhibiting four traits or "*conceptual markers*" and—as a corollary—would stop being identified in this category if they were to lose any of the four markers. The first marker is that the company runs a data-centric model and has massive access to consumer data which can be leveraged or exploited. The second marker is that 'Big Tech' companies have a vast user base and are "*multi-sided platforms that demonstrate strong network effects*". The third and fourth markers are the infrastructural and civic roles of these companies respectively, i.e., they not only control critical societal infrastructure (which is often acquired through lobbying efforts and strategic mergers and acquisitions) but also operate "*consumer-facing platforms*" which enable them to generate consumer dependence and gain huge power over the flow of information among citizens. It is these four markers that collectively define 'Big Tech'. [U. Aneja and A. Chamuah, *What is Big Tech? Four Conceptual Markers*]

Since the power held by Big Tech is not only immense but also self-reinforcing, it endangers market competition, often by hindering other players from entering the market. Should competition law respond

to this threat? If yes, how? Alok P. Kumar & Manjushree R.M. explore the purpose behind competition law and find that competition law is concerned not only with consumer protection but also—as evident from a conjoint reading of Articles 14 & 39 of the Indian Constitution—with preventing the *concentration* of wealth and material resources in a few hands. Seen in this light, the law must strive to protect "*the competitive process*". But the present legal framework is too obsolete to achieve that aim. Current understanding of concepts such as 'relevant market', 'hypothetical monopolist' and 'abuse of dominance' is hard to apply to Big Tech companies which operate more on data than on money. The solution, it is proposed, lies in having *ex ante* regulation of Big Tech rather than a system of only *subsequent* sanctions through a possible code of conduct created after extensive stakeholder consultations. [A.P. Kumar and Manjushree R.M., *Data, Democracy and Dominance: Exploring a New Antitrust Framework for Digital Platforms*]

Market dominance and data control give an even greater power to Big Tech companies, i.e., control over the flow of information among citizens. Given the vital link between democracy and flow of information, many have called for increased control over social media with a view to checking misinformation. Rahul Narayan explores what these demands might mean for free speech theory. Could it be (as some suggest) that these demands are "*a sign that the erstwhile uncritical liberal devotion to free speech was just hypocrisy*"? Traditional free speech theory, Narayan argues, is inadequate to deal with the misinformation problem for two reasons. First, it is premised on protecting individual liberty from the authoritarian actions by governments, "*not to control a situation where baseless gossip and slander impact the very basis of society*." Second, the core assumption behind traditional theory—i.e., the possibility of an organic marketplace of ideas where falsehood can be exposed by true speech—breaks down in context of modern era misinformation campaigns.

Therefore, some regulation is essential to ensure the prevalence of truth. [R. Narayan, *Fake News, Free Speech and Democracy*]

Jhalak Kakkar and Arpitha Desai examine the context of election misinformation and consider possible misinformation regulatory regimes. Appraising the ideas of self-regulation and state-imposed prohibitions, they suggest that the best way forward for democracy is to strike a balance between the two. This can be achieved if the State focuses on regulating algorithmic transparency rather than the content of the speech—social media companies must be asked to demonstrate that their algorithms do not facilitate *amplification* of propaganda, to move from behavioural advertising to contextual advertising, and to maintain transparency with respect to funding of political advertising on their platforms. [J.M. Kakkar and A. Desai, *Voting out Election Misinformation in India: How should we regulate Big Tech?*]

Much like fake news challenges the fundamentals of free speech theory, it also challenges the traditional concepts of international humanitarian law. While disinformation fuels aggression by state and non-state actors in myriad ways, it is often hard to establish liability. Shreya Bose formulates the problem as one of causation: "*How could we measure the effect of psychological warfare or disinformation campaigns…?*" E.g., the cause-effect relationship is critical in tackling the recruitment of youth by terrorist outfits and the ultimate execution of acts of terror. It is important also in determining liability of state actors that commit acts of aggression against other sovereign states, in exercise of what they perceive—based on received misinformation about an incoming attack—as self-defence. The author helps us make sense of this tricky terrain and argues that Big Tech could play an important role in countering propaganda warfare, just as it does in promoting it. [S. Bose, *Disinformation Campaigns in the Age of Hybrid Warfare*]

The last two pieces focus attention on real-life, concrete applications of technology by the state. Vrinda Bhandari highlights the use of facial recognition technology ('FRT') in law enforcement as another area where the state deploys Big Tech in the name of 'efficiency'. Current deployment of FRT is constitutionally problematic. There is no legal framework governing the use of FRT in law enforcement. Profiling of citizens as 'habitual protestors' has no rational nexus to the aim of crime prevention; rather, it chills the exercise of free speech and assembly rights. Further, FRT deployment is wholly disproportionate, not only because of the well-documented inaccuracy and bias-related problems in the technology, but also because—more fundamentally—"*[t]reating all citizens as potential criminals is disproportionate and arbitrary*" and "*creates a risk of stigmatisation*". The risk of mass real-time surveillance adds to the problem. In light of these concerns, the author suggests a complete moratorium on the use of FRT for the time being. [V. Bhandari, *Facial Recognition: Why We Should Worry the Use of Big Tech for Law Enforcement*]

In the last essay of the series, Malavika Prasad presents a case study of the Pune Smart Sanitation Project, a first-of-its-kind urban sanitation programme which pursues the Smart City Mission ('SCM'). According to the author, the structure of city governance (through Municipalities) that existed even prior to the advent of the SCM violated the constitutional principle of self-governance. This flaw was only aggravated by the SCM which effectively handed over key aspects of city governance to state corporations. The Pune Project is but a manifestation of the undemocratic nature of this governance structure—it assumes without any justification that 'efficiency' and 'optimisation' are neutral objectives that ought to be pursued. Prasad finds that in the hunt for efficiency, the design of the Pune Project provides only for collection of data pertaining to users/consumers, hence excluding the

marginalised who may not get access to the system in the first place owing to existing barriers. "*Efficiency is hardly a neutral objective,*" says Prasad, and the state's emphasis on efficiency over inclusion and participation reflects a problematic political choice. [M. Prasad, *The IoT-loaded Smart City and its Democratic Discontents*]

We are confident that readers will find the essays insightful. As ever, we welcome feedback.

A. Introduction

What is Big Tech?
Four Conceptual Markers

By Urvashi Aneja & Angelina Chamuah[1]

Almost a decade ago, in the wake of the Arab Spring, technology and social media companies were celebrated across the globe as harbingers of new modes of democratic participation, individual freedoms, and liberation. But, cut to the present, there is a growing tech-lash against 'Big Tech', with concerns ranging from market monopolization to interference in democratic processes.[2] In June 2020, United States lawmakers called upon the CEOs of four big tech companies, Apple, Amazon, Facebook and Google, to testify at a hearing in front of the House Judiciary Committee on allegations related to the abuse of monopoly power and anti-competitive practices.[3] Prior to this, the Federal Trade Commission in the US had conducted investigations into Facebook's abuse of user privacy following the Cambridge Analytica case.[4] The European Union(EU) has also launched several antitrust investigations into Big Tech companies like Google for violating the EU's competition laws due to its dominant market position.[5]

The term Big Tech is one amongst many other monikers, labels, and abbreviations, such as the GAFA[6] and FAANG[7], which have been accorded to a collection of large scale, predominantly American 'technology' companies in recent years. Other terminologies used in association with the term include the Big Five[8] - a collective moniker for the US technology giants that includes Google, Amazon, Facebook, Apple and Microsoft; and Big Nine to include Chinese technology companies Tencent, Alibaba and Baidu.[9]

These companies are collectively projected to control 30% of the world's gross economic output by 2030.[10] The revenue generated by these companies year on year has been compared to the GDP of small nations[11]. Yet, each of these companies have different business

[1] Urvashi Aneja is the Founding Director of Tandem Research and she can be reached at urvashi@tandemresearch.org. Angelina Chamuah is a Research Fellow at Tandem Research and she can be reached at angelina@tandemresearch.org.

[2] Clara Hendrickson and William A. Galston, 'Big Tech Threats: Making Sense of the Backlash against Online Platforms' (*Brookings Institute*, 28 May 2019) https://www.brookings.edu/research/big-tech-threats-making-sense-of-the-backlash-against-online-platforms/.

[3] Makena Kelly, 'Big Tech is Going Under Trial', (*The Verge*, 28 July 2020) https://www.theverge.com/2020/7/28/21344920/big-tech-ceo-antitrust-hearing-apple-facebook-amazon-google-facebook.

[4] Tony Romm and Craig Timberg, 'FTC Opens Investigation into Facebook after Cambridge Analytica Scrapes Millions of Users' Personal Information' (*Washington Post*, 8 April 2019) https://www.washingtonpost.com/news/the-switch/wp/2018/03/20/ftc-opens-investigation-into-facebook-after-cambridge-analytica-scrapes-millions-of-users-personal-information/.

[5] Alex Webb, 'The U.S. and Europe Still Don't See Eye to Eye on Big Tech.' (*Bloomberg*, 28 October 2020) https://www.bloomberg.com/opinion/articles/2020-10-28/europe-is-still-ahead-of-u-s-in-fight-against-google-facebook-apple.

[6] GAFA is an acronym for Google, Apple, Facebook and Amazon. Kabir Chibber, 'American Cultural Imperialism has a New Name: GAFA (*Quartz*, 1 December 2014) https://qz.com/303947/us-cultural-imperialism-has-a-new-name-gafa/.

[7] FAANG is an acronym that stands for stocks of US tech companies: Facebook, Amazon, Apple, Netflix, and Google. Bill Hobbs, 'FAANG Stands for Five Very Successful Tech Companies that Can Move the Stock Market - Here's What to Know about Investing in Them' (*Business Insider*, 6 November 2020) https://www.businessinsider.in/stock-market/news/faang-stands-for-five-very-successful-tech-companies-that-can-move-the-stock-market-heres-what-to-know-about-investing-in-them/articleshow/79089922.cms.

[8] Conor Sen, 'The 'Big Five' Could Destroy the Tech Ecosystem' (*Bloomberg*, 15 November 2017) https://www.bloomberg.com/opinion/articles/2017-11-15/the-big-five-could-destroy-the-tech-ecosystem.

models, market interactions, and societal influence. Google gets its advertising revenue from clicked-on paid links; Facebook gets its ad revenue from attention grabbing content, Apple relies on the sale of electronic hardware, and Microsoft dominates the market for enterprise solutions.

The practice of pre-fixing the 'big' in front of an industry or sector has had previous iterations in the case of global corporations and market monopolies such as Big Tobacco and Big Pharma. Intended to index scale and alleged monopolisation of a sector, the 'Big' in Big Tech refers to the staggering scale that many of the companies clubbed under this header have achieved in the last decade.

But what is Big Tech? Are there a common set of characteristics beyond market power and being technology companies? How does bigness relate to societal power and influence? How is Big Tech different from other types of Big Business?

These questions are even more urgent with the Covid-19 pandemic, as both the market share and societal influence of Big Tech companies is increasing. In contrast, to the many businesses across the globe, including tech companies, struggling with cash reserves and the fallout of the current economic crisis[12], Big Tech companies continue to thrive.

In the third quarter of 2020, Big Tech companies reported record revenues, both during and because of the pandemic. Amazon, reportedly, has been the biggest beneficiary of the pandemic, reporting gross revenues of more than $96 billion, representing 37 percent year on year growth, due to an increase in online sales.[13] Facebook profits jumped 29 percent, despite the backlash against its content moderation policies.[14] Google's parent company Alphabet similarly reported increased revenues, with search advertising revenue growing 6 percent and YouTube ad spending rising 32 percent. Google's cloud computing business grew 45

[9] Amy Webb, 'The Big Nine: How the Tech Titans and Their Thinking Machines Could Warp Humanity' (2020) New York: PublicAffairs.

[10] Ajai Sreevatsan, 'How Big Tech Reset will Impact India' (*LiveMint*, 15 October 2020) https://www.livemint.com/technology/tech-news/how-big-tech-reset-will-impact-india-11602773100875.html.

[11] Fernando Belinchón and Qayyah Moynihan '25 Giant Companies That are Bigger than Entire Countries' (*Business Insider*, 25 July 2018) https://www.businessinsider.com/25-giant-companies-that-earn-more-than-entire-countries-2018-7?IR=T.

[12] Jon Swartz, 'Big Tech Keeps Getting Bigger, as Antitrust Inquiries Continue to Multiply' (*MarketWatch*, 12 February 2020) https://www.marketwatch.com/story/big-tech-keeps-getting-bigger-as-antitrust-inquiries-continue-to-multiply-2020-02-11.

[13] Daisuke Wakabayashi, Karen Weise, Jack Nicas and Mike Isaac, 'Big Tech Continues Its Surge Ahead of the Rest of the Economy' (*The New York Times*, 29 October 2020) https://www.nytimes.com/2020/10/29/technology/apple-alphabet-facebook-amazon-google-earnings.html.

[14] Ibid.

[15] Ibid.

[16] Aaron Holmes, 'Big Tech Companies Hired Aggressively During the Last Financial Crisis, and They're Doing it Again. Here's what Apple, Google, Amazon, and Facebook are Looking For' (*Business Insider*, 13 April 2020) https://www.businessinsider.in/tech/news/big-tech-companies-hired-aggressively-during-the-last-financial-crisis-and-theyre-doing-it-again-heres-what-apple-google-amazon-and-facebook-are-looking-for-/articleshow/75128739.cms.

percent.[15] Similarly, several Big Tech companies have been on a hiring spree since the pandemic began.[16] For instance, Amazon added more than 36,400 people to its workforce in three months ending June 2020, an increase of 34 percent year over year with plans to hire more.[17] Throughout the pandemic, companies such as Amazon, Apple and Google have also positioned themselves as providers of essential services and cutting-edge solutions during the crisis.

B. The Four Conceptual Markers of Big Tech

[17] Annie Palmer, 'Amazon is on a Hiring Spree amid Widespread Coronavirus Layoffs and Record Unemployment' (*CNBC*, 9 September 2020) https://www.cnbc.com/2020/09/09/amazon-is-on-a-hiring-spree-amid-widespread-coronavirus-layoffs-and-record-unemployment.html.

This chapter seeks to go beyond Big Tech as a definitional label, to delineate its conceptual contours, and situate it within a broader context of meaning. A definition of a term or a noun condenses meaning into a single statement, delineating the 'content' which the category articulates. A conceptual analysis resembles a definition to the extent that it also aims at condensing meaning; but, it does not concentrate meaning in a single statement. Rather, it explores what characterises the term or noun. A thick signifier goes beyond a conceptual framework to situate the concept's key dimensions within a broader context of meaning.[18] Unpacking a term as a thick signifier thus draws attention to how a concept acquires meaning in context.[19]

[18] Jef Huysmans, 'Security! What Do You Mean? From Concept to Thick Signifier' (1998) 4(2) European Journal of International Relations, 226-255.

[19] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30(1) Journal of Information Technology 75-89.

Even as a large part of the policy and civil society has trained its gaze upon the incumbents of the label, i.e., Google, Amazon, Facebook and to some extent Chinese tech companies, Big Tech is a concept and not simply a static set of companies —new companies may enter this category just as existing ones may drop out of it. In this section, we identify four conceptual markers shared by Big Tech companies - i.e. data-centric business models, the demonstration of strong network effects, the provision of critical market and societal infrastructure and performance of civic functions. The salience of these conceptual markers, how they combine, and their impact on markets and societies may vary across time and place.

I. Data-centric Models

The collection, analysis, and monetization of data are central to value creation in the digital economy.[20] Big Tech companies collect and process a large proportion of the world's data.[21] Facebook processes 2.5 billion pieces of content and 500+ terabytes of data each day.[22] The nature of data collection has evolved as the digital touchpoints between users and Big Tech companies have expanded from only computers and mobile devices to include digital assistants like Amazon's Alexa, Google's Home Mini, and Apple's Siri.[23] This data collection also extends to non-commercial interactions such as search engine queries, social media likes and even items left un-bought in a user's cart. In 2019, for example, it was revealed by an anonymous whistleblower that Google had been collecting data for a year on patients in 21 US states in the form of lab results, doctor diagnoses and hospitalization records, among other categories, including patient names and dates of birth.[24]

Pulitzer Prize finalist Julia Angwin traces the evolution of this data-centric business model to the early 2000s. She suggests that the bursting of the dot-com bubble led many Silicon Valley companies to search for new business models, leading to the birth of a new strategy based on targeted advertising.[25]

Harvard professor Shoshana Zuboff traces the origins of this data-based business model to Google. She states that 'Google realized that all the 'behavioural surplus' data it was generating, could actually be used as 'prediction products', that could nudge consumers towards certain preferences and habits in a new 'behavioural futures market."[26] She hypothesizes that once Google demonstrated the commercial value of data, others like Facebook followed suit. Data intelligence derived from collecting vast troves of consumer data by these companies has enabled them to push for products and services along many verticals and market segments.

[20] United Nations Conference on Trade and Development *Digital Economy Report 2019 | Value Creation and Capture: Implications for Developing Countries* (2019) https://unctad.org/en/PublicationsLibrary/der2019en.pdf.

[21] Nick Srnicek, 'We Need to Nationalise Google, Facebook and Amazon. Here's Why' (*The Guardian*, 30 August 2017) https://www.theguardian.com/commentisfree/2017/aug/30/nationalise-google-facebook-amazon-data-monopoly-platform-public-interest.

[22] Josh Constine, 'How Big Is Facebook's Data? 2.5 Billion Pieces Of Content And 500+ Terabytes Ingested Every Day' (*TechCrunch*, 22 August 2012) https://techcrunch.com/2012/08/22/how-big-is-facebooks-data-2-5-billion-pieces-of-content-and-500-terabytes-ingested-every-day.

[23] Rozita Dara, 'The Dark Side of Alexa, Siri and Other Personal Digital Assistants' (*The Conversation*, 18 December 2019) https://theconversation.com/the-dark-side-of-alexa-siri-and-other-personal-digital-assistants-126277.

[24] Rob Copeland, 'Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans' (*Wall Street Journal*, 11 November 2019) https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790.

[25] Julia Angwin, Dragnet nation: a quest for privacy, security, and freedom in a world of relentless surveillance' (2020) New York: St. Martins Griffin.

[26] Shoshana Zuboff, ,The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power' (2020) New York: PublicAffairs.

Big Tech companies leverage the collected data in several ways—from targeted advertising (e.g. Google and Facebook) and optimizing e-commerce operations (e.g. Amazon and Alibaba) to diversifying their portfolio of products and services. Apple stands in slight contrast since its core business model does not depend on leveraging personal data. However, many of the apps it owns collect individual data with the aim of better personalization. Big Tech's massive access to consumer data has also been put to use during the Covid-19 pandemic. For instance, Google launched a global movement tracker in 131 countries to show governments how their populations were moving during the lockdown.[27]

The Covid-19 pandemic has only enhanced the ability of Big Tech companies to collect user data, as digital consumption habits of users have changed - with users spending more time on their devices, e-commerce sites, social media and teleconferencing platforms.[28] Similarly, the Apple-Google contact tracing application also potentially provides these companies access to more than 3 billion users globally, and with that access to troves of location data.[29] Data collected across these platforms can ultimately be used to create in-depth, granular and real-time behaviour profiles of consumers.

[27] Isobel Hamilton, 'Fascinating Google Data from 131 Countries Shows Where People Go amid Lockdowns - with Park and Grocery Visits Plummeting as much as 90%' https://www.businessinsider.in/tech/news/fascinating-google-data-from-131-countries-shows-where-people-go-amid-lockdowns-with-park-and-grocery-visits-plummeting-as-much-as-90/articleshow/74968713.cms.

[28] Ella Koeze and Nathaniel Popper, 'The Virus Changed the Way We Internet' (*The New York Times*, 7 April 2020) https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html

[29] Privacy International, 'Covid Contact tracing apps are a complicated mess: What you need to know' (19 May 2020) https://privacyinternational.org/long-read/3792/covid-contact-tracing-apps-are-complicated-mess-what-you-need-know.

II. Network Effects

While most technology companies today employ a data-centric business model, not all can be called Big Tech. Unlike most other firms, Big Tech companies gain immense scale and resilience because they are structured as multi-sided platforms that demonstrate strong network effects.[30]

The more users that are on the platform, the more valuable the platform becomes to other users. More users mean more data, which implies a stronger ability to outcompete rivals through better product design and more efficient operations.[31] Many Big Tech companies offer free or discounted products and services to kick-start this cycle and accumulate initial users.[32] Once

[30] Joshua White, , Antonie Chapsal and Aaron Yeater, 'European Union – Two-Sided Markets, Platforms and Network Effects' (*Global Competition Review*, 7 December 2019) https://globalcompetitionreview.com/insight/e-commerce-competition-enforcement-guide/1177729/european-union-–-two-sided-markets-platforms-and-network-effects.

[31] 'The World's Most Valuable Resource is No Longer Oil, but Data' (*The Economist*, 6 May 2017) https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[32] Nick Srnicek, Platform

Capitalism'(2017) Cambridge, UK: Polity.

[33] Chris Yeh and Reid Hoffman, 'Blitzscaling: The Lightening-Fast Path to Building Massively Valuable Companies' (2018) HarperCollins.

[34] Libra was rebranded as Diem and the independent organization that runs the project, the Libra Association, will now be known as the Diem Association, in an effort to distance itself from Facebook. Jacob Kastrenakes, 'Libra Cryptocurrency Project Changes Name to Diem to Distance itself from Facebook' (*The Verge*, 1 December 2020) https://www.theverge.com/2020/12/1/21755078/libra-diem-name-change-cryptocurrency-facebook; Mike Isaac and Nathaniel Popper, 'Facebook Plans Global Financial System Based on Cryptocurrency' (*The New York Times*, 18 June 2019) https://www.nytimes.com/2019/06/18/technology/facebook-cryptocurrency-libra.html.

[35] Spencer Soper, 'Amazon Looks to Disrupt Healthcare by Entering the Medical Supplies Marketplace' (*Business Standard*, 16 January 2020) https://www.business-standard.com/article/companies/amazon-looks-to-disrupt-healthcare-by-entering-medical-supies-marketplace-118071100108_1.html.

[36] Rob Copeland (n 24).

[37] Martin Moore, 'Tech Giants and Civic Power' (2016) Centre for the Study of Media, Communication and Power, King's College London.

[38] Nizar Abdelkafi, Christina Raasch, Angela Roth and R. Srinivasan, 'Multi-Sided Platforms' (2019) 29 Electron Markets 553-559.

[39] Aditi Shrivastava, 'Amazon Launches Food Delivery Service in India' (*The Economic Times*, 21 May 2020) https://tech.economictimes.indiatimes.

a platform begins to gain traction, users face a high cost of switching to another service provider. Such network effects give companies a 'first-scaler advantage', allowing them to dominate markets eventually.[33]

Market dominance in one sector also enables Big Tech companies to influence other sectors through vertical and horizontal integration. They can leverage their existing user base and accumulated data intelligence to enter new markets. For example, Google bundles its apps and search engine onto Android phones as default; Facebook had tried to launch its own finance system with the creation of a cryptocurrency, Libra;[34] and Amazon is seeking to disrupt the health care sector by entering the online medical supplies market.[35] Operating in many distinct sectors also allows cross-subsidization—the economic losses from a product with low revenues but large number of users can be balanced with other arms of the business that are more commercially viable.[36]

Finally, digital monopolies, unlike traditional monopolies, have the kind of network effort that seemingly enables consumer choice.[37] Google Search is often seen as enabling consumer choice by helping users navigate an over-abundance of choice while simultaneously funnelling users through its own platform. By integrating maps directly into the Search Engine Optimization (SEO), Google benefits from network effects. Indirect network effects are also accrued through other businesses integrating Google Maps into their websites and platforms.[38]

The network effects of Big Tech companies have expanded even further during the pandemic. Increased permeation on digital technology in everyday lives, with open opportunities created by tighter markets during the pandemic, has enabled Big Tech to shore up existing network effects and enter new markets. Amazon, for example, launched its food delivery service to meet customer demands during the pandemic.[39] Similarly,

com/news/internet/amazon-launches-its-food-delivery-service-in-india/75864051.

Google, which has benefitted from existing network effects, has seen a steep growth in the use of its teleconferencing tool and cloud services.[40] Former CEO of Google, Eric Schmidt, said that the company is now focused on accelerating tech adoption in telehealth, remote learning, and broadband.[41]

[40] 'Big Tech's Covid-19 Opportunity' (*The Economist*, 4 April 2020) https://www.economist.com/leaders/2020/04/04/big-techs-covid-19-opportunity.

III. Infrastructural Role

Big Tech companies provide critical market and societal infrastructure. Their products and services have attained such levels of use that they appear to be closer to traditional infrastructure providers in scale, ubiquity, and the necessity to everyday life.[42]

[41] Naomi Klein, 'How Big Tech Plans to Profit from the Pandemic' (*The Guardian*, 13 May 2020) https://www.theguardian.com/news/2020/may/13/naomi-klein-how-big-tech-plans-to-profit-from-coronavirus-pandemic.

[42] Jean-Christophe Plantin, Carl Lagoze, Paul N. Edwards and Christian Sandvig 'Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook' (2018) 20(1) New Media & Society 293-310.

Like railroads or other utilities, Big Tech companies provide many essential services for individuals, businesses, and even governments.[43] For example, Big Tech companies provide core market infrastructures such as cloud services, software development kits and other business development tools. A wide ecosystem of businesses and third-party developers benefit from these tools. Similarly, companies like Google and Facebook are part of our everyday informational infrastructure. According to Brooklyn Law School Professor K. Sabeel Rahman, they facilitate the 'distribution of and access to news, ideas and information upon which our economy, culture and politics depend.'[44]

[43] AWS Public Sector Blog Team, 'AWS Achieves Full Empanelment for the Delivery of Cloud Services by India's Ministry of Electronics and Information Technology' (*AWS Amazon*, 13 December 2017) https://aws.amazon.com/blogs/publicsector/aws-achieves-full-empanelment-for-the-delivery-of-cloud-services-by-indias-ministry-of-electronics-and-information-technology/.

[44] Sabeel Rahman, 'The New Utilities: Private power, Social Infrastructure, and the Revival of the Public Utility Concept' (2017) 39 Cardozo Law Review 1621.

To a significant extent, Big Tech companies have acquired this coveted position through strategic mergers and acquisitions. For example, Google added one new company to its portfolio every ten days in the early 2010s. Facebook has acquired 92 companies since 2007, most notably Instagram and WhatsApp.[45] Equally important has been their lobbying influence. As Foroohar notes, the largest corporate lobbyists in Washington today are Google and Amazon, and early lobbying success in the patent regime allowed Big Tech firms to make it harder for smaller companies to file for patents.[46] Similarly, heavy capital investments by these companies also make it harder for smaller firms to compete.

[45] Tim Wu and Stuart Thompson, 'The Roots of Big Tech Run Disturbingly Deep' (*The New York Times*, 07 June 2019) https://www.nytimes.com/interactive/2019/06/07/opinion/google-facebook-mergers-acquisitions-antitrust.html.

[46] Rana Foroohar, 'How Big Tech is Dragging us towards the Next Financial Crash' (*The Guardian*, 08 November 2019) https://www.theguardian.com/business/2019/nov/08/how-big-tech-is-dragging-us-towards-the-next-financial-crash.

The infrastructural role of Big Tech is only growing in the context of the Covid-19 pandemic. Existing delivery infrastructure, and access to capital, enabled Amazon to present itself as a crucial provider of essential goods during the lockdown period in many countries. Similarly, many workplaces were able to transition to a work from home protocol due to the already existing infrastructure of digital conferencing tools. In 2020, the usage of Google Meet saw a 30-times growth in the early months of the pandemic, with the service hosting up to 100 million meeting participants each day.[47]

[47] Brian Barrett, 'How Google Meet Weathered the Work-From-Home Explosion' (*Wired*, 08 November 2020) https://www.wired.com/story/how-google-meet-weathered-work-from-home-explosion/.

IV. Civic Function

Big Tech companies have assumed a civic role in society through their consumer-facing platforms. Consumers are dependent on these platforms for essential services like news, commerce, and social interactions.[48] This helps Big Tech firms dominate what Tristan Harris calls the 'attention economy'.[49] Through 'data intelligence', they can shape preferences and behavior- to know and influence how we think and interact. This gives them civic power in society.

[48] Martin Moore (n 37).

[49] Nicholas Thompson, 'Tristan Harris: Tech Is 'Downgrading Humans.' It's Time to Fight Back' (*Wired*, 23 April 2019) https://www.wired.com/story/tristan-harris-tech-is-downgrading-humans-time-to-fight-back.

Steven Lukes identifies three faces of power: decision-making power, non-decision-making power, and ideological power. Decision making power involves a focus on behaviour in the making of decisions or issues over which there is an observable conflict of interest. The lobbying efforts of large technology companies around key internet and data governance issues is a pertinent example of such power. Non-decision-making power is that which sets the agenda and makes certain issues legitimate/ illegitimate for discussion in public forums. The investments of large technology companies in public policy and scientific research around the world is one such example of such non-decision-making power. The third face of power, what he calls 'ideological power', refers to the ability to influence people's wishes and thoughts,

even making them want things opposed to their own self-interest.

Moore argues that it is the third face of power identified by Lukes that helps understand the influence of 'tech-giants.' He frames this influence in terms of 'civic power' and identifies six types:

> the power to command attention;
> the power to communicate news;
> the power to enable collective action;
> the power to give people a vote;
> the power to influence people's vote; and
> the power to hold power to account.

Ultimately this civic power that makes it more difficult or complicated to identify and regulate their decision and non-decision-making power.[50] This ability to shape world views and beliefs also distinguishes Big Tech from other forms of Big Business, such as Big Pharma or Big Tobacco.

[50] Martin Moore (n 37).

A necessary condition of such civic power is that they are consumer-facing technologies. Consumer dependence and desire for these consumer products is what enables such civic power. For instance, with 400 million users, WhatsApp in India has become a critical medium for political parties[51] and the state[52] to organise and develop collective campaigns, reaching a wide and new user base. Despite their financial 'bigness', Microsoft or IBM are often not associated with Big Tech because this civic role is an essential conceptual marker of Big Tech. They primarily operate as enterprise-level companies, or back-end companies, and thus have not assumed some of the civic roles of companies like Google or Facebook.

[51] Madhumita Murgia, 'India: The WhatsApp Election' (*Financial Times*, 05 May 2019) https://www.ft.com/content/9fe88fba-6c0d-11e9-a9a5-351eeaef6d84.

[52] Rajesh Kurup, 'COVID-19: Govt of India launches a WhatsApp Chatbot' (*The Hindu Businessline*, 25 March 2020) https://www.thehindubusinessline.com/info-tech/covid-19-india-launches-a-whatsapp-chatbot/article31127438.ece.

The civic function played by Big Tech companies has also increased with the pandemic. Both Google and Facebook, for example, have reported an increase in the

amount of time people spend using their services.[53] Their role as informational gateways continues to give them excessive influence in determining what information people can access.[54] A recent report in Politico, for example, draws attention to how Google's implementation of advertising bans related to the Coronavirus pandemic, under a policy on 'sensitive' topics, ended up blocking government public service announcements.[55] Even governments are using Facebook to live broadcast public messages and engage with their citizenry. The Apple-Google contact tracing tool is an example of how these companies are increasingly setting technological standards for nation-states.[56]

[53] The Economist (n 40).

[54] Nick Statt, 'Major Tech Platforms Say They're 'Jointly Combating Fraud and Misinformation' about COVID-19' (*The Verge*, 16 March 2020) https://www.theverge.com/2020/3/16/21182726/coronavirus-covid-19-facebook-google-twitter-youtube-joint-effort-misinformation-fraud.

[55] Steven Overly and Leah Nylen, 'How the Virus Could Boomerang on Facebook, Google and Amazon' (*Politico*, 01 May 2020) https://www.politico.com/news/2020/05/01/facebook-google-amazon-coronavirus-227522.

[56] Stephen Warwick, 'Five EU states criticize Apple and Google Over Contact Tracing in Letter' (*iMore*, 27 May 2020) https://www.imore.com/five-eu-states-criticise-apple-and-google-imposing-technical-standards-over-contact-tracing.

C. Cyclical relationship of conceptual markers

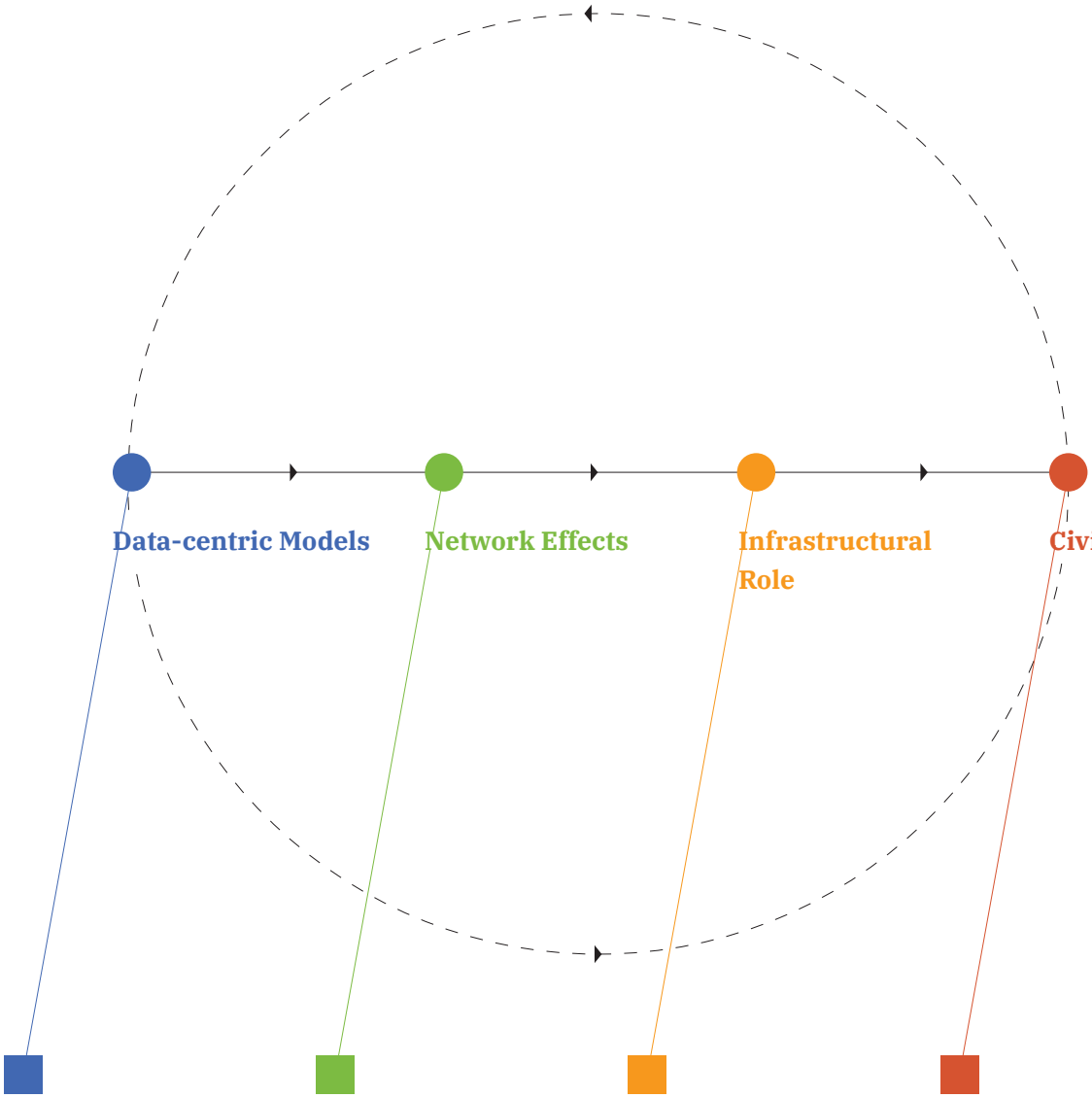
Together, these four conceptual markers characterize Big Tech as data-driven, large-scale, consumer-facing technology platforms that provide essential market and information infrastructure for a digital society. The combination of these features allows them to play civic roles in society, thereby also exerting civic power alongside market power.

Each of these four conceptual markers is an integral interconnected part of a single moving system, which influence each other in a cyclical movement. For example, the large amounts of data collected by Big Tech make their services more customized and responsive. This increases the platform's attractiveness for users and enhances network effects. Higher user engagement and dependence, in turn, leads to an increasing civic role for these platforms. This relationship also works in the opposite direction. The civic role they gain through user attention and public participation, when combined with existing market power, further enhances data collection and aggregation. It also increases the platform's efficiency and public utility.

Cyclical Relationship between Conceptual Markers

These markers exist in a cyclical relationship, building and reinforcing each other.

This diagram draws on examples from Big Tech companies to illustrate each of the markers.



Facebook processes 2.5 billion places of content and 500+ terabytes of date each day. Facebook had multiple touch points for data collection across social media interations and other businesses using the platform.

By integrating maps directly into the SEO, Google benefits from network effects. Indirect network effects are also accrued through other businesses integrating Google Maps into their websites and platforms.

Many other sellers gather on Amazon to sell their products rather than selling them directly. Similarly, content creators rely on YouTube to monetize videos. AWS also dominates the cloud market.

Whatsapp has become a critical medium for civic society to organise and develop collective campaigns, reaching a wide and new user base.

For instance, Facebook derives immense network effects from the number of users on the platform. As more and more users join the platform, it provides greater incentives for others to join as well, as the usefulness of the platform increases. Starting with a very limited number of profiles in the social network, which began in 2004, Facebook today has a global presence with more than 2.7 billion monthly average users. Facebook's business, like Google, is based primarily on targeted advertising, which relies on user behaviour data to curate advertisements. As a vast social network, many consumers use Facebook for purposes other than social networks - for business marketing, and as a source of news and information.

Additionally, Facebook is not just one entity, but a collection of several different companies, including WhatsApp and Instagram. In India, WhatsApp is not only used by governments and political parties for broadcasting public information and campaigning but has also recently started providing financial services in the form of WhatsApp pay. As powerful gatekeepers of information, Facebook has increasingly come to play civic functions in society aside from their market functions.

D. Conclusion: Concepts in Context

Big Tech is a concept, not a static set of companies. New companies may enter this category just as existing ones may drop out of it. Alibaba-owned UC Browser and Reliance owned Jio Platforms are a case in point. Concepts must also be situated in context - in this case, in the context of India's digital transformations.

Alibaba-owned UC Browser and Reliance owned Jio Platforms are a case in point. At its peak, in 2016, Alibaba-owned UC Browser had a 60% market share in India and was used by more than 300 million people.[57] It was the most popular mobile browser in India but has now been surpassed by Google, leaving UC with only 24% of the market share as of 2019.[58]

[57] Nilesh Christopher, 'Browser Wars: How Google beat Chinese Giant UC in India' (*The Ken*, 30 May 2019) https://the-ken.com/story/google-chrome-uc-browser-war/.

[58] Ibid.

As of May 2020, Jio Platforms was the fourth largest Indian company by market capitalization.[59] Until July 2020, Jio Platforms has gathered more than 390 million users, and its deal with Facebook is likely to enhance the collective network effects of both companies, potentially enabling access to close to a billion users in India. Additionally, during the pandemic, Reliance also launched Jio Mart, across 200 cities in India, to sell essential commodities such as groceries from neighbourhood stores using WhatsApp. A report by Bernstein, a research and brokerage firm, suggests that Reliance Industries and Facebook are looking to build an ecosystem of 10 key services, including retail, payments and advertising.[60]

Similarly, Bug Tech's conceptual contours also draw attention to the role of the Indian state, since it is actively leveraging data analytics and digital platforms for governance. It also maintains and runs many essential digital infrastructures such as the India Stack that many private and public enterprises rely on.

This new form of state-backed tech infrastructure shares many conceptual markers of Big Tech. It is based on data processing, has tremendous market-shaping power, provides essential digital infrastructure, and plays a civic function. Unlike Big Tech, however, the state's civic functions enable its market role, rather than vice-versa.

Situating the concept in context also draws attention to the differences in the role that Big Tech companies play in India. Unlike the global North, Big Tech is a key part of India's development story. Big Tech companies provide critical digital infrastructure that enables new forms of democratic and economic participation for people and businesses alike. This infrastructure partially compensates for pre-existing gaps in state, market and R&D capacity in India. Amazon, for instance, has been running its public sector programme in India

[59] Ankit Gohel, 'RIL Gains 4% after Vista Equity's investment in Jio Platforms: Know More about the Deal' (*CNBC TV18*, 08 May 2020) https://www.cnbctv18.com/market/stocks/ril-gains-4-after-vista-equitys-investment-in-jio-platforms-know-more-about-the-deal-5873261.htm.

[60] PTI, 'Jio-Facebook Platform Approach can Open Digital Ecosystem, Market Worth $2 Trillion by 2025' (*Economic Times*, 10 June 2020) https://tech.economictimes.indiatimes.com/news/internet/jio-facebook-platform-approach-can-open-digital-ecosystem-market-worth-2-trillion-by-2025-report/76309667.

since 2017 and is now an approved cloud service provider for the Indian government.[61] Facebook has partnered with the National Disaster Management Authority (NDMA) to offer tools that help the latter respond more effectively to natural disasters.[62] With 95% of India's desktop search inquiries, Google is a gateway to the internet for a vast majority of Indians.[63] The Indian government has also launched a chatbot on WhatsApp to provide access to an emergency helpline and Covid-19 information.[64]

There has been a lot of attention on 'Big tech' as a collection of companies. However, understanding it as a concept, and situating it within diverse contexts, points attention to the broader effects of intensive data collection practices, strong network effects, and dominant market and civic infrastructures on individuals, markets, and societies. These concepts enable us to understand the structural underpinnings of a phenomenon, rather than surface actors alone. Understanding big tech as a conceptual formation and reading it in light of the creation of data-based platforms and other digital infrastructures for civic obligations by the state as well as the growth of new companies such as Reliance Jio can also help anticipate some of the promises and perils to come.

[61] Ibid.

[62] Yossi Matias, 'Keeping People Safe with AI-enabled Flood Forecasting' (*Google Blog*, 24 September 2018) https://www.blog.google/products/search/helping-keep-people-safe-ai-enabled-flood-forecasting/.

[63] While exact numbers on usage are hard to come by, as companies often self-report them, Statista shows that Google search constitutes 95% of all desktop search enquiries in India.

[64] Anumeha Chaturvedi, 'Government Launches Chatbot on WhatsApp to Create Awareness about Coronavirus, Curb Misinformation' (*The Economic Times*, 22 March 2020) https://economictimes.indiatimes.com/tech/internet/govt-launches-chatbot-on-whatsapp-to-create-awareness-about-coronavirus-curb-misinformation/articleshow/74750648.cms?from=mdr.

Data, Democracy and Dominance: Exploring a new antitrust framework for digital platforms

By Alok Prasanna Kumar and Manjushree RM[1]

A. Introduction

> *"In politics, we will have equality, and in social and economic life, we will have inequality. In politics, we will be recognizing the principle of one man-one vote and one vote, one value. In our social and economic life, we shall, by reason of our social and economic structure, continue to deny the principle of one man, one value. How long shall we continue to live this life of contradictions? How long shall we continue to deny equality in our social and economic life? If we continue to deny it for long, we shall do so only by putting our political democracy in peril."*
>
> -Dr BR Ambedkar[2]

> *"The most visible manifestations of the consolidation trend sit right in front of our faces: the centralization of the once open and competitive tech industries into just a handful of giants: Facebook, Amazon, Google, and Apple.... Big tech is ubiquitous, seems to know too much about us, and seems to have too much power over what we see, hear, do and even feel."*
>
> -Tim Wu[3]

The internet, as we know it in 2020, is a very different place from what it was in the 90s and early 2000s. There is perhaps not even one internet anymore.[4] There is probably a Chinese internet behind the "Great Firewall", there is a "Russian internet", an emerging "European Internet" with its own data protection, privacy and copyright rules, and one for the rest of the world, dominated by US based tech giants such as Facebook, Amazon, Google and Apple. That the "internet" of 2020 belies the expectation of decentralized, world spanning network with free flow of information is a reality.

[1]* The authors, Alok Prasanna Kumar and Manjushree RM, are Senior Resident Fellow and Research Fellow at Vidhi Centre for Legal Policy, respectively. They may be reached at alok.prasanna@vidhilegalpolicy.in and manjushree@vidhilegalpolicy.in.

[2] 'Constituent Assembly of India Debates (Proceedings) – Volume XI' (25 November 1949) https://www.constitutionofindia.net/constitution_assembly_debates/volume/11/1949-11-25.

[3] Time Wu, *The Curse of Bigness: Antitrust in the new Gilded Age* (Columbia Global Reports 2018) 21.

[4] 'What is the "splinternet"?' (*The Economist*, 22 November, 2016) https://www.economist.com/the-economist-explains/2016/11/22/what-is-the-splinternet.

This new internet has revolutionized how businesses operate. It has changed the way goods and services are transacted, and how communication and social interactions take place. Market dynamics have changed and the world has witnessed the emergence and proliferation of platforms, networks and multi-sided markets.

But this change has come with its drawbacks. Data aggregation by so-called "big-tech companies", coupled with data-driven network effects and economies of scope and scale, creates insurmountable barriers which hinder other competitors from finding their footing in such markets.[5] Further, big-tech companies also engage in aggressive acquisition of emerging technology start-ups, resulting in fewer companies organically growing to a comparable size and resulting in the concentration of economic power in a few hands.[6]

[5] *Wu* (n 3).

[6] *Wu* (n 3).

Addressing the concentration of economic power in a few hands is the goal and purpose of competition law (or antitrust law as it is also called). Whether it is the United States' Sherman Antitrust Act, 1890 or the Indian Competition Act, 2002, laws that prohibit monopolization and anti-competitive behaviour have been on the books in some form or the other, across the world, over the last 130 years. However, the rise of big-tech has posed a challenge to competition law itself. The challenge in our view is twofold - of whether competition regulators are adequately empowered under existing legislation to act against platforms; and how competition regulators, even if adequately empowered, should undertake enforcement against companies transacting in data?

First, at the policy level, new competition dynamics in the digital economy raise questions on the normative scope of competition law itself. Competition law, of late, has come to concern itself with consumer welfare.[7] Whether it is in increased prices for the consumer or the reduction in choices, the impact on the consumer has become

[7] *Wu* (n 3) 102-18.

the key focus of competition enforcement (with notable exceptions).[8] However, in a market characterized by 'free' products, can the problems associated with the exclusion of competition, arguably without obvious consumer 'harm,' fall within the scope of competition enforcement?

For instance, let's consider Google's search engine function, by far the most dominant search engine with almost 97.12% share in the market.[9] It is available to users without any charge, and has managed to hold on to this position for the better part of two decades, without the emergence of any other comparable competitor. How then do we frame the question on whether Google's dominant position has served or harmed consumers within the framework of competition?

Secondly, at the enforcement level, competition regulators tackle the added complexity of conducting their investigations in a dynamic environment, where the assessment of competitive pressures and the ability of markets to self-correct are not straightforward. Competition regulators may quickly find that the ground beneath them is shifting far quicker than they can react to the changes. Consider the sudden rise of Tik-Tok as a social media platform that challenged the dominance of Facebook even though, on the face of it, the two could not be more different in how users create, share and consume content.[10]

In this article we go in depth into these two aspects of competition regulation of platforms in the context of competition law and policy.

In response to the first question raised, we argue that although competition law engages principally with consumer welfare, it is also equally concerned with the preservation of a competitive process, and thereby the overall health of the market. We additionally argue that preserving broad-based participation in a market is a policy goal for competition law. In response to the

[8] See for instance, *European Union v Google* (Case AT.40411).

[9] 'Search Engine Market Share Worldwide' (*StatCounter, 2020*), https://gs.statcounter.com/search-engine-market-share.

[10] Josh Constine, 'Zuckerberg misunderstands the huge threat of TikTok' (*Tech Crunch*, 02 October, 2019), https://techcrunch.com/2019/10/01/instagram-vs-tiktok./.

second question, we argue that competition law, as it stands, does not account for the specific features of new age markets. It, therefore, continues to grapple with the difficulty of regulating the conduct of big-tech companies effectively, to the detriment of smaller competitors. We posit that the current competition law framework must be updated to restore competition in this "winner-takes-all" market.

The paper starts with the exploration of goals of India's competition law through a brief exploration of its interlinkages with the Constitution of India ('the Constitution'). In doing so, we demonstrate that competition law is not concerned only with fair play in the market but also with the preservation of democratic principles. Second, we briefly evaluate the extant competition framework applicable to the digital economy in India, and demonstrate their inability to account for the peculiarities of such markets. Drawing from the conclusion of our previous argument, we conclude that the present neoclassical framework is not adequate to ensure a competitive process in markets that are inherently prone to concentration. To this effect, we propose an *ex-ante* framework to regulate platforms that have attained a 'significant market status'. Finally, in conclusion, we recommend implementation strategies and briefly explore alternatives to the proposed solution.

B. Constitutional principles underlying Competition Law

As the Ambedkar quote which began this article shows, India's constitution framers were very much concerned about the potential for economic power to distort India's democratic constitution. This finds reflection in the Preamble to the Constitution as well, where the aim is to secure not just social and political justice, but also "economic justice". The most obvious way in which this has been reflected in the Constitution is under Article 39, specifically, clauses (b) and (c) which state:

> *"39. Certain principles of policy to be followed by the State: The State shall, in particular, direct its policy towards securing*
> *...*
> *(b) that the ownership and control of the material resources of the community are so distributed as best to subserve the common good;*
> *(c) that the operation of the economic system does not result in the concentration of wealth and means of production to the common detriment;"*

Article 39 is contained within Part IV of the Constitution which relates to the "Directive Principles of State Policy". While the provisions of Part IV do not confer any enforceable rights on citizens, they are nonetheless important guides for the state's policies.[11] The Monopolies and Restrictive Trade Practices Act, 1969 expressly states that it is being made in pursuance of clauses (b) and (c) of Article 39.[12] Some key interventions during the Constituent Assembly debates tell us what the framers had in mind when they inserted clauses (b) and (c) of Article 39.

Purnima Banerji, in her speech on 24th November, 1949 pointed to Article 39 of the Constitution with specific references to clauses (b) and (c) as being "fundamental in the governance of the country". She emphasised that far from creating a space for a laissez faire form of government, these two clauses expected the government to also encourage active citizenship in a democracy. Articles 38 and 39, in her view, were the "cornerstones of the Constitution."[13] *Jaspat Roy Kapoor* uses Article 39 as an example of how the framers of the Constitution adopted "socialistic principles" in the Constitution[14] -- an assertion that was later included in the Preamble itself by the 42nd Amendment to the Constitution.

Clauses (b) and (c) of Article 39 have a certain "special status" under the Constitution itself with the introduction of Article 31-C through the Twenty Fifth Amendment

[11] *Minerva Mills v Union of India* (1980) 3 SCC 625.

[12] Monopolies and Restrictive Trade Practices Act, 1969, Preamble.

[13] 'Constituent Assembly of India Debates (Proceedings) – Volume XI' (n 2) 11.164.52.

[14] *Ibid* 11.161.190.

which deemed that laws giving effect to these clauses would not violate Article 14 or 19. While a part of Article 31-C was struck down for violating the basic feature of judicial review under the Constitution,[15] the main part of the article nonetheless stands.

The scope and interpretation of clauses (b) and (c) of Article 39 has received judicial attention only since the 1990s as the idea that fundamental rights could be expanded by reading in directive principles into their content took hold.[16] Specifically a link was drawn between Article 14 which guarantees the right to equal protection of law and Article 39 (b) to hold that it was incumbent upon the state to ensure that its laws and policies did not create concentration of resources in a few hands.[17]

A conjoint reading of Article 14 and clause (b) and (c) of Article 39 of the Constitution requires the state to actively take measures that prevent the concentration of wealth and resources in a few hands thereby ensuring economic equality.[18] This ties up with the goal of economic justice contained in the Preamble to the Constitution. As the speeches of the members of the Constituent Assembly, including Dr Ambedkar's, as the chairman of the drafting committee, make clear, economic justice is integral to the achievement of political and social justice. Also, that a democracy will not last very long if it is unable to ensure equality of economic opportunity and reduce the concentration of economic power and resources in a few hands.

Even though the Competition Act, 2002 makes no explicit reference to the provisions of the Constitution in its Preamble, the interpretation and application of the law will need to keep constitutional principles in mind. Furthermore, the Act, alone cannot exhaust all the possible approaches to address economic inequalities and concentration of economic power in India. In fact, the Act does not cover the entirety of competition law in

[15] *Kesavananda Bharati v State of Kerala* AIR 1973 SC 1461.

[16] On reading directive principles into fundamental rights., see *Randhir Singh v Union of India* (1982) 1 SCC 618.

[17] In re *Natural Resources Allocation* (2012) 10 SCC 1.

[18] Zoheb Hossain and Alok Prasanna Kumar, 'The New Jurisprudence of Scarce Natural Resources: An Analysis of the Supreme Court's Judgment in Reliance Industries Limited v. Reliance Natural Resources Limited (2010) 7 SCC 1' (2010) 4 Indian Journal of Constitutional Law 105.

India either. For instance, the Telecommunications Regulatory Authority of India Act, 1997 requires TRAI to take measures to promote competition within the telecom sector[19] whereas laws such as the Motor Vehicles Act, 1988, and the Electricity Act, 2000 impose a similar mandate on state level authorities.[20]

Considering this, how should monopolies or dominance in "big tech" be addressed? We explore this question, particularly in reference to what the Competition Commission of India ('the Commission') may do, and what changes may be needed to the Competition Act, 2002, in the next section.

[19] The Telecom Regulatory Authority of India Act, 1997, s 11.

[20] The Motor Vehicles Act, 1998, s 67; The Electricity Act, 2003, s 23.

C. Decoding Dominance in Platform Markets

1. The present framework for assessing dominance

In India, the Competition Act, 2002 ('the Act') prohibits dominant companies and commercial entities from abusing their dominance.[21] It presupposes that practices enumerated in section 4[22] are abusive *only* if carried out by dominant entities. As such, establishing 'dominance' is an inevitable first step for the Commission in assessing whether a certain practice is abusive. The Act, much like other antitrust regimes in the world,[23] follows an *ex-post* model of regulating abuse of dominance where the Commission intervenes only when prohibitions in section 4 are breached.[24]

Section 4 of the Act defines 'dominance' as a position enjoyed by an enterprise that allows it to operate independently of competitive forces, and/ or affect its competitors or consumers in its favour.[25] While assessing dominance, the Commission delineates the 'relevant market', within which the position of the enterprise is examined.[26] Following this, the Commission assesses whether an enterprise enjoys dominance by accounting for factors which include, *inter alia*, market share, size, and resources of the enterprise and barriers of entry to competitors.[27] As there is no statutory bright line test for dominance,[28] it is assessed on a case-to-case basis.[29]

[21] The Competition Act, 2002, s 4.

[22] The Competition Act 2002, s 4(3).

[23] International Telecommunication Union, 'Competition Policy in Telecommunications: The Case of the United States of America' (Workshop on Competition Policy in Telecommunications, Geneva, November 2002); Peter Alexiadis, 'Balancing the Application of Ex Post and Ex Ante Disciplines in Electronic Communications Markets: Square Pegs in Round Holes?' in Eugène Buttigieg (ed), *Rights and Remedies in a Liberalised and Competitive Internal Market* (University of Malta 2012).

[24] The Competition Act 2002, s 19(1).

[25] Explanation (a) to the Competition Act 2002, s 4.

[26] The Competition Act 2002, s 19(5).

[27] The Competition Act 2002, s 19(4).

[28] *ESYS Information Technologies Pvt Ltd and Intel Corporation (Intel Inc) & Ors* (Case No. 48 of 2011).

[29] *Mr. Ramakant Kini v Dr. L.H. Hiranandani Hospital, Powai, Mumbai* (Case No.39 of 2012).

2. The limitations of section 4 of the Act in case of digital platforms

Modern antitrust law is premised on neoclassical economics which presumes that the goal of any private entity is maximizing profits. The business models of platforms, however, prioritize growth over profits, i.e., expansion of their user-base as opposed to profit maximization.[30] This significantly alters the presupposed incentives that platforms have in the medium to short term, and therefore analysing the behaviour of such platforms requires a departure from the neoclassical frame of reference.

The trouble begins with defining a 'platform'. The rapidly evolving boundaries of the digital market and platforms has led to a general lack of consensus on the normative definition of a platform.[31] Functionally, however, a platform may be defined as a market wherein an intermediary lays out a system with entry points for other parties to operate. These intermediaries grant such parties access to one another (such as dating applications, radio taxi aggregation applications, marketplaces and social networking sites), and often also serve as the infrastructure upon which third parties develop product offerings (such as Google's Play Store and Apple's Appstore). Their business models rely on connecting distinct user groups on different sides of the platform, making them 'multi-sided'.

i. Platforms as data aggregators

The business model of most digital platforms is based on users' personal data, and flow of this data from one side to another.[32] Platforms collect, store, and use large amounts of data, derived from consumers that transact upon them.[33] This accumulated consumer data is a veritable goldmine for those that require large data samples to study population-wide trends, such as

[30] Lina Khan, 'Amazon's Antitrust Paradox' (2018) 126(3) YLJ, https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5785&context=ylj.

[31] Michael Katz, 'Exclusionary Conduct in Multi-Sided Markets' (*Organisation for Economic Co-operation and Development*, 2017) https://one.oecd.org/document/DAF/COMP/WD(2017)28/FINAL/en/pdf.

[32] Ling-Chieh Kung and Guan-Yu Zhong, 'The Optimal Pricing Strategy for Two-sided Platform Delivery in the Sharing Economy' (2017) Transportation Research: Logistics and Transportation Review Part E 101, https://scholars.lib.ntu.edu.tw/bitstream/123456789/455958/1/SSRN-id2931383.pdf.

[33] Cassandra Liem and Georgios Petropoulos, 'The economic value of personal data for online platforms, firms and consumers' (LSE Business Review, 19 January 2016) https://blogs.lse.ac.uk/businessreview/2016/01/19/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/.

consumption trends and consumer preferences. Digital platforms have taken to monetising and selling such data, enabling them to transact at multiple sides of a platform, where one side is subsidised by the other.[34] For instance, the services that Google or Facebook give their users for free are entirely subsidised by businesses that buy the data these companies collect from users. What appears as a 'free' experience, therefore, is not free - the implicit price is the user's data itself, the knowledge of which is more valuable than any fee such a user would be willing to pay.[35] This contrasts with traditional markets, where money is the sole medium of exchange. The absence of a monetary price poses significant challenges[36] to the determination of a 'relevant market',[37] which relies on a price-based 'hypothetical monopolist test'.[38]

Data also uniquely plays to the advantage of such platforms to enter other related markets. Google, a search engine's entry into comparison shopping, the e-market place giant Amazon's entry into retail through Amazon Basics, are examples of the consequential vertical integration due to data. Further, as platforms control entry points into a given market, they also perform the role of gatekeepers. There is fear that once such platforms enter adjacent markets, aggregated data at their disposal will result in foreclosure of new entrants who then cannot compete as efficiently without access to this critical input.[39]

Additionally, singular access to aggregated data can present a form of competitive advantage.[40] A data-rich incumbent is able to further bolster its market position through an effect known as the 'feedback loop'. Feedback loops manifest in two ways: A 'user feedback loop' where an entity with a large user base is able to collect more data to improve the quality of its service and thereby

[34] Evans notes with respect to zero-price platforms *"Charging nothing for a product or service enables them to make money, somehow, somewhere else."* see David S. Evans, 'The Antitrust Economics of Free' (2011) John M. Olin Law & Economics Working Paper 555, https://docplayer.net/11563755-The-antitrust-economics-of-free-david-s-evans-the-law-school-the-university-of-chicago-may-2011.html.

[35] Chris Jay Hoofnagle and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price' (2014) 61 UCLA L. Rev., https://www.uclalawreview.org/pdf/61-3-2.pdf.

[36] 'Report of the Competition Law Review Committee' (Ministry of Corporate Affairs 2019) https://www.ies.gov.in/pdfs/Report-Competition-CLRC.pdf.

[37] The Commission's approach towards delineating relevant markets has been inconsistent in case of platforms. See *Ashish Ahuja v Snapdeal* (Case No. 17 of 2014); *All India Vendors Association v Flipkart* (Case no. 20 of 2018).

[38] Magali Eben, 'Market Definition and Free Online Services: The Prospect of Personal Data as Price' (2018) 14(2) Journal of Law and Policy for the Information Society, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3207201.

[39] European Round Table for Industry, 'Shaping Competition Policy in the Era of Digitisation' (2018), https://ec.europa.eu/competition/information/digitisation_2018/contributions/ert.pdf.

[40] Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the Digital Era' (European Commission, 2019) https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

acquire new users, and a 'monetization feedback loop' where platforms are able to cash in on the aggregated user data to improve targeted advertisement, which in turn brings in more revenue to invest in the quality of the platform service and, thereby, attracts more users.[41] Such feedback loops reinforce the strength of an incumbent giant in the market, and therefore constitute a novel barrier to entry.

ii Data-Driven Network effects

'Network effects' refer to increased utility that a user derives from a service, when the number of other users consuming the service increases.[42] For instance, the utility of Amazon, increases for a consumer with the number of sellers on the marketplace and *vice versa*. Similarly, the more users a social network like Facebook has, the more utility it has to each of its users. Therefore, a competitive lead in a digital market is self-reinforcing. Services of platforms become more valuable to consumers as more people use them. This creates an effect where not only the product, but also the network of its users bear utility to the user. The greater is the popularity of a digital platform, the harder it becomes to create a more attractive competitor. This grants an incumbent an enormous beginner's move advantage.[43] Consequently, for a new entrant seeking to compete with incumbents, not only does the entrant have to offer a better-quality product, but also convince users to migrate to the new platforms by breaking the 'lock-in effect' created by the incumbent. This self-reinforcing mechanism also presents itself as a competitive advantage to an incumbent entity.

[41] The Secretariat, Organisation for Economic Co-operation and Development, 'Big Data: Bringing Competition Policy to the Digital Era' (*Organisation for Economic Co-operation and Development*, 2016) https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf#_ga=2.106957570.1680213474.1559388897-1619135612.1554836539.

[42] The Secretariat, United Nations Conference on Trade and Development, 'Competition issues in the digital economy' (*United Nations Conference on Trade and Development*, 2019) https://unctad.org/system/files/official-document/ciclpd54_en.pdf.

[43] Andrei Hagiu and Julian Wright, 'When Data Creates Competitive Advantage' (*Harvard Business Review*, 2020) https://hbr.org/2020/01/when-data-creates-competitive-advantage.

iii. Economies of scale

'Economies of scale' refers to a situation where the per-capita cost of production of a good or services decreases with the increase in the number of goods or services produced. While this generally holds true for all markets, the way this phenomenon plays out is far more extreme in case of digital platforms.[44] The increment in the cost of production of service to a new consumer acquired is almost negligible in case of a platform. Every consumer that gets on a platform pays a price for the same, without the platform incurring almost any cost towards the provision of a good or service to the consumer. This peculiarity also results in pre-existing dominant players having a huge competitive advantage over new entrants in terms of the price at which the service of the platform is offered. Additionally, in order to grow in size to reach economies of scale, big platforms (which may not necessarily be dominant in a given market) defer their profits indefinitely by running at losses.

From the above, it is evident that, where a consumer does not pay a monetary price but putatively receives digital services for 'free', it is difficult to identify whether any two services compete to fulfil the same need of a user. It is also evident that unique features of platform markets, such as consumer data feed-back loops, network-effects and economies of scale pivots the market in favour of an incumbent entity, making such markets inherently prone to concentration.[45] Such markets are also known as '*Schumpeterian markets*', where entities do not compete *in* the market, but compete *for* the market,[46] resulting in a winner-takes-all dynamic. As these markets are not designed to support multiple firms competing on quality or price, market share does not serve as

[44] Richard A. Posner, 'Antitrust in the New Economy' (2000) John M. Olin Program in Law and Economics Working Paper 106/2000, https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1057&context=law_and_economics.

[45] Heike Schweitzer, Justus Haucap, Wolfgang Kerber and Robert Welke, 'Modernising the law on abuse of market power: Report for the Federal Ministry for Economic Affairs and Energy (Germany)' (Bundesministerium für Wirtschaft und Energie, 2018) https://www.bmwi.de/Redaktion/DE/Downloads/Studien/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen-zusammenfassung-englisch.pdf?__blob=publicationFile&v=3.

[46] Lina Khan, 'Amazon's Antitrust Paradox' (2018) 126(3) YLJ, https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5785&context=ylj.

a useful proxy for dominance.[47] Further, the conjoint effect of a beginner's move advantage of an incumbent platform which is amplified by data-driven network effects and feedback loops, present exponentially laborious barriers of entry to competitors, the magnitude of which is not adequately comprehended in the present framework for dominance. This results in situations where an entity, although not dominant as per the Act, may behave and influence markets in ways that dominant entities do.[48]

This raises two questions to the competition enforcement in India. First, in a market that is oligopolistic at best, and one that structurally disincentivizes a competitive process, is ex-post intervention adequate? Second, given the role of platform giants as gatekeepers and their self-reinforcing characteristics which fortify their position, should the same standard for dominance as contemplated in section 4 of the Act be applicable? We seek to explore alternatives as explained below.

[47] Maxwell Meadows, 'The Essential Facilities Doctrine in Information Economies: Illustrating Why the Antitrust Duty to Deal is Still Necessary in the New Economy' (2015) 25 Fordham Intell. Prop. Media & Ent. L.J., https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1608&context=iplj.

[48] The Commission has repeatedly held that Amazon is not a dominant entity despite its ability to as act as a gatekeeper. See *Delhi Vyapar Mahasangh v Flipkart and Ors.* (Case no. 40 of 2019); *Lifestyle Equities C.V. and Another v Amazon Seller Services Private Ltd. and Ors.* (Case no. 9 of 2020).

D. Adopting the strategic market status standard and *ex-ante* code of conduct to regulate digital platforms

Competition authorities globally have preferred an *ex-post* approach to *ex-ante* intervention, as the latter bears the risk of false positives and a consequent chilling effect on competition and innovation. This premise may, however, require rethinking in the case of platforms, for reasons explained below.

First, there is abundant literature that underscores the symbiotic relationship between competition authorities, and sectoral authorities who regulate their sectors *ex-ante*.[49] *Ex-post* competition enforcement works best when complemented with, and supported by, *ex-ante* regulation. Sectoral regulators, through *ex-ante* regulation, 'set the rules of the game' and competition authorities, through *ex-post* regulation, act as 'umpires of the game'. More simply put, sectoral regulators who possess the technical expertise in a given sector often

[49] John C. Hilke, 'Improving Relationships Between Competition Policy and Sectoral Regulation' (Fourth Meeting of The Latin American Competition Forum, San Salvador, 2006)http://www.oecd.org/daf/competition/prosecutionandlawenforcement/38819635.pdf; Gary Hewitt, 'Relationship between Regulators and Competition Authorities' (*Organisation for Economic Co-operation and Development*, 1998) http://www.oecd.org/regreform/sectors/1920556.pdf; Paul Crampton, 'Striking the Right Balance between Competition and Regulation: The Key is Learning from our Mistakes' (APEC-OECD Co-operative Initiative on Regulatory Reform: Third Workshop, Korea, 2002) https://www.oecd.org/regreform/2503205.pdf.

prescribe and regulate what should be done by entities, while competition authorities, with their economic expertise, prescribe what should not be done. They have convergent roles in pursuing the same goal of maximizing consumer welfare.[50] The resultant enforcement from a combination of the two approaches effectively regulates a market and sets boundaries for players to operate within. In India, digital platforms do not fall under the purview of a specific sector or a statute, although aspects of it are regulated in a fragmented manner primarily by the Ministry of Electronic Information and Technology and the Ministry of Commerce. The lack of a streamlined *ex-ante* regulation has not only created a blind spot in the regulation of digital platforms, but has also compromised the efficacy of *ex-post* regulation by the Commission.

Second, *ex-post* enforcement does not always lead to optimal restoration of competition in evolving and fast paced markets, especially involving gatekeepers. As noted by the United Kingdom's Office of Telecommunications, *ex-ante* regulation is specifically required for those entities that act as gatekeepers but may "*escape the legal/economic definition of dominance (although they have the clear potential to become dominant).*"[51] and are characterised by "*significant switching costs in moving to another supplier or service*".[52] Further, as evidenced by the recent United States' House Judiciary Committee's investigations into giants such as Apple, Google, Facebook and Amazon,[53] investigations into incumbent players in such markets can be resource-intensive and time-consuming. In the meanwhile, the market may irreversibly tip in favour of the dominant firm and consequently drive out competitors. The harm thus resulted both to the market and competitors is irremediable.

[50] Maher M. Dabbah, 'The Relationship between Competition Authorities and Sector Regulators' (2011) Camb. Law J., https://www.jstor.org/stable/41300946?seq.

[51] Hewitt (n 49) 23.

[52] Ibid.

[53] 'Antitrust Investigation of the Rise and Use of Market Power Online and the Adequacy of Existing Antitrust Laws and Current Enforcement Levels' (*House Committee on the Judiciary*, 2019) https://judiciary.house.gov/issues/issue/?IssueID=14921.

Third, *ex-post* competition investigations are an *ad hoc* solution, as they are limited to the narrow claims made in each specific case. They may do little to address similar anti-competitive conduct arising in regard to same entity's conduct in a different / associated market[54] or a different entity's conduct resulting in the same issues as investigated.[55] When an entity's behaviour or the problems raised by different entities are in a recurring pattern, addressing them through *ex-ante* regulation results in significantly increased administrative efficiency.

In light of the above limitations, a recourse to an *ex-ante* competition framework for digital platforms is the need of the hour: one that sets the rules for platforms to play by, thereby ensuring that the market remains fair and contestable. This approach finds support in the recommendations of the United Kingdom's Report of the Digital Competition Expert Panel[56] and the proposed Digital Services Act package in the European Union[57]. This approach is also in line with the United States' Stigler Committee Report on Digital Platforms,[58] which espouses the use of *ex-ante* competition intervention as a complimentary tool to effectively tackle anti-competitive behaviour by incumbent platforms in the digital markets whose precise antitrust implications remain obscure. It is therefore important that the code of conduct clarifies principally acceptable conduct between digital platforms and their users, set around certain core principles. Such principle-based regulation confers a balance between providing certainty to market players while providing flexibility to update the rules in line with the course of the market, which is especially important in a market that thrives on innovation.

Additionally, it is also important that such a code is made exclusively applicable to particularly powerful platforms, whose position is not strictly understood through the parameters of section 4 of the Act, given its limitations as demonstrated. Instead, a threshold called

[54] Google has been subject to repeated antitrust scrutiny by the Commission. See *Umar Javeed and Ors v Google LLC and Ors*. (Case no. 39 of 2018); *Matrimony.com Limited v Google LLC and Ors. and Consumer Unity and Trust Society v Google LLC* (Case no 7 and 30 of 2012).

[55] The Commission has noted, for instance, that self-preferencing is a recurring concern. 'Market study on E-Commerce in India: Findings and Observations' (*The Competition Commission of India*, 2020) https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-study-on-e-Commerce-in-India.pdf.

[56] 'Unlocking digital competition' (Digital Competition Expert Panel 2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf (Expert Panel).

[57] 'The Digital Services Act package' (*European Commission*, 2020) https://ec.europa.eu/digital-single-market/en/digital-services-act-package.

[58] 'Stigler Committee on Digital Platforms: Final Report' (Chicago Booth, 16 September 2019) https://www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report.

'significant market status', should be considered as an alternate for statutory dominance.[59] This approach enables the regulation of platforms who have not yet strictly attained 'dominance' as under section 4 of the Act, but are nevertheless powerful enough to influence market/s.[60] This significant market status may be defined using certain parameters which include the extent of the platforms' vertical integration across markets and their ability to, *inter alia*, control others' market access, charge higher and discriminatory fees/prices both to consumers and sellers, manipulate search rankings and results and influence the brand image of others.[61]

Finally, it is imperative that the code is created through extensive stakeholder consultations that follow the concept of 'participative antitrust'. Participative antitrust refers to the process of active engagement with stakeholders for the purposes of designing their own regulatory architecture[62]. In digital markets, platforms would be incentivized in designing an *ex-ante* code of conduct as they stand to benefit from the clarity and certainty that the code shall bring about.[63] With the combined approach of an *ex-ante* code of conduct coupled with *ex-post* regulation through the Act, the tools at the disposal of the Commission to address problems of concentration in cases of digital platforms will be appreciably improved.

E. Conclusion

Competition law has historically developed as an antidote to the emergence of monopolies – prompted by the fear that economic inequalities and concentrated economic power might upend democracy. It is therefore not surprising that both competition law and democracy look to ensure freedom of individual choice, abolition of concentration of power, and ensuring free and fair participation.[64] As such, the Competition Act, 2002 espouses the twin goal of ensuring consumer welfare and freedom of trade for participants in the Indian

[59] Expert Panel (n 56).

[60] A diluted threshold for intervention has also been espoused by the UK's expert Panel on Digital Platforms. See Expert Panel (n 56); Laurent Garzaniti, Thomas Janssens and Tone Oeyen, 'Abuse of economic dependence: Belgian Competition Authority adds another tool to its enforcement toolkit' (*Freshfields Bruckhaus Deringer*, 26 March 2019) http://knowledge.freshfields.com/en/Global/r/3925/abuse_of_economic_dependence.

[61] Expert Panel (n 56).

[62] Oliver J. Bethell, Gavin N. Baird and Alexander M. Waksman, 'Ensuring innovation through participative antitrust'(2020) 8(1) Journal of Antitrust Enforcement, https://doi.org/10.1093/jaenfo/jnz024.

[63] The Commission has attempted to identify and clarify certain anti-competitive practices in relation to E-commerce platforms in to order to promote certainty in their regulation. See 'Market study on E-Commerce in India: Findings and Observations' (*The Competition Commission of India*, 2020) https://www.cci.gov.in/sites/default/files/whats_newdocument/Market-study-on-e-Commerce-in-India.pdf.

[64] 'Report of the Working Group on Competition Policy' (Planning Commission 2007), https://niti.gov.in/planningcommission.gov.in/docs/aboutus/committee/wrkgrp11/wg11_cpolicy.pdf.

[65] The Competition Act, 2002, Preamble.

markets,[65] through prohibitions against anti-competitive agreements and combinations, and abuse of dominance.

While the existing competition law has been successful in regulating concentration in most markets, its inability to regulate incumbent digital giants has given rise to considerable scrutiny. Particularly, the proliferation of digital platforms, such as Amazon, Facebook and Google which cater to different sets of user groups, and the using of data from one to provide services to the other, has rendered the application of traditional competition tools obsolete.

In consequence, the aggregation of data coupled with data-driven network effects and economies of scope and scale, has created insurmountable barriers which hinder other competitors from finding their footing in such markets. Further, such entities also engage in aggressive acquisition of emerging technology start-ups, resulting in fewer companies organically growing to a comparable size, leading to foreclosure of markets to competitors and concentration of economic power in a few hands. This forces policy makers to reassess the goals of competition law and align the regulation of platforms with such goals, as opposed to shoehorning it within the existing framework.

What does this entail?

As a way forward, we propose that an *ex-ante* code of conduct to regulate those platforms that have a strategic market status should be introduced. If the purpose of competition law is not only consumer welfare but also the constitutional goal of prevention of concentration of economic power in a few hands, the answer cannot lie solely within the four corners of a competition law, enforced *ex-post facto* by the Commission. What is needed therefore is a law (such as the code of conduct as explained above) or a set of laws which consider the

need to be able to act against platforms *ex-ante*. At the same time, the Commission cannot also be entirely divested of its powers to act *ex-post facto* and needs to be given sufficient capacity to address the difficulties of ensuring the enforcement of competition laws against platforms.

One approach to this problem might involve data protection laws that regulate how entities collect, store and process personal and non-personal data. As of writing, Parliament is discussing the Personal Data Protection Bill, 2019 which seeks to regulate the manner of collection, storage, and processing of personal data. While the law has its critics and might not be as robust as expected,[66] nevertheless, data protection laws might be one route to checking the power of platforms.

In addition, as proposed above, the Ministry of Corporate Affairs may formulate an *ex-ante* code and direct the Commission under section 55 of the Act[67] to enforce the same. For this purpose, it may be prudent to set up a specialized digital wing within the Commission with an array of experts such as economists, engineers and policy makers, to implement and suggest changes to the code of conduct in accordance with the trajectory of digital markets.

Other options to regulate data-rich platforms includes the creation of a cross-sectoral National Digital Policy that helps regulation, including competition enforcement, to navigate this unchartered territory by tapping into the synergies created between different regulators such as MeitY and the Ministry of Commerce and Industry.

Finally, the need for a strong competition policy is now more pressing than ever. A well-designed competition policy that clearly lays down the Act's goals, objectives and enforcement priorities will guide the Commission in tackling novel problems in such dynamic markets.

[66] See for instance Megha Mandavia, 'Personal Data Protection Bill can turn India into 'Orwellian State': Justice BN Srikrishna' (*Economic Times*, 12 December, 2019) https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-can-turn-india-into-orwellian-state-justice-bn-srikrishna/articleshow/72483355.cms?from=mdr.

[67] The Competition Act 2002, s 55.

Fake News, Free Speech and Democracy

By Rahul Narayan[1]

A. Introduction

1 There is a certain poetic justice in the fact that the presidency of the 45th US President is ending just like it began: with a dispute about the size of the crowds present on the streets.[2] From "existentialist Willie"[3] to "alternative facts", there is a rich vein of humour around ludicrous explanations for the whoppers we have been fed by our politicians and leaders since time immemorial.

2 What is different about the current moment is that any appreciation of the humour in the situation is coupled with an undercurrent of worry about the widespread ubiquity of fake news and disinformation and its deleterious impact on democracy. President Obama mentioned in an interview to the Atlantic Magazine, *"If we do not have the capacity to distinguish what's true from what's false, then by definition the marketplace of ideas doesn't work. And by definition our democracy doesn't work. We are entering into an epistemological crisis."*[4]

3 Laura Chinchilla, the ex-President of Costa Rica and head of the Kofi Annan Commission on Elections and Democracy in the Digital Age has written in the New York Times, *"It is our capacity for reasoned communication that makes elections possible and allows our representative political systems to function and adapt. Freedom to speak empowers citizens, individually or collectively, to advance their interests and shape the institutions whose decisions impact their lives. Yet today we are deeply concerned about the very survival of democracy and the rule of law. These civic guarantees make possible our coexistence, particularly at a time when bogus information rapidly spreads through social media, radical political content explodes across digital channels and public debates increasingly veer toward extremism."*[5]

[1] Rahul Narayan, BCL (Oxon.), Advocate-on-Record, Supreme Court of India available at raol.narayan@gmail.com.

[2] Daniel Politi, 'Trump Administration Ending Like It Began: Lying About Crowd Size' (*Slate*, 14 November 2020) https://slate.com/news-and-politics/2020/11/trump-administration-ending-lying-crowd-size-protest-march.html.

[3] Timothy Noah, 'Bill Clinton and The Meaning Of "Is"' (*Slate*, 13 September 1998) https://slate.com/news-and-politics/1998/09/bill-clinton-and-the-meaning-of-is.html.

[4] Jeffrey Goldberg, 'Why Obama fears for our democracy' (*The Atlantic Daily*, 16 November 2020) https://www.theatlantic.com/ideas/archive/2020/11/why-obama-fears-for-our-democracy/617087/.

[5] Laura Chincilla, 'Post-Truth Politics Afflicts The Global South Too' *(New York Times*, 18 October 2019) https://www.kofiannanfoundation.org/supporting-democracy-and-elections-with-integrity/annan-commission/post-truth-politics-afflicts-the-global-south-too/.

4 The British Parliament has published a Report on Disinformation and Fake News[6] which states in its summary:

> *"We have always experienced propaganda and politically-aligned bias, which purports to be news, but this activity has taken on new forms and has been hugely magnified by information technology and the ubiquity of social media. In this environment, people are able to accept and give credence to information that reinforces their views, no matter how distorted or inaccurate, while dismissing content with which they do not agree as 'fake news'. This has a polarising effect and reduces the common ground on which reasoned debate, based on objective facts, can take place. Much has been said about the coarsening of public debate, but when these factors are brought to bear directly in election campaigns then the very fabric of our democracy is threatened."*[7]

[6] 'Disinformation and 'Fake News': Final Report' (2019) Parliamentary House of Commons, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

[7] Ibid 5.

5 The potential of fake news or misinformation[8] to disrupt democratic functioning has attracted too much public and scholarly attention for at least half a decade to be dismissed as merely a passing fad. Yet, this is a relatively new kind of problem that faces free speech law and theory,[9] and one that is the opposite of how the problem has usually been conceived. Throughout history and in theory it is the lack of freedom of expression that has hampered democracy and not a surfeit thereof. Free speech and self- government go hand in hand.[10] Censorship is the enemy of freedom. Free speech enthusiasts have always said that the problem of free speech can be solved by more free speech. Content based restrictions have always been discouraged.[11]

[8] For the purposes of this essay I have not defined the terms fake news, disinformation and misinformation and have used the same interchangeably to mean **intentional** spreading of incorrect information. For different ideas on what constitutes fake news, see for example, Nikhil Pahwa, 'What is Fake News' (*Medianama*, 01 March 2017) https://www.medianama.com/2017/03/223-what-is-fake-news/.

[9] Tim Wu, "Is the First Amendment Obsolete" (2018) 117 Mich. Law. Rev. 547.

[10] Alexander Meiklejohn, *Free Speech and Its Relation to Self-Government,* (1st edn., 1948) Harper & Bros.

[11] *Police Department of Chicago v Mosley* (1972) 408 US 92; *Rosenberger v Rectors and Visitors of the University of Virginia* (1995) 515 US 819.

6 Accordingly, the new genre of thought that calls for some level of "control" or oversight over social media in order to maintain the integrity of democratic institutions

has been met by incredulous disbelief by free speech liberals as well as populist conservatives, both of whom feel that this is just view point discrimination and a sign that the erstwhile uncritical liberal devotion to free speech was just hypocrisy.[12]

[12] See for example, Kelafa Sanneh, 'The Hell You Say' (*The New Yorker*, 03 August 2015) https://www.newyorker.com/magazine/2015/08/10/the-hell-you-say.

7 Widespread dissemination of disinformation in democratic societies does offer a serious challenge to traditional ways of understanding and studying both free speech and democracy. It most emphatically does not offer itself to easy or elegant solutions based on first principles. If anything, long held doctrinal shibboleths lead us to a conundrum that impairs our ability to clearly see the problem or identify solutions.
The Traditional Position, such as it is, may be encapsulated as follows:

TP1 Democracy is based on votes of citizens who make choices based on information. Self- government depends on free speech and expression.

TP2 No one has a monopoly on wisdom or the truth. The marketplace of ideas must be the arbiter of truth. The more the freedom of expression, the better it is for truth.

TP3 Censorship distorts the marketplace of ideas and makes it more difficult for citizens to find the truth or make informed choices in exercise of their democratic mandate.

TP4 Even knowably false speech has value because it promotes "the clearer perception and livelier impression of truth, produced by its collision with error"[13]

TP5 Censoring false information to save democracy would destroy freedom of expression and thus destroy democracy itself.

[13] John Stuart Mill, *On Liberty* (2nd edn, 1859) JW Parker & Son 33.

8 In the first part of this essay entitled "The nature of the problem", I propose to deal with issues arising from the increasing ubiquity of fake news and the impact that has

on the assumptions of the Traditional Position leading to the inevitable conclusion that some level of regulation is required. In the latter part of this essay entitled "Some considerations for regulations", I intend to identify some considerations that ought to inform the formulation of reasonable regulations dealing with fake news.
Finally, I conclude this essay by exploring the impact of disinformation on democracy and what we can hope for from regulation.

B. Nature of the problem

9 A democracy can be defined in many ways starting from its etymological definition as "rule by the people".[14] Alexander Meiklejohn was speaking particularly of American democracy but he stated a normative truth applicable to all democratic systems when he stated that in a democratic system *"It is ordained that all authority to exercise control and to determine common action belongs to "We the people". We, and we alone, are the rulers".*[15] He explains the need for information and the free exchange of ideas in the following language:

> *"Now, in that method of political self-government, the point of ultimate interest is not the words of the speakers but the minds of the hearers. The final aim of the meeting is the voting of wise decisions. The voters, therefore, must be made as wise as possible. The welfare of the community requires that those who decide issues shall understand them. They must know what they are voting about. And this, in turn, requires that so far as time allows, all facts and interests relevant to the problem shall be fully and fairly presented to the meeting. Both facts and figures must be given in such a way that all the alternative lines of action can be wisely measured. As the self- governing community seeks, by the method of voting, to gain wisdom in action, it can find it only in the minds of its individual citizens. If they fail, it fails. That is why freedom of discussion for those minds may not be abridged"*[16]

[14] See Definition of Democracy in *The Encyclopaedia Britannica: A Dictionary of Arts, Sciences, and General Literature* (Hugh Chisholm, 9th edn, United States: Little, Brown 1889).

[15] Alexander Meiklejohn (n 10) 15-16.

[16] Ibid 24-25.

10 The importance of information and the "right to know" has also been recognised by the Indian Supreme Court[17] in a plethora of cases.[18] In *Dinesh Trivedi v Union of India*, it held:

> *"16. In modern constitutional democracies, it is axiomatic that citizens have a right to know about the affairs of the Government which, having been elected by them, seeks to formulate sound policies of governance aimed at their welfare. However, like all other rights, even this right has recognised limitations; it is, by no means, absolute..."*

11 It follows from the above that legally and otherwise, there exists a right to know that is a necessary concomitant of the right to free speech and is part of the right of political participation that can be enforced in courts of law. The right to access information is vital for self-government and democracy.

12 How should we consider fake news or disinformation in this context?

12.1 Propaganda and dissemination of false or misleading information impact the ability of citizens to "know" and thus to make informed decisions. A survey revealed that nearly a third of Americans had encountered some fake news prior to the election of 2016 and between 80 to 90 percent could not tell whether or not the same was genuine or fake.[19]

12.2 "Citizens can only make truly informed choices about who to vote for if they are sure that those decisions have not been unduly influenced."[20]

12.3 Many malign actors understand information *"in weaponised terms, as a tool to confuse, blackmail, demoralise, subvert and paralyse."*[21] There has been

[17] It is arguable that the US Supreme Court has in the past recognised the validity of arguments for a right to know- in particular in cases dealing with the Fairness Doctrine. However, it is unclear how the Court would deal with such arguments today in the light of the precedent in *Citizens United v FEC* 558 UD 310 (2010).

[18] *SP Gupta v Union of India* 1981 Supp SCC 87; *State of UP v Raj Narain* (1975) 4 SCC 428; *ADR v Union of India* (2002) 5 SCC 294; *Dinesh Trivedi v Union of India* (1997) 3 SCC 306; *Ministry of Information and Broadcasting v Cricket Association* (1995) 2 SCC 161; *Indian Express v Union of India* (1985) 1 SCC 641; *Reliance Petrochemicals v Indian Express* (1988) 4 SCC 592; *Supreme Court v Subhash Chandra* (2020) 5 SCC 481.

[19] Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven, CT, Yale University Press: 2017), 265.

[20] *Investigation into the use of data analytics in political campaigning: a report to Parliament* (*ICO*, 06 November 2018) 6.

[21] Ginsburg and Huq, *How to save a Constitutional democracy* (1st edn., 2019) OUP 110; Peter Pomerantsev, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money,* (Interpreter, 2014).

universal alarm about foreign sources of misinformation impacting elections and political discourse.[22]

12.4 There are concerns that people can be misled by sinister agendas based in part on micro-targeting.[23] Deep-fakes are a particular problem that would add considerably to the difficulty in being able to tell truth from untruth.[24] At least one study has confirmed that micro-targeting techniques can amplify the effects of deep-fakes, by enabling malicious political actors to tailor deep-fakes to susceptibilities of the receiver. The study found that attitudes toward the depicted politician are significantly lower after seeing the deep-fake, but the attitudes toward the politician's party remain similar to the control condition. On zooming in on the micro-targeted group, the study found that both the attitudes toward the politician and the attitudes toward his party score significantly lower than the control condition, suggesting that micro-targeting techniques can indeed amplify the effects of a deep-fake, but for a much smaller subgroup than expected.[25] There does not appear to a study on this but selective editing of political speeches to show speakers in a bad light has been ubiquitous on social media and WhatsApp in India, influencing what millions of people believe about such leaders and certainly having an impact on electoral choices.

12.5 Disinformation further adds to the poison of Hate Speech, resulting in more potent tropes to target minorities.[26] Hate speech interspersed with misinformation[27] spread on social media has provoked and helped in orchestrating violence against minorities.[28] The harm of hate speech is the systematic undermining of the equal standing of persons, rendering them vulnerable to attacks, discrimination and worse.[29] The injury is diffuse

[22] 'Disinformation and 'Fake News': Final Report' (*Parliamentary House of Commons*, 2019) https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf; Cynthia Kroet, 'Russia spread fake news during Dutch elections: Report" (*Politico*, 04 April 2017) https://www.politico.eu/article/russia-spread-fake-news-during-dutch-election-report-putin/; Jeff Seldin, "Russia leading drumbeat' of misinformation ahead of US presidential election" (*VOA News*, 07 September 2020).

[23] Emily Stewart, 'Why everybody is freaking out about political ads on Facebook and Google' (*Vox*, 27 November 2019), https://www.vox.com/recode/2019/11/27/20977988/google-facebook-political-ads-targeting-twitter-disinformation.

[24] Whyte C, 'Deepfake news: AI-enabled disinformation as a multi-level public policy challenge' (2020) J Cyber Policy, https://doi.org/10.1080/23738871.2020.1797135.

[25] Dobber T et al, 'Do (microtargeted) deep fakes have real effects on political attitudes?' (2020) Int J Press/Politics, https://doi.org/10.1177/1940161220944364.

[26] Shivam Vij, "India's anti-muslim fake news factories are following the anti-semitic playbook", (*The Print*, 27 May 2020) https://theprint.in/opinion/india-anti-muslim-fake-news-factories-anti-semitic-playbook/430332/; Tate Ryan-Mosely, 'Its 2020 and anti-semitism is an electoral tactic again' (*MIT Technology Review*, 02 November 2020) https://www.technologyreview.com/2020/11/02/1011603/its-2020-and-anti-semitism-is-an-electoral-tactic-again/.

[27] Archit Mehta, 'Delhi Riots: The link between Misinformation and Radicalisation' (*The Wire*, 24 August 2020) https://thewire.in/communalism/delhi-riots-misinformation-radicalisation-social-media.

[28] The Delhi Assembly is desirous of obtaining testimony from Facebook executives over the Delhi riots of 2020. The matter is currently *sub-judice* in the Supreme Court of India.

[29] Jeremy Waldron, *The Harm in Hate Speech* (2014).

among large groups and may act insidiously and indirectly. At least two of the greatest tragedies of the twentieth century- the holocaust[30] and the Rwandan genocide[31] were made possible because of the widespread prevalence of hate speech interspersed with misinformation against the Jews or the Tutsis. Journalists and publishers have been convicted of war crimes and even genocide. Courts in India are examining the role played by disinformation spread on media that caused the Covid-19 epidemic to be blamed on a minority community.[32]

12.6 There is a species of fake news or disinformation that can aid in what can be called "democratic erosion".[33] Targeted disinformation campaigns direct mistrust at constitutional, public structures and authorities, including the legislature, judiciary, bureaucracy, the media, the opposition, the election commission, and political parties.[34] This is exceedingly grave as faith in public institutions is exactly why Constitutions have endured in democracies such as the UK, US and even India.[35] Cynicism, losing of faith by disinformation campaigns, whether by opportunistic politicians or by international actors, is a real danger to democratic and constitutional structure. There is always the possibility of violent action as an antidote to the perceived election victory of those who run an international ring of paedophiles![36] This distrust also has an impact on the ability of governments to deal with pandemics or health crises.[37]

12.7 The gravity of the problems of disinformation have only been magnified by Covid-19 pandemic. People are spending much more time online and are more exposed to fake news and disinformation than ever before.[38]

[30] Gordon Gregory S, The forgotten Nuremberg Hate Speech Case: Otto Dietrich and the future of persecution law (2014 75 *Ohio State Law Journal*) 571.

[31] *The Prosecutor v Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze* (Appeal Judgement) (28 November 2007, *ICTR-99-52-A*) https://www.refworld.org/cases,ICTR,48b5271d2.html.

[32] 'Plea In Supreme Court seeks directive to Media not to demonise entire Muslim Community for Covid spread' (*India Legal Live*, 08 October 2020) https://www.indialegallive.com/constitutional-law-news/courts-news/plea-in-supreme-court-seeks-directive-to-media-not-to-demonize-entire-muslim-community-for-covid-spread/.

[33] Ginsburg and Huq, (n 21) 43.

[34] Brian Ball, 'Defeating Fake News; On Journalism, Knowledge and Democracy', *Moral Philosophy and Politics*.; Andrea Butler, 'Protecting the Democratic Role of the Press: A Legal Solution to Fake News', (2018) 96 Wash U. L. Rev. 419.

[35] The Constitution is the ultimate "rule of recognition" for the purposes of HLA Hart. It is also the *grundnorm* as per Kelsen.

[36] Referencing the QAnon conspiracy in the US.

[37] Shruti Menon, 'Coronavirus: The Human Cost of Fake News in India', (*BBCWorld*, 30 June 2020) https://www.bbc.com/news/world-asia-india-53165436;
Niranjan Sahu, 'How Fake News is complicating India's war against Covid-19', (*ORF Online*, 13 May 2020) https://www.orfonline.org/expert-speak/how-fake-news-complicating-india-war-against-covid19-66052/.

[38] Alex Hern, 'Facebook, QAnon and the world's slackening grip on reality', (*The Guardian*, 11 November 2020) https://www.theguardian.com/technology/2020/nov/11/how-2020-transformed-big-tech-the-story-of-facebook-qanon-and-the-worlds-slackening-grip-on-reality.

13 The Traditional Position identified in Part A of this essay does not offer clear solutions to this problem. Free speech doctrine evolved to protect speakers from the wrath of authoritarian governments not to control a situation where baseless gossip and slander impact the very basis of society.[39]

[39] Incidentally eavesdropping and spreading rumours were punishable under the Justice of Peace Act, 1361 and are identified as offences in William Blackstone, *Commentaries on the Laws of England* (8th edn., Clarendon Press, Oxford,1778), Vol. IV., 167-168.

13.1 The *first* problem with disinformation or fake news is that it is no longer speech that is scarce or suppressed but has the attention of listeners.[40] The problem isn't too few speakers but too many. It is not silence that impoverishes the public square but a cacophony of discordant noises that drives away citizens from it. The "veil of ignorance", to paraphrase John Rawls, becomes all the more impossible to pierce because of "attentional scarcity".[41] How can one separate the signal from the noise?

[40] Tim Wu, (n 9) P. 548.

[41] Ibid.

13.2 *Second*, censorship in the internet age does not mean the enactment of Licensing Acts like in the 1642[42] but an indirect *de facto* targeting of dissenting voices or opposition leaders targeted by bots or troll armies spouting vicious abuse, doxing, spreading of fake news, deep-fake videos or the flowing of social media with disinformation to confuse rather than enlighten.[43] To confine the definition of censorship to official proscription and to treat these techniques as the normal back and forth of communication is to make a category mistake- these are attempts to silence that are every bit as serious as official censorship and must be treated by law as such. In his seminal article provocatively titled, "Is the First Amendment Obsolete", Tim Wu states:[44]

> *"As Zeynep Tufekci puts it, "censorship during the Internet era does not operate under the same logic [as] it did under the heyday of print or even*

[42] A history of prior restraint law reveals a continuous legal regime of seeking permission before any book was printed from the 1500s till the abolition of the Star Chamber in 1641; then the Licensing Act 1643, the Press Act 1662 till all such laws were allowed to lapse in 1694. See, F Siebert, *Freedom of the Press in England* 1476-1776 (Urbana, University of Illinois Press, 1952); David S Bogen, *The Origins of Freedom of Speech and Press,* (1983) 42 Maryland Law Review, 429.

[43] Tim Wu (n 9).

[44] Ibid. Also see, for example, Shreya Ganguly, 'Youtube disabled 210 channels for videos undermining Hong Kong protests', (*Medianama*, 23 August 2019) https://www.medianama.com/2019/08/223-youtube-disables-210-channels-for-videos-undermining-hong-kong-protests/.

broadcast television."1 Instead of targeting speakers directly, it targets listeners or it undermines speakers indirectly. More precisely, emerging techniques of speech control depend on (1) a range of new punishments, like unleashing "troll armies" to abuse the press and other critics, and (2) "flooding" tactics (sometimes called "reverse censorship") that distort or drown out disfavored speech through the creation and dissemination of fake news, the payment of fake commentators, and the deployment of propaganda robots."

13.3 *Third*, as anyone foolhardy enough to read comments on anything online discovers in a minute, the market place of ideas has not been served well by the glut of information and misinformation. If anything, the marketplace of ideas has operated contrary to the expectations of John Stuart Mill or Alexander Meiklejohn and confounds much more than it clarifies. In an era where expression is "cheap"[45] and where there appear no guardrails or gatekeepers, expression is not always well considered, well researched or adding value to public debate.

13.4 *Fourth*, we all are inexorably being nudged into living in our own bubbles[46] with nary a thought to the wider world outside because of the commercial interest of big tech in offering information and knowledge tailored to our interests, inclinations or pre-conceived notions based on the carefully curated details about our browsing and internet habits available to them. One has to make a special effort to be exposed to different things. Obviously this in not particularly conducive to any effort to "finding" the "truth". Those who say you are entitled to your opinion but not your facts have clearly not spent enough time on the Internet.

[45] Eugene Volokh, 'Cheap Speech and what it will do', (1995) 104 Yale Law Journal 1508.

[46] There is a hilarious sketch on Saturday Night Live about the liberal bubble and how it completely failed to anticipate the election of Donald Trump in 2016. See Megan Barber, 'Saturday Night Live punctures the Liberal Bubble', (*The Atlantic*, 21 November 2016) https://www.theatlantic.com/entertainment/archive/2016/11/saturday-night-live-social-scientist/508337/.

13.5 *Fifth,* who would have thought that indiscriminate freedom of speech would cause the problem rather than cure it? The old bromides of *"[t]he remedy for speech that is false is speech that is true"* and that, as a general matter, *"suppression of speech by the government can make exposure of falsity more difficult, not less so"*, as expounded by the US Supreme Court in *US v Alvarez,*[47] seem like empty incantations because the problem is caused by more speech and the genuine difficulty faced by the unwary in being able to distinguish fact from fabrication.

[47] *US v Alvarez* 567 US 709 (2012).

14 It is pertinent to consider the four justifications offered by John Stuart Mill for free speech:[48]

[48] JS Mill, 'Of the Liberty of Thought and Discussion', *On Liberty* (2nd edn., 1859) JW Parker & Son, London, https://www.utilitarianism.com/ol/two.html.

> *First, if any opinion is compelled to silence, that opinion may, for aught we can certainly know, be true. To deny this is to assume our own infallibility.*
>
> *Secondly, though the silenced opinion be an error, it may, and very commonly does, contain a portion of truth; and since the general or prevailing opinion on any object is rarely or never the whole truth, it is only by the collision of adverse opinions that the remainder of the truth has any chance of being supplied.*
>
> *Thirdly, even if the received opinion be not only true, but the whole truth; unless it is suffered to be, and actually is, vigorously and earnestly contested, it will, by most of those who receive it, be held in the manner of a prejudice, with little comprehension or feeling of its rational grounds. And not only this, but, fourthly, the meaning of the doctrine itself will be in danger of being lost, or enfeebled, and deprived of its vital effect on the character and conduct: the dogma becoming a mere formal profession, inefficacious for good, but cumbering the ground, and preventing the growth of any real and heartfelt conviction, from reason or personal experience.*

It is difficult to see any justification that is not linked to finding out the truth or ensuring that truth prevails over falsehood. Mill's formulation of this indirect justification of false speech has been subjected to criticism because Mill has examined false speech in religious and political matters to the exclusion of examining discourse about "facts."[49] Disagreement on religious dogma or political conviction is usually in good faith while misinformation about facts is not. Meiklejohn argued against censorship in the interest of allowing citizens complete information to make up their mind. Ultimately, both support free speech for instrumental reasons.[50] To subject speech without truth to stricter regulatory scrutiny in comparison to other speech is a departure from traditional doctrine but is not completely inconsistent with its aim and objectives. Learned Hand, J in *International Brotherhood of Electric Workers Local 501 v. NLRB,*[51] spoke of the First Amendment as follows:

> *The interest, which it guards, and which gives it its importance, presupposes that there are no orthodoxies- religious, political, economic, or scientific- which are immune from debate and dispute. Back of that is the assumption- itself an orthodoxy, and the one permissible exception- that truth will be most likely to emerge, if no limitations are imposed upon utterances that can with any plausibility be regarded as efforts to present grounds for accepting or rejecting propositions whose truth the utterer asserts, or denies.*

15 Even in the celebrated case of *Entick v. Carrington*, the judgment of Lord Camden striking down general warrants found it apposite to end with *"One word more for ourselves; we are no advocates for libels, all Governments must set their faces against them, and if juries do not prevent them they may prove fatal to liberty, and the worst Government better than none at all."*[52]

[49] Mark Spottswood, 'Falsity, Insincerity and the Freedom of Expression', (2008) 16 Will. & Mary Bill Rts. J. 1203; James Fitzjames Stephen, *Liberty Equality, Fraternity* (2nd edn., 1874, RJ White Ed. Cambridge Uni. Press, 1967).

[50] Dworkin argues for freedom of speech in the interest of self-actualization. See R. Dworkin, 'The coming battles over Free Speech', (1992) New York Review; R Dworkin 'Free Speech and its limits', (1992) New York Review.

[51] *International Brotherhood of Electric Workers Local 501 v NLRB* 181 F.2d 34 (2nd Circuit 1950).

[52] *Entick v Carrington* 1765 EWHC KB J98.

16 Reasonable regulation[53] to ensure that truth prevails in the public sphere and that misinformation does not derail public reason and decision making is qualitatively different from "censorship" of unpleasant views. It is undertaken for different reasons and leads to different outcomes. Even the most ardent capitalists accept that market failure may on occasion need regulatory oversight. Free speech absolutists may have to do the same for the collapsing marketplace of ideas.

[53] An excellent explanation of reasonable restrictions is contained in *VG Row v State of Madras* AIR 1952 SC 196, per Patanjali Shastri, J.

C. Some Considerations for Regulation

17 Reasonable regulations will have to aim at controlling the onslaught of fake news while continuing to keep at askance heavy headed state censorship. This will require treading a delicate path. The following considerations may be worth thinking about:

18 *First*, no one forces anyone to believe fake news or to act or vote in a particular way because of such fake news. It is likely that there are plenty of factual sources widely available to immediately rebut the most egregious pieces of disinformation if the person makes the conscious effort to look. It is true that the public sphere is simply polluted so much by misinformation that it has becomes ill suited for democratic ends.[54] It is also true that such an inquiry may be difficult when it comes to less egregious untruths. Intuitively it seems, though that if falsehoods have grown in scale, it is frequently because people choose to believe in them, not because they are so bamboozled that they cannot find rebuttals on the internet. What matters in a democracy is that people are able to choose the government they want- whether they want such government for the right reasons or for the wrong can be a matter of moral concern but hardly one to lament the death of democracy. If we accept the authority of the choice of the people as sovereign, then as per Raz, we are pre-empted from questioning the basis of that choice.[55] For the purposes of accepting the democratic character of a polity, it is the will of the people that matters and not the multifarious causes of such will. That the choice is

[54] Tim Wu, (n 9).

[55] See generally Joseph Raz, *The Authority of Law* (1st edn., OUP, Oxford 1979).

not perfect or well informed impacts the quality of decision making in a democracy, but does not damage the essential democratic structure based on the choice of citizens. There is a kind of arrogance in presuming to know what is good for people better than themselves or to presume that their vote depends on this one piece of misinformation.

19 *Second,* banning or removal of disinformation or fake news *per se* would be a disproportionate and a-historical response in most cases, though not all. The banning of dissident websites on the charge of disseminating fake news has already begun[56] and people ought to be wary of empowering the state much leeway in this area. We must be conscious that the cure must not be worse than the disease. Ginsburg and Huq identify three "floor" requirements for a liberal constitutional democracy- free and fair elections, liberal rights of speech and association necessary for the democratic process and the "rule of law". They state:

> *"One cannot have meaningful political competition without relatively free ability to organise and offer policy proposals, criticise leaders, and demonstrate in public without official intimidation...Liberal rights to speech and association are a necessary prophylaxis against anticompetitive behaviour on the part of prospective holders of government power. By ensuring that losers can speak, they lower the stakes of winning, and thus make political competition possible...they provide an essential core of set of entitlements necessary for meaningful democratic competition."*[57]

20 Meiklejohn offers a vigorous defence of hearing false and bad ideas and rejects outright barring of views that are "false or dangerous" stating:

> *"Just so far as, at any point, the citizens who are to decide an issue are denied acquaintance with information or opinion or doubt or disbelief or*

[56] Freedom on the Net 2020, (*Freedom House*, 2020) https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow.

[57] Ginsburg and Huq (n 21) 9-12.

criticism, which is relevant to that cause, just so far the result must be ill-considered, ill-balanced planning, for the general good. It is that mutilation of the thinking process of the community against which the first amendment to the constitution is directed. The principle of the freedom of speech springs from the necessities of the program of self-government. It is not a Law of Nature or of Reason in the abstract. It is a deduction from the basic American agreement that public issues shall be decided by universal suffrage."[58]

21 Rather than focus on outright bans, regulation must be directed towards greater transparency while respecting the value of "anonymous speech".[59] The recent decision by Twitter to mark posts that are questionable is an excellent one[60] as is the decision by Facebook to warn users that articles that they are sharing are over 3 months old.[61] In fact fact-checks before permitting posts to go viral may be an effective way to check the spread of misinformation. The discussions around "linking" social media accounts with personal ID in India[62] were rejected by the Government[63] and the Courts.[64] In any case they ought to be an absolute non-starter for privacy concerns being thoroughly disproportionate to the object sought to be achieved[65]. What would be useful would be the ability to track the post rather than the person posting. Of course, if the post is a crime, the normal procedures to capture the person posting must be taken. However, linking all posts to their creators is a recipe for a chilling effect on all freedom of expression online. On the other hand, disclosure of the location of the post may be very useful indeed. It was revelatory that a lot of "fake news" directed at Trump supporters was actually the handiwork of teens located in small town Macedonia.[66] The British Parliamentary committee was alarmed at the number of posts from the Russian Federation. Outright bans are justifiable only in the case of hate speech upon receipt of complaints though banning only ought to be the last resort in stopping such material from going viral.

[58] Alexander Meiklejohn, (n 10) 25-26.

[59] *NAACP v Alabama* 357 US 449 (1958) encapsulates the reasons why anonymous speech is valuable.

[60] Yoel Roth and Nick Pickles, 'Updating our Approach to Misleading Information' (*Twitter Blog*, 11 May 2020) https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.html; Georgia Wells, 'Twitter says Labels and Warnings slowed spread of False Election claims', (*Wall Street Journal*, 11 November 2020) https://www.wsj.com/articles/twitter-says-labels-and-warnings-slowed-spread-of-false-election-claims-11605214925.

[61] Aroon Deep, 'Facebook to warn users if they are sharing older articles' (*Medianama*, 26 June 2020) https://www.medianama.com/2020/06/223-facebook-older-articles-90-days/.

[62] Apurva Vishwanath, 'Should Aadhar link to social media accounts? The questions before SC', (*Indian Express*, 23 October 2019) https://indianexpress.com/article/explained/should-aadhaar-link-to-social-media-accounts-the-questions-before-sc-6082794/.

[63] 'No Proposal to link Aadhaar to Social Media, Says Prasad', (*Indian Express*, 06 February 2020) https://indianexpress.com/article/technology/tech-news-technology/no-proposal-to-link-aadhaar-to-social-media-says-prasad-6253348/.

[64] 'SC declines to entertain plea to link Aadhaar, Social Media Accounts', (*LiveMint*, 27 May 2020) https://www.livemint.com/news/india/sc-declines-to-entertain-plea-to-link-aadhaar-social-media-accounts-11590522911720.html.

[65] Nikhil Pahwa, 'Against Facebook-Aadhaar Linking', (*Medianama*, 23 August 2019) https://www.medianama.com/2019/08/223-against-facebook-aadhaar-linking/; Gautam Bhatia, "Don't link Aadhaar to social media accounts', (*Hindustan Times*, 25 October 2019) https://www.hindustantimes.com/analysis/don-t-link-aadhaar-with-social-media-accounts-analysis/story-YZtNU4aLvWN7Q2mw0c3gsI.html.

[66] Samanth Subramanian, 'Inside the Macedonian Fake-News Complex' (*Wired Magazine*, 15 February 2017), https://www.wired.com/2017/02/veles-macedonia-fake-news/.

22 *Thirdly,* a distinction needs to be drawn between disinformation and fake news that misdirects or aims to misdirect the public at large and such misinformation that is voluntarily shared between willing persons, who, are part of groups or collectives that exist to share such misinformation. The first kind of disinformation must be targeted by regulation in order to protect the right of the consumer to know the truth and not be misled. The regime of labelling and fact checking would be effective in this regard. The second kind of disinformation must be targeted by regulation insofar as it constitutes hate speech or has the tendency to incite criminal action. This would require immediate action by the social media company, in terms of banning or otherwise.

23 *Fourthly,* paradoxically, the biggest boon and the biggest curse of social media stems from the same source- the power of amplification. Rumour and gossip have existed in every society and have shaped views in democracies and autocracies alike for the entirety of human history. The problems pointed out in this essay and others have not been created by social media but have been amplified by it. Amplification, or sharing has caused the impact that has raised concerns in so many people. By itself, the right to free speech and expression of speakers does not include the right to immediate amplification.[67] As such, controls on the power to amplify do not need to meet the tests prescribed for reasonable restrictions on free speech. Further, the power to amplify can be regulated as a reasonable restriction on the power and ability of big tech companies to conduct their business. Most laws in place target the process of amplification of fake news and temper the protection offered by intermediary liability on the same.[68]

24 *Fifthly,* the regulation of election laws is the obvious place to begin regulation of advertisements or news items that impact electoral choices. The recently

[67] *Morse v Frederic* 551 US 393 (2007).

[68] For example the laws in Ethiopia, Germany and France do this. The discussions to Section 230 of the Communications Decency Act in the USA and to section 79 of the IT Act in India are also likely to go on these lines.

imposed ban on political ads on Facebook or twitter has received mixed reviews[69] but some experimentation is bound to occur as companies deal with unprecedented situations. The decision in *Citizens United*[70] is likely to act as a roadblock in the United States.

[69] Emily Stewart, 'Facebook is banning political ads...after the election', (*Vox*, 07 October 2020) https://www.vox.com/recode/21506912/facebook-bans-political-ads-trump.

[70] *Citizens United v FEC* 558 US 310 (2010).

25 *Sixthly,* there are few areas of law that have seen the sort of whiplash inducing sea change in perspective as has free speech in these times of "fake news" or alternative facts. New laws on "fake news" have been passed or are being drafted in the UK[71], France,[72] Germany,[73] the US, India and elsewhere. Because of the delicate nature of balancing required between the Traditional Position and the unique pathologies of fake news, it is likely that the laws passed shall be work in progress and that countries shall learn from the best practices in other jurisdictions. This is as it should be. We are crossing the river by feeling the stones.

[71] The Parliamentary Report envisages a law.

[72] Law passed in November 2018.

[73] The Network Enforcement Act (Netz DG) passed in 2018

D. Conclusions

26 One of the most chilling cinematic indictments of the nature of disinformation and the impact it may have on ordinary people dates from 1943 and deals with the 'spiteful hysteria'[74] as a result of false rumours spread through poison letters in a small town.[75] *Le Corbeau* made by Henri-Georges Clouzot during the Nazi occupation of France attracted a lightning storm of criticism from the Nazi authorities (because it condemned the concept of informing on your neighbours, a primary technique of occupation) by the French Right (who thought it was anti national as it showed the French in a bad light) and by the French Resistance on the Left (who thought it defeatist and anti-heroic). To this day, *Le Corbeau* remains as disturbing and as immediate as it was in 1943, not in the least because of its ambiguous ending that offers no easy hope or solution and because of the merciless portrait it paints of ordinary people.

[74] This useful phrase is from the review: Le Corbeau (*Times Out*, 1943) https://www.timeout.com/movies/le-corbeau-1943.

[75] The blurb for the Criterion Collection release of Le Corbeau reads as follows: *A mysterious writer of poison-pen letters, known only as Le Corbeau (the Raven), plagues a French provincial town, unwittingly exposing the collective suspicion and rancor seething beneath the community's calm surface. Made during the Nazi Occupation of France, Henri-Georges Clouzot's* Le Corbeau *was attacked by the right-wing Vichy regime, the left-wing Resistance press, the Catholic Church, and was banned after the Liberation. But some—including Jean Cocteau and Jean-Paul Sartre—recognized the powerful subtext to Clouzot's anti-informant, anti-Gestapo fable, and worked to rehabilitate Clouzot's directorial reputation after the war.* Le Corbeau *brilliantly captures a spirit of paranoid pettiness and self-loathing turning an occupied French town into a twentieth-century Salem.*

27 It is tempting to think that the spiteful hysteria or paranoia in *Le Corbeau* was confined to a particular time and place in history (the Nazi occupation of France). However, one cannot but wonder about the state of mind of people who believe the QAnon conspiracy or who planned an elaborate scheme to kidnap Governor Whitmer of Michigan.[76] The fact that nearly half of Republicans feel that the 2020 elections were 'stolen'[77] in the absence of any credible proof remains a sobering thought.

28 In this essay, I have examined the problems that fake news and disinformation create in the democratic process and how the Traditional Position on free speech does not offer solutions to such problems. I have proposed looking at fake news from a fresh perspective considering its nature and how it impacts society. I have then suggested the need for reasonable regulation that must be evolved to balance the new concerns raised by fake news with the Traditional Position. Since efforts to combat fake news are in their infancy, it may be too soon to judge them on their efficacy.

[76] Chuck Goudie and Barb Markoff, 'Disturbing new details in alleged plot to kidnap Michigan Governor Gretchen Whitmer', (*abc7 news*, 19 November 2020) https://abc7chicago.com/michigan-governor-gretchen-whitmer-kidnapping-plot-militia/8079861/.

[77] Alexa Lardieri, 'Half of Republicans believe President Trump won election, Poll finds' (*US News*, 18 November 2020) https://www.usnews.com/news/politics/articles/2020-11-18/half-of-republicans-believe-trump-won-election-poll-finds.

Voting out Election Misinformation in India: How should we regulate Big Tech?

By Jhalak M. Kakkar[1] and Arpitha Desai[2]

A. Introduction

One of the vital aspects of a democratic society is the presence of a healthy and open public sphere where citizens can deliberate upon social issues, ideas, and opinions. A vibrant public sphere allows for a representative and inclusive system of government and puts in place a system of accountability to check the government. Hence, democracies have evolved to guarantee free speech and expression and protect the freedom of the media and press. The press has played a critical role in facilitating the creation and dissemination of quality and accurate information amongst citizens, and has strengthened the public sphere. The emergence of the Internet has broadened the ambit of the public sphere, with Big Tech[3] and other technology companies including messaging platforms, social networking sites and content providers (internet platforms) becoming key forums for interaction between citizens and consumption of news and information.[4] Alongside this, political parties are increasingly harnessing internet platforms for their election campaigns, to share information with citizens and place political advertisements.[5]

However, through the centuries, we have seen that the free flow of information is vulnerable to 'misinformation'.[6] In fact, the emergence of web-based publishing platforms and social media has further enabled the swift spread of misinformation.[7] In this essay, we refer to misinformation to mean "false or inaccurate information that is deliberately created and is intentionally or unintentionally propagated".[8] In the context of elections, such misinformation relates to electoral processes and includes the dissemination of 'fake news'[9] and spread of false information or statements that discredit opponents, influence election outcomes, falsify polling information, etc.

[1] Jhalak is Programme Manager for the Technology and Society Team at the Centre for Communication Governance, National Law University, Delhi. She has an LLM from Harvard Law School on a Fulbright-Nehru Master's Fellowship and a social science and law degree from the National University of Juridical Sciences, Kolkata, India. She can be reached at jhalak.kakkar@gmail.com or @JhalakKakkar on Twitter. We would like to thank our student research assistants, Saachi Agrawal and Vedika Rathore, for their research support.

[2] Arpitha is a public policy lawyer and a Master of Arts in Law and Diplomacy candidate at the Fletcher School of Law and Diplomacy, Tufts University. She has a bachelor's degree in arts and law from Symbiosis Law School, Pune. She can be reached at apitha.desai@tufts.edu or @arpithadesai on Twitter.

[3] Big Tech refers to the largest and most dominant companies in the internet and information technology industry and includes Amazon, Apple, Google, Twitter, Facebook, and Microsoft.

[4] Erlis Çela, 'Social Media as a New Form of Public Sphere' European Journal of Social Sciences (2015) 4(1), 195-200.

[5] Nalin Mehta, 'Digital Politics in India's 2019 General Elections' (*Economic & Political Weekly*, 28 December 2019) https://www.epw.in/node/155766/pdf.

[6] Lejla Turčilo and Mladen Obrenović, 'Misinformation, Disinformation, Malinformation: Causes, Trends, and Their Influence on Democracy' (*Heinrich Böll Foundation*, August 2020) https://hk.boell.org/sites/default/files/importedFiles/2020/11/04/200825_E-Paper3_ENG.pdf; Cherilyn Ireton et al, 'Journalism, 'Fake News' & Disinformation' (*United Nations Educational, Scientific and Cultural Organization*, 2018) https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf.

[7] Dr. Žiga Turk, 'Technology as Enabler of Fake News and a Potential Tool to Combat It' (*Policy Department for Economic, Scientific and Quality of Life Policies*, May 2018) https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619008/IPOL_IDA(2018)619008_EN.pdf; Natalie Nougayrede, 'In this age of propaganda, we must defend ourselves. Here's how' (*The Guardian*, 31 October 2018) https://www.theguardian.com/commentisfree/2018/jan/31/propaganda-defend-russia-technology;

Several significant factors have driven the aggravation of the challenges around misinformation.
While traditional media organisations rely on credible reporting by professional accredited journalists, and content is subject to editorial scrutiny, the emergence of the internet has enabled any user to create and circulate information and news.[10]
While misinformation on internet platforms may arise from user-generated content; it is amplified by the underlying technology and design of internet platforms.[11]

Part B of this essay highlights the role of internet platforms in the spread of election misinformation, the various technology and design features of the internet platforms that have contributed to this phenomenon, and the conflicting interests and incentives of the key stakeholders in this domain to tackle this challenge. Part C discusses how political parties and other groups leverage internet platforms to spread false and misleading information about elections, political processes, parties and candidates. In Part D of the essay, we discuss how the existing legal framework in India that governs the publication and sharing of news and information across various media is inadequate to tackle the issue of election misinformation. Through an analysis of self-regulatory measures taken by internet platforms, in Part E we argue that self-regulatory efforts need to be complemented by regulatory interventions. In Part F, we explain why India should steer clear of seeking to regulate speech and content on internet platforms while attempting to regulate misinformation. We conclude by recommending specific co-regulatory and legislative steps that India should adopt to address the root causes of election misinformation and, at the same time, uphold free speech principles.

Peter Fernandez, 'The technology behind fake news' Library Hi Tech News (2017) 34(7), 1-5. Cherilyn Ireton et al,'Journalism, 'Fake News' & Disinformation' (*United Nations Educational, Scientific and Cultural Organization*, 2018) 23 https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0_0.pdf.

[8] Liang Wu et al, 'Misinformation: Definition, Manipulation, and Detection' ACM SIGKDD Explorations Newsletter (2019) 21(2).

[9] Fake news can be defined as *"information that mimics news media content in form but not in organisational process or intent"*, with fake news outlets lacking *"the news media's editorial norms and processes for ensuring the accuracy and credibility of information"*. D. Lazer et al., 'The science of fake news' Science (2018) 6380, 1094.

[10] Turk (n 7).

[11] 'The digital transformation of news media and the rise of online disinformation' (*European Commission*, 26 April 2018) https://ec.europa.eu/jrc/en/news/digital-transformation-news-media-and-rise-fake-news.

B. Role of internet platforms in the spread of election misinformation

The technology and design features of internet platforms that amplify misinformation include micro-targeting of content based on questionable data collection and user profiling practices, algorithms that encourage filter bubbles and echo chambers leading to polarisation of user opinions, bots that amplify the reach of the content, and a business model fuelled by targeted behavioural advertising.[12] These features propel particular polarising or manipulative content towards specifically targeted users. The targeting of content towards relevant users is fuelled by the collection and processing by the internet platform of significant datasets of the user's demographic information like age, income, religion, caste, gender and location, and other information and characteristics based on interests and behaviour on the platform.[13] This data is used for political profiling to identify vulnerable groups whose opinions can be influenced and manipulated.[14] Based on such information, political parties can strategically choose their audience and target their advertisements on internet platforms. In turn, voters are shown particular political advertisements to influence and manipulate their voting behaviour.[15] Such targeting of content along with the use of bots and other features enables the content to go viral and amplifies a specific opinion.[16] Hence, internet platforms have significant power over information flows and public discourse.[17]

Over the last several years, around the world, we have seen various instances of how misinformation on internet platforms can impact democratic processes such as in the elections in the United States,[18] European Union ('EU'),[19] and India.[20] In particular, the Facebook-Cambridge Analytica incident has raised fundamental questions around the role that internet platforms play in delivering fake news to voters and the resultant impact this can have on democratic elections.[21] Election misinformation unreasonably burdens voters and requires them to determine the authenticity of the information being shared with them,

[12] 'It's the Business Model: How Big Tech's Profit Machine is Distorting the Public Sphere and Threatening Democracy' (*Ranking Digital Rights, 2020*) https://rankingdigitalrights.org/its-the-business-model/.

[13] Shivam Shankar Singh, 'How To Win An Indian Election: What Political Parties Don't Want You To Know' Penguin eBury Press 2019; Carole Cadwalladr, Emma Graham-Harrison, 'How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool' (*The Guardian*, 17 March 2018) https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm.

[14] Yochai Benkler, Robert Faris, Hal Roberts, 'Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics' Oxford University Press 2018; Sangeeta Mahapatra, Johannes Plagemann, 'Polarisation and Politicisation: The Social Media Strategies of Indian Political Parties' (*German Institute of Global and Area Studies*, 01 March 2019) https://www.jstor.org/stable/resrep24806.

[15] Advaita Kala, Om Routray, Osama Manzar, 'Is social media polarising society?' (*The Hindu*, 13 December 2018) https://www.thehindu.com/opinion/op-ed/is-social-media-polarising-society/article25682726.ece; P. J. George, 'Should online political advertising be regulated?' (*The Hindu*, 08 November 2019) https://www.thehindu.com/opinion/op-ed/should-online-political-advertising-be-regulated/article29912107.ece; Prashant Singh, Meghna Sharma, 'In political micro-targeting, the vulnerable Indian voter' (*The Hindu*, 17 February 2020) https://www.thehindu.com/opinion/op-ed/in-political-micro-targeting-the-vulnerable-indian-voter/article30836813.ece.

[16] Ibid.

[17] Ibid.

[18] Hunt Allcott, Matthew Gentzkow, 'Social Media and Fake News in the 2016 Election' *Journal of Economic Perspectives* (2017) 31(2), 211–236; Philip N. Howard et al, 'Social Media, News and Political Information during the US Election: Was Polarizing Content Concentrated in Swing States?', COMPROP DATA MEMO (2017) https://arxiv.org/ftp/arxiv/papers/1802/1802.03573.pdf.

[19] 'Review of European and national elections' (*European Parliament*, September 2019) https://op.europa.eu/en/publication-detail/-/publication/1f2a7ac7-d8f7-11e9-9c4e-01aa75ed71a1.

which impedes their ability to make an informed choice.[22] Given the challenges of targeted misinformation and political advertisements influencing voter behaviour, it is imperative to examine the role of internet platforms in election misinformation, their responsibility in tackling misinformation on their platforms, and potential regulatory mechanisms to address this flow of misinformation.

Any regulatory intervention has to be designed so that it does not negatively impact the freedom of speech and expression of individuals and have a chilling effect on this right, which in turn, can have a detrimental impact on democracy. The conflicting interests and incentives of key stakeholders in the domain also make designing effective regulatory interventions challenging. For instance, political parties and the government often benefit from the spread of election-related misinformation, and hence may be disinclined to tackle the spread of misinformation through appropriate regulation. In the Indian context, we have seen minimal steps by the government or political parties to address election-related misinformation. The Election Commission of India ('ECI'), India's independent constitutional body tasked with overseeing elections, is one of the few stakeholders making some attempts to address the issue by way of statute. On the other hand, global experience across countries including Brazil,[23] Singapore, [24] and Philippines[25] has shown us that often when governments do frame legislation to address misinformation, they design regulation that empowers them with wide powers to curtail speech and legitimate dissent, which impinge free speech, and consequently, the effective functioning of democracy. If we look at another key stakeholder, the internet platforms, their design and business practices further their business model of earning revenues from targeted advertising. However, it is these very design features and business practices that enable the viral and targeted spread of election misinformation, and consequently complicates

[20] Samir Patil, 'India Has A Public Health Crisis. It's Called Fake News.' (*The New York Times*, 29 April 2019) https://www.nytimes.com/2019/04/29/opinion/india-elections-disinformation.html.

[21] Alex Hern, 'Cambridge Analytica: how did it turn clicks into votes?' (*The Guardian*, 06 May 2018) https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie.

[22] Juhi Ahuja, 'Fake News and India's Democracy' (*The Diplomat*, 02 June 2018) https://thediplomat.com/2018/06/fake-news-and-indias-democracy/

[23] Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, PLS 2630/2020.

[24] The Protection from Online Falsehoods and Manipulation Act 2019, No. 18 of 2019 (POFMA).

[25] The Anti-False Content Act Senate 2019, Bill No. 1492.

[26] 'State-wise voter turnout' (*Election Commission of India*, 11 October 2019) https://eci.gov.in/files/file/10971-12-state-wise-voters-turn-out/?do=download&r=30089&confirm=1&t=1&csrfKey=e3db0bb1e71a9d71832ab80327a252aa; Anuja, Pretika Khanna, '2019 Lok Sabha election clocks highest ever turnout at 67.11%' (*Livemint*, 21 May 2019) https://www.livemint.com/elections/lok-sabha-elections/at-67-11-2019-turnout-highest-for-lok-sabha-polls-15583762726 09.html.

the approach of these platforms in tackling misinformation. Additionally, these internet platforms may be reluctant to check the actions of political parties on their platforms, since it is these parties that ultimately frame legislation and regulate various aspects of these platforms.

C. Misinformation on internet platforms in the context of Indian elections

India has over 900 million voters, and in the recent 2019 General Elections, 67% of them had casted their vote.[26] Over the last decade, India has seen massive growth in Internet usage[27] and has the largest number of Facebook and WhatsApp users worldwide.[28] In fact, 80% of Indian adults say they own or share a mobile phone, and 81% of them state that the mobile phone has given them access to news and information on key issues.[29] Hence, there is an increasing reliance on internet platforms to access information and news.

However, increasingly, misinformation campaigns are being circulated through these internet platforms like Twitter,[30] Facebook,[31] and WhatsApp,[32] to spread false and misleading information about elections, political processes, parties and candidates.[33] It has been found that over 53% of Indians received fake news in the lead up to the 2019 General Elections with WhatsApp and Facebook being the key platforms for the circulation of such misinformation.[34] The source of this political misinformation and divisive propaganda is not only the media and government but also political parties and organised interest groups or individuals[35] having a particular vested interest to influence public opinion in a specific direction. This misinformation misleads voters, adversely impacts trust in democratic institutions and undermines the democratic nature of free and fair elections.[36] Hence, though internet platforms have made news and information around elections more accessible to people, they have also given impetus to polarising content that is detrimental to a democratic society.[37]

[27] Noshir Kaka et al, 'Digital India: Technology to transform a connected nation' (*McKinsey Global Institute*, 2019) 23 https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20India%20Technology%20to%20transform%20a%20connected%20nation/MGI-Digital-India-Report-April-2019.ashx.

[28] Sandhya Keelery, 'Internet usage in India-statistics and facts' (*Statista*, 07 July 2020) https://www.statista.com/topics/2157/internet-usage-in-india/.

[29] Responses to this survey were collected from 3,505 adults over 18 years of age through in-person interviews in several languages including Assamese, Bengali, English, Gujarati, Hindi, Kannada, Malayalam, Marathi, Punjabi, Oriya, Tamil, and Telugu.'International Methodology - India', (*Pew Research Centre*, 08 January 2019) https://www.pewresearch.org/methodology/international-survey-research/international-methodology/mobile-technology-and-its-social-impact/india/all-year; 'Mobile Technology and Its Social Impact Survey 2018' (*Pew Research Centre*, 25 March 2019) https://www.pewresearch.org/fact-tank/2019/03/25/indian-elections-nearing-amid-frustration-with-politics-concerns-about-misinformation/.

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

[31] ibid; Kevin Ponniah, 'WhatsApp: The 'black hole' of fake news in India's election' (*BBC News*, 05 April 2019) https://www.bbc.com/news/world-asia-india-47797151.

During the 2019 General Elections, the political machinery of parties embraced various strategies to distribute political content through WhatsApp groups.[38] This content distribution was done by dedicated cyber troops comprising of full-time workers employed year-round to manipulate public opinion online,[39] as well as thousands of office bearers and volunteers at the local level.[40] This content targets not only political rivals but also religious minorities and other dissenting individuals to sow bias and prejudice.[41]

Political parties have leveraged encrypted channels such as WhatsApp to create groups consisting of profiled voters (based on religion, caste, gender, income, etc.) to spread polarising misinformation.[42] WhatsApp has agreed to share metadata (IP address, device number, etc.) with law enforcement agencies to trace the source of misinformation.[43] However, it is critical to see how the spread of misinformation will be prevented without breaking encryption and impinging on the right to privacy and free speech of users.

Another key element of this content dissemination is political advertising on internet platforms such as Facebook and Google.[44] Since spending on political advertising on these platforms is not only done by political parties but also affiliated groups, the extent of political spending on these platforms is unclear. For instance, recent data shows that the Bharatiya Janata Party ('BJP'), the ruling party, was the largest political advertiser on Facebook in India, followed by organisations that seem to be related to the BJP such as "My First Vote for Modi", "Bharat ke Mann ki Baat", and "Nation with NaMo".[45] Such opacity raises serious concerns about the level of scrutiny that may need to be adopted by the ECI and internet platforms to track digital spending on political content and advertisements and resultant outreach of certain political parties and their affiliates.

[32] ibid; Gopal Sathe, 'How The BJP Automated Political Propaganda on WhatsApp' (*The Huffington Post*, 19 April 2019) https://www.huffingtonpost.in/entry/bjp-automated-political-propaganda-whatsapp-sarv_in_5cb62076e4b082aab08d7f18.

[33] Philippa Williams, Lipika Kamra, 'India's WhatsApp election: political parties risk undermining democracy with technology' (*University of Oxford*, 14 March 2019) https://www.qeh.ox.ac.uk/blog/indias-whatsapp-election-political-parties-risk-undermining-democracy-technology.

[34] 'Masses, Message and Medium: Interrogating Dissemination, Penetration and Impact of Fake News through Social Media Technologies in India' (*Social Media Matters & Institute for Governance, Policies, & Politics*, April 2019) https://drive.google.com/file/d/16IDfzX79vGx5OAuXgKHSnILBZHj22Uuc/view.

[35] Anuradha Rao, 'How did Social Media Impact India's 2019 General Election' (*Economic and Political Weekly*, 28 December 2019) https://www.epw.in/node/155783/pdf.

[36] Williams, Kamra (n 27) https://www.qeh.ox.ac.uk/blog/indias-whatsapp-election-political-parties-risk-undermining-democracy-technology.

[37] Rao (n 35).

[38] Sahana Udupa, 'Digital Disinformation and Election Integrity: Benchmarks for Regulation' (*Economic and Political Weekly*, 28 December 2019) https://www.epw.in/node/155940/pdf.

[39] Cyber troops are defined as government or political party actors tasked with manipulating public opinion online. Samantha Bradshaw & Philip N. Howard, Troops, 'Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation' Computational Propaganda Research Project, University of Oxford, UK, Working Paper No. 2017, 12, 3 http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf.

[40] Udupa (n 38).

[41] Snigdha Poonam, Samarth Bansal, 'Misinformation is Endangering India's Election' (*The Atlantic*, 01 April 2019) https://www.theatlantic.com/international/archive/2019/04/india-misinformation-election-fake-news/586123/.

[42] Ponniah (n 31).

[43] Press Trust of India, 'Whatsapp monitoring: FB moots 'prospective' solution, fails to appease govt' (*Business Standard*, 15 September 2019) https://www.business-standard.com/article/pti-stories/facebook-global-exec-moots-prospective-solution-on-whatsapp-issue-govt-stands-firm-on-traceability-119091500194_1.html.

[44] Mehta (n 5).

[45] Krishn Kaushik, 'BJP tops political ad spend on Facebook India' (*The Indian Express*, 27 August 2020) https://indianexpress.com/article/india/facebook-india-ad-money-bjp-congress-6571461/.

[46] The Information Technology Act 2000, s.79 read with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Internet platforms need to comply with existing statutory frameworks that regulate their operations and the content being posted on their platforms. Besides this, internet platforms have designed their content guidelines to govern speech, in the form of user-generated content, on their platforms. Under current Indian legislation, internet platforms may avail safe harbour protection for content posted by third-party users, as long as the platform adheres to certain requirements.[46] Given the role that the design of the algorithms of internet platforms play in enabling the rapid spread of misinformation both in the form of targeted content and political advertisements, we need to critically examine the notion that these platforms are neutral and hence exempt from any obligation to address this issue. However, content regulation is only one element of the overall regulatory framework that has to be framed to address the challenge posed by election misinformation. An effective regulatory framework needs to enhance transparency and accountability around the design and functioning of internet platforms such as the design of their algorithms, collection and use of user data, the role of bots, and targeted advertising business model.

D. Current regulatory framework for misinformation in India

[47] POFMA (n 24).

[48] *Lutte contre la haine sur internet* 2020.

Several government ministries and statutory frameworks regulate the media and information domain in India. While the regulatory frameworks around traditional media address the need for accurate reporting and prohibit false statements, statutory frameworks regulating internet platforms have limited provisions that tackle aspects related to misinformation. Countries such as Singapore[47] and France[48] have specific laws that prohibit misinformation and fake news that may have an adverse effect on the election outcomes. Though India does not have any specific statutory framework or guidelines regulating misinformation or prosecuting those spreading misinformation, there are certain provisions that address misinformation in certain qualified

circumstances. E.g., Section 505 of the Indian Penal Code, 1860 ('IPC') penalises the publication of rumours that may *inter alia* threaten public tranquillity, cause fear or panic to the public or incite any class or community of persons to commit any offence against any other class or community. However, as we discuss later in this essay, it is not advisable at this stage to adopt such a regulatory approach that curtails free speech.

Given the volume of misinformation that is created and circulated on internet platforms by users, including journalists, political parties, and candidates, and the nature of information flows on these internet platforms, the regulation of these platforms would have to be distinct from regulations governing traditional media and require a careful analysis of how such information is disseminated online. While traditional media content is created by accredited journalists, scrutinised by editors, and distributed through conventional channels that often require regulatory licenses or permits, content on internet platforms is largely created and circulated by users without any editorial scrutiny. Add to this the technological design of internet platforms that not only enhance the reach of information but also amplify the spread of misinformation. Before we discuss potential regulatory approaches for misinformation on internet platforms, it is useful to look at a snapshot of how regulation around election misinformation has evolved so far in the context of both traditional media and internet platforms.

I. Traditional media

Traditional media including newspapers, television, and radio have distinct regulatory frameworks in India. These frameworks emphasise the publishing of accurate content in the context of elections and call for reporting objectively about elections and candidates.[49] Additionally, the press is prohibited from publishing unverified or false statements that may prejudice the prospect of a political candidate in the election.[50] For

[49] The Press Council Act 1978; Guidelines to Media on Election Reporting, Press Council of India http://presscouncil.nic.in/OldWebsite/Election%20Reporting-Guidelines%20to%20Media%20and%20Authorities.pdf.

[50] Ibid.

television, channels are prohibited from carrying programs that are false or contain half-truths.[51] Specifically, in the context of elections, news channels have been directed to avoid rumours, baseless speculation, disinformation, especially concerning political parties and their candidates, and instead, maintain accuracy and truth.[52]

[51] The Cable Television Network Rules 1994, rule 6(d).

[52] Guidelines for Election Broadcasts, News Broadcasting Standard Authority https://eci.gov.in/files/file/2173-guidelines-for-broadcasts-media-to-observe-during-election-issued-by-nbsa; Code of Ethics & Broadcasting Standards, News Broadcasting Association http://www.nbanewdelhi.com/assets/uploads/pdf/code_of_ethics_english.pdf.

II. Internet platforms

New media such as social media platforms, news aggregators, and digital media do not have specific statutory frameworks that regulate them. They are broadly regulated by the Information Technology Act, 2000 ('IT Act'), certain specific provisions of the IPC and Criminal Procedure Code, 1973 ('CrPC'), and instructions issued by the ECI.

(i) Information Technology Act

The IT Act is the primary legislation regulating online content, exchange of information online and e-commerce. While the IT Act regulates various types of content on these platforms, such as obscene material, there is no particular provision in the law that deals with misinformation. There are a few provisions under the IT Act which are relevant in the context of a discussion around misinformation:

> *Section 79* enables intermediaries to seek safe harbour protection and be exempt from liability for third-party content, even when such content is in breach of other laws. This immunity depends on the intermediary (1) only providing access to a communication system and performing the role of a platform and not a speaker,[53] (2) not being involved in "*initiating transmission, selecting the receiver of the transmission or selecting or modifying the information contained in the transmission*"[54], and (3) conducting due diligence.[55] These due diligence obligations of an intermediary are enumerated in the Information Technology

[53] The Information Technology Act 2000, s. 79(2)(a).

[54] The Information Technology Act 2000, s. 79(2)(b).

[55] The Information Technology Act 2000, s. 79(2)(c).

(Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021('IG Rules').[56] Among other obligations, intermediaries are obligated to take down 'unlawful content' on receiving actual knowledge.[57] The ambit of unlawful content includes content that is defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise contrary to any law in force.[58] This list does not refer to misinformation as being within the ambit of such unlawful content. However, given the broad wording of the provision, there may be scope for an expansive interpretation of the Rule by the judiciary.

IG Rules: require intermediaries to inform users through their rules and regulations, privacy policy or user agreement that they must not host, display, upload, modify, publish, store, transmit, update or share on their platform information that is (a) in violation of a law such as the IPC,[59] or (b) deceiving or misleading with respect to the origin of the message,[60] or (c) is knowingly and intentionally patently false or misleading in nature but may reasonably be perceived as a fact.[61] These provisions could be potentially brought into play with respect to misinformation.

The IG Rules require significant social media intermediaries to enable the identification of the first originator of the information on their platform when required to do so by authorised government agencies or by a judicial court order for certain purposes including national security, and public order.[62] Besides this, the IG Rules require significant social media intermediaries to deploy technology-based measures or automated tools to proactively identify and remove unlawful content that has previously been requested by a government authority or court to be taken down.[63]

[56] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(d).

[57] Safe harbour protection granted under Section 79 of the IT Act lapses when an intermediary receives "actual knowledge" of any unlawful content on its platform. The Supreme Court of India read down the term "actual knowledge", used in Section 79, to mean that the intermediary would be required to remove or disable access to unlawful material only upon receiving knowledge that a court order has been passed asking the intermediary to do so, or upon receiving notification from an appropriate government; *Shreya Singhal v Union of India* AIR 2015 SC 1523.

[58] The Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(1)(b)(ii).

[59] The Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(1)(b)(v).

[60] The Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021, rule 3(1)(b)(vi).

[61] Ibid.

[62] The Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(2). As per the Rules, significant social media intermediaries are defined as social media platforms with more than a fifty lakh registered user base.

[63] The Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(4).

(ii)_____ECI instructions

Besides the provisions and rules under the IT Act, the ECI has issued instructions in the context of social media use by candidates. The ECI requires candidates to provide information about their social media accounts, seek permission before placing political advertisements, and disclose expenditure on election campaigning done on social media.[64]

(iii)_____Indian Penal Code

The IPC does not have any particular provision that addresses misinformation.[65] However, it does have a specific provision that makes punishable the publication of false statements concerning the character and conduct of a candidate with the intention of affecting the outcome of the election.[66]

(iv)_____Code of Criminal Procedure

Section 144 of the CrPC empowers local administrations to issue prohibitory orders to avoid disturbances such as protests or riots.[67] In exercise of this power, government functionaries have suspended access to mobile and internet networks to preserve law and order when they believe the safety of individuals is at risk. Before the 2019 General Elections, Kashmir,[68] West Bengal[69] and Rajasthan[70] witnessed the suspension of Internet services to ensure the maintenance of law and order and national security and curb the spread of misinformation. This practice has raised concerns around impinging the right to speech and access information, which are critical in the context of elections.

E. Self-Regulation

From the previous section on the current regulatory framework, we can conclude that presently there is limited regulation in India designed to tackle the challenge of misinformation on internet platforms. Following concerns raised by the Government and ECI[71] on the severe implications of misinformation on democratic elections, internet platforms have taken up

[64] Instructions of the Commission with respect to use of social media in election campaigning, Election Commission of India https://eci.gov.in/files/file/637-instructions-of-the-commission-with-respect-to-use-of-social-media-in-election-campaigning/?do=download&r=1384&confirm=1&t=1&csrfKey=e3db0bb1e71a9d71832ab80327a252aa (Social Media Instructions).

[65] There are other provisions of the IPC that have to do with speech and may be relevant in certain situations in the context of misinformation. These include sedition (s. 124A), obscenity (s. 292), defamation (s. 499), intentional insult with the intent to cause breach of peace(s. 504), statements having the potential to result in public mischief (s.505), hurting religious sentiments (s. 295A), and promoting enmity between different groups and doing acts prejudicial to the maintenance of harmony (s. 153A).

[66] The Indian Penal Code 1860, s. 171G.

[67] The Code of Criminal Procedure 1973.

[68] Fayiq Wani, 'Mobile internet services suspended in Kashmir parts as Lok Sabha Polls Phase 2 begins' (*News Nation*, 18 April 2019) https://english.newsnationtv.com/election/lok-sabha-election-2019/mobile-internet-services-suspended-in-kashmir-parts-as-lok-sabha-polls-phase-2-begins-article-220972.html.

[69] James Griffiths, 'India is cutting people off from the internet in the middle of its election' (*CNN*, 08 May 2019) https://edition.cnn.com/2019/05/08/tech/india-election-internet-shutdowns/index.html.

[70] Ibid.

[71] Anumeha Chaturvedi, '2019 - The year of fake news' (*The Economic Times*, 20 December 2019) https://economictimes.indiatimes.com/news/politics-and-nation/fake-news-still-a-menace-despite-government-crackdown-fact-checkers/articleshow/72895472.cms?from=mdr.

initiatives to mitigate the risks posed by election misinformation.

I. Steps taken by internet platforms to combat misinformation

In an attempt to increase the confidence in the electoral process, internet platforms (including Facebook, Twitter, Google, WhatsApp, ShareChat, and TikTok) in collaboration with an industry body, Internet and Mobile Association of India ('IAMAI'), agreed to and adopted a Voluntary Code of Ethics for the 2019 General Elections ('IAMAI Code').[72] By way of the IAMAI Code, internet platforms have committed to implement measures to curb the spread of misinformation on their platforms and ensure the ethical use of social media with the objective of maintaining the integrity of the election process. Among several measures, internet platforms will now follow the 'silent period' rule,[73] verify advertisers of political advertisements and be in constant communication with the ECI for notifying any violations under the Representation of the People Act, 1951.[74]

In tune with the commitments made under the IAMAI Code, internet platforms have introduced various fact-checking features and changes in their platforms to fight misinformation, ensure transparency and raise awareness about recognising fake news. We discuss some of the key steps below.

(i) Political advertisements

Both Facebook and Google launched political advertisements transparency initiatives ahead of the 2019 General Elections. By establishing a publicly available, searchable repository of political advertisements, both companies reported the exact number of political advertisements they received, from whom, and the amount spent on political advertising.[75] However, this does not adequately account for transparency around political advertisements and content posted by affiliate groups or individuals,

[72] 'Voluntary Code of Ethics' (*Internet and Mobile Association of India*, 2019) https://static.pib.gov.in/WriteReadData/userfiles/IAMAI-ECI%20VCE.pdf.

[73] Section 126 of the Representation of People Act, 1951, *inter alia*, prohibits election campaign activities through public meetings, processions, etc., and displaying of election matters by means of television and similar apparatus. The purpose sought to be served by this prohibition is to provide a period of tranquillity (silence period) for the electors before the voting day.

[74] IAMAI Code (n 72).

[75] 'Ad Library' (*Facebook*) https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=IN. 'Political advertising for India' (*Google Transparency Report*) https://transparencyreport.google.com/political-ads/region/IN.

[76] Jason Abbruzzese and Ben Collins,

including spending towards such content.

On the other hand, Twitter, which earlier carried political advertisements on its platforms, has prohibited all forms of political content including advertisements that contain references to political parties or candidates, appeals for votes or solicitations of financial support on the ground that such content may spread misleading misinformation and risk politics and civic discourse.[76] Conservative groups have criticised Twitter's ban on the grounds that it may result in censorship and restrict free speech.[77] This is in stark contrast to Facebook's stance that private companies should not censor politicians and the news, and should provide a platform for all political parties and candidates.[78] However, critics have highlighted that political advertisement spending may create a power asymmetry with only the wealthy political parties having access to such paid channels, which may, in turn, hurt the level playing field during elections.[79]

In India, despite the ECI pre-certifying political advertisements on social media, what is concerning is the lack of transparency as to what data is being used to target advertisements to users and how the design of the internet platforms enables the targeting of such advertisements to influence voter opinion. If internet platforms continue to profile and micro-target voters based on abusive data practices, merely implementing content guidelines that regulate false information would not be enough to tackle misinformation.

(ii)_____Fact-checking mechanisms

Most internet platforms including Google,[80] Twitter,[81] Facebook,[82] and WhatsApp[83] have collaborated with third-party fact-checking organisations to identify and prevent the spread of fake news during elections. Internet platforms like Facebook have adopted various measures to limit the distribution of and access to false and unverified information, restrict the ability of

'Twitter to stop accepting political ads' (*NBC News*, 31 October 2019) https://www.nbcnews.com/tech/tech-news/twitter-stop-accepting-political-ads-n1074171.

[77] Ibid.

[78] Dylan Byers, 'Facebook's Zuckerberg holds line on political ads, but microtargeting could change' (*NBC News*, 05 November, 2019) https://www.nbcnews.com/tech/tech-news/facebook-s-zuckerberg-holds-line-political-ads-microtargeting-could-change-n1076566.

[79] Shivam Vij, 'This election is not a level-playing field' (*The Print*, 29 April 2019) https://theprint.in/opinion/this-election-is-not-a-level-playing-field/228588/.

[80] 'How Google Fights Disinformation' (*Google Blog*, February 2019) https://www.blog.google/documents/37/How_Google_Fights_Disinformation.pdf.

[81] Colin Crowell, 'Our approach to bots and misinformation' (*Twitter Blog*, 14 June 2017) https://blog.twitter.com/en_us/topics/company/2017/Our-Approach-Bots-Misinformation.html; Yoel Roth, Ashita Achuthan, 'Building rules in public: Our approach to synthetic & manipulated media' (*Twitter Blog*, 04 February 2020) https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html.

[82] Ahead of the state elections conducted in Karnataka in 2018, Facebook teamed up with an internationally certified fact-checking organisation, Boom, to help prevent the spread of fake news. Karishma Mehrotra, 'Facebook partners with local fact-checkers for Karnataka elections' (*The Indian Express*, 18 April 2018) https://indianexpress.com/article/technology/social/facebook-partners-with-local-fact-checkers-for-karnataka-elections-5142965/.

[83] Manish Singh, 'WhatsApp pilots new feature to fight misinformation: Search the web' (*TechCrunch*, 04 August 2020) https://techcrunch.com/2020/08/04/whatsapp-pilot-search-the-web-fight-spread-of-misinformation/; 'Here's how WhatsApp plans to fight fake news in India' (*Business Today*, 11 January 2019) https://www.businesstoday.in/buzztop/buzztop-feature/heres-how-whatsapp-plans-to-fight-fake-news-in-india/story/309163.html; Shweta Ganjoo, 'Here is how WhatsApp is fighting fake news on its platform, one feature at a time' (*India Today*, 22 March 2019) https://www.indiatoday.in/technology/news/story/here-is-how-whatsapp-is-fighting-fake-news-on-its-platform-1482463-2019-03-20.

malicious actors to monetise or advertise such posts, show articles that have been verified by fact-checkers, and alert users and page administrators if they are sharing any story determined to be false.[84]

On the other hand, encrypted platforms like WhatsApp have also introduced a fact-checking helpline through which users can send messages, images, video, and text in multiple languages for fact-checking.[85] Additionally, WhatsApp now limits the number of times users can forward a message to only five times to prevent the spread of frequently forwarded messages that may contain misinformation.[86]

Fact-checking and media literacy programmes by independent fact-checking organisations, digital media outlets, and internet platforms have played a key role in educating voters about recognising and fighting fake news. The government, ECI, internet platforms, and civil society must enhance these efforts through collaboration and coordination so as to foster an informed public sphere.

(iii) Take-down of misinformation or removal of fake accounts

Given the prevalence of political bots and fake accounts that facilitate the dissemination of election misinformation, divisive content and fake news online, internet platforms have said that they are stepping up efforts to purge fake accounts.[87] Prior to the 2019 General Elections, Facebook reported that it removed close to 700 pages on the grounds that they were engaging in 'coordinated inauthentic behaviour' and posting partisan content about Indian politics.[88] Similarly, in 2018, Twitter suspended several accounts that were running in the name of the ECI and misleading the public.[89]

[84] To prevent the spread of hoax posts, when stories on Facebook are identified as false news and unverified information, the distribution of and access to such posts are reduced in the 'News Feeds' of users, which in turn, restricts the ability of malicious actors to monetise or advertise such posts. Facebook claims that this has allowed it to reduce the distribution of fake news by 80%. In addition to limiting fake news' visibility, Facebook combats fake news by showing articles by other publishers' as well as the fact checker's article in a 'Related Articles' widget right below the fake story in the News Feed. This gives users "easier access to additional perspectives and information, including articles by third-party fact checkers". Facebook also alerts people and page administrators if they are trying to share a story or have shared a story that has been determined to be false. Sara Su, 'New Test With Related Articles' (*Facebook Blog*, 25 April 2017) https://about.fb.com/news/2017/04/news-feed-fyi-new-test-with-related-articles/; Thuy Ong, 'Facebook begins fact-checking news for users in India, one of its largest markets' (*The Verge*, 17 April 2018) https://www.theverge.com/2018/4/17/17246658/facebook-third-party-fact-checking-india; 'Announcing Third-Party Fact-Checking in India' (*Facebook Blog*, 16 April 2018) https://about.fb.com/news/h/announcing-third-party-fact-checking-in-india/.

[85] Scroll Staff, 'WhatsApp launches new fact-checking service to fight fake news ahead of elections' (*Scroll.in*, 02 April 2019) https://scroll.in/latest/918725/whatsapp-launches-new-fact-checking-service-to-fight-fake-news-ahead-of-elections

[86] 'More changes to forwarding' (*Whatsapp Blog*, 21 January 2019) https://blog.whatsapp.com/more-changes-to-forwarding/?lang=en.

[87] Sankalp Phartiyal, Aditya Kalra, 'Despite being exposed, fake news thrives on social media ahead of India polls' (*Reuters*, 03 April 2019) https://www.reuters.com/article/india-election-socialmedia-fakenews-idUSKCN1RE08Z.

[88] Nathaniel Gleicher, 'Removing Coordinated Inauthentic Behaviour and Spam From India and Pakistan' (*Facebook*, 01 April 2019) https://about.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/.

[89] Bharti Jain, 'Twitter suspends fake Election Commission accounts' (*The Times of India*, 14 November 2018) https://timesofindia.indiatimes.com/india/twitter-suspends-fake-election-commission-accounts/articleshow/66619564.cms.

II. Limitations of the self-regulatory approach

Self-regulatory codes such as the IAMAI Code and other voluntary steps taken by the internet platforms are a welcome start in the fight against misinformation. However, self-regulatory measures are increasingly being viewed as inadequate to counter the proliferation of misinformation and fake news and may need to be complemented by government intervention for effective enforcement.[90] Based on the EU experience experimenting with self-regulation to tackle misinformation, this is the view that is emerging in the EU as well.

On the behest of the European Commission, social media companies operating in the EU adopted a self-regulatory code known as the Code of Practice on Disinformation ('EU Code') in October 2018.[91] Signatories to the EU Code committed to taking relevant action in specified fields, namely, disrupting the advertising revenues of those spreading disinformation, making political and issue-based advertising more transparent, addressing fake accounts and online bots, and empowering consumers and the research community.[92]

In September 2020, the European Commission published its first annual assessment of the policies and tools adopted by the internet platforms to implement the commitments made in the EU Code[93] and concluded that though the EU Code has established a common framework for tackling disinformation, it suffers certain drawbacks. These drawbacks include the self-regulatory nature of the EU Code, the lack of uniformity of implementation, and the lack of clarity around its scope and key concepts.[94] The assessment also proposes adopting a co-regulatory approach that would establish appropriate enforcement mechanisms, sanctions, and redress mechanisms.[95] Other EU Member States[96] and media associations[97] have also highlighted the lack of sanctions within the EU Code and called for more accountability from the social media companies in case of any non-compliance.

[90] Udupa (n 38).

[91] 'Code of Practice on Disinformation', (*European Commission*, 2018) https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[92] Ibid.

[93] 'Assessment of the Code of Practice on Disinformation' (*European Commission*, September, 2020) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69212.

[94] Ibid.

[95] Ibid.

[96] 'Countries call on EU to tackle disinformation more decisively' (*Defend Democracy*, 07 June 2020) https://defenddemocracy.eu/the-corona-virus-pandemic-throws-a-critical-light-on-current-eu-efforts-to-tackle-disinformation/.

[97] 'The EFJ calls for stronger measures to tackle online platforms' disinformation' (*European Federation of Journalists*, 15 June 2020) https://europeanjournalists.org/blog/2020/06/15/the-efj-calls-for-stronger-mea

sures-to-tackle-disinformation-on-online-platforms/.

Consequently, given the increasing consensus around the insufficiency of the self-regulatory approach in effectively tackling the challenge posed by election misinformation to democratic functioning, it is imperative that we explore key co-regulatory and regulatory interventions that could be made in the Indian context.

F. Regulation: The way forward

Effective regulation of election misinformation lies in finding a workable, ethical solution that taps the potential of internet platforms and, at the same time, mitigates the risks of misuse and negative impact of these platforms on democratic processes. Given the beneficial impact internet platforms yield over facilitating public discourse and political participation by voters, it is essential that any regulation of digital content should uphold the principles of free speech. While it may be challenging to eliminate the spread of misinformation on internet platforms, steps that modify the designs and systems enabling the spread of misinformation, can be taken to minimise the flow of misinformation.

In response to the rapid dissemination of election misinformation, regulators worldwide have introduced legislation to identify, combat, and condemn misinformation and fake news. However, several of these laws including those adopted by Germany[98] and Singapore[99] have been criticised on the grounds that regulation of certain categories of speech such as political or commercial speech would impinge on free speech rights and may also threaten the privacy of voters.[100] We draw on this experience, to discuss in Section F.I., why India should steer clear of seeking to regulate speech and content on internet platforms while attempting to regulate misinformation.

The European Commission is moving towards a co-regulatory approach to regulating internet platforms,

[98] *Netzwerkdurchsetzungsgesetz* 2017 (NEA).

[99] POFMA (n 24).

[100] 'Germany: Flawed Social Media Law' (*Human Rights Watch*, 14 February 2018) https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law; 'Singapore: Reject Sweeping 'Fake News' Bill' (*Human Rights Watch*, 03 April 2019) https://www.hrw.org/news/2019/04/03/singapore-reject-sweeping-fake-news-bill; Udbhav Tiwari, 'Mozilla's analysis: Brazil's fake news law harms privacy, security, and free expression' (*Mozilla Blog*, 30 June 2020) https://blog.mozilla.org/netpolicy/2020/06/29/brazils-fake-news-law-harms-privacy-security-and-free-expression/.

which can be seen in the recently proposed Digital Services Act[101] and Digital Markets Act.[102] These regulations call for service providers to work under codes of conduct to address the negative impacts of illegal content and manipulative and abusive activities which are particularly harmful to vulnerable recipients of online services.[103] In the Indian context, though co-regulatory models are not often adopted, an effective law could be framed with extensive stakeholder input and public consultation to ensure that any proposed law accounts for varied interests. We draw on the approaches being developed in various countries and discuss in Section F.II., the potential co-regulatory and legislative steps that can be taken in the Indian context to tackle election misinformation.

[101] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services 2020/0361 and amending Directive 2000/31/EC (DSA).

[102] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector 2020/0374 (DMA).

[103] DSA (n 101); DMA (n 102).

I. Internet Platforms and Governments: Arbiters or censors of speech?

In Germany, the Network Enforcement Act ('NEA') imposes fines of up to 50 million Euros on internet platforms that fail to take down "illegal content" within 24 hours.[104] The scope of illegal content is broad and includes malicious propaganda, defamation, public incitement to crime, incitement to hatred, disseminating portrayals of violence, and threatening the commission of a felony.[105] The content listed above may be relevant in the context of election misinformation.[106] The responsibility to determine the legality of content and interpret the provisions of the law has been conferred upon internet platforms.[107] Human rights advocates have criticised the NEA on the ground that it incentivises over-policing of speech by platforms and therefore infringes upon the right to free speech.[108] The potential over-regulation of content due to platforms lacking the legal expertise to determine the contours of legal and illegal speech may result in censorship of information that may actually be in the public interest.[109]

On the other hand, Singapore's Protection from Online Falsehoods and Manipulation Act ('POFMA'), passed in

[104] NEA, art. 1 § 3(1).

[105] The NEA does not create new categories of illegal content and instead, proposes to implement existing provisions within the German criminal code.

[106] Rebecca Zipursky, 'Nuts About NETZ: The Network Enforcement Act and Freedom of Expression' Fordham International Law Journal (2019) 42(4) 7, 1325-1374.

[107] NEA, art. 1 § 3(2).

[108] 'Flawed Social Media Law' (*Human Rights Watch*, 14 February 2018) https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law; Heidi Tworek and Paddy Leerssen, 'An Analysis of Germany's NetzDG Law' (*Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression*, 2019) https://pure.uva.nl/ws/files/40293503/NetzDG_Tworek_Leerssen_April_2019.pdf.

[109] Ibid.

2019, confers upon government authorities unbridled power to prohibit the communication of false statements that may be against 'public interest' and are likely to "*influence the outcome of a presidential election, general election, by-election or referendum*".[110] However, this power to determine the scope of such false information exposes free speech to arbitrary interpretation and regulation.[111] Additionally, government authorities can direct digital platforms to serve correction notices or stop notices to end-users to either correct or take down content in their posts that is deemed to be against the public interest.[112] In practice, however, this law has been misused to stifle legitimate dissent by opposition leaders who are found questioning the ruling political party's policies online.[113]

Hence, while any potential fake news legislation can restrict the spread of misinformation and penalise those propagating it, such regulation runs the risk of endangering free speech and press freedom which are the cornerstone of any democracy. Taking cues from global experiences as well our own in India, enforcing any law that regulates speech online is likely to infringe upon the fundamental rights of freedom of speech and expression, suppress public debate, and censor legitimate dissent. Furthermore, conferring powers on the government or police force to determine what constitutes misinformation may result in arbitrary interpretation and even misuse. Such abuse of the law has been seen with the working of Section 66A of the IT Act which prohibited the dissemination of false information to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will.[114] In fact, it continues to be used by the government and police to stifle dissent, despite being struck down as unconstitutional by the Supreme Court.[115]

[110] POFMA, s.7(1)(b)(iv).

[111] 'Singapore: New law on "online falsehoods" a grave threat to freedom of expression' (*Article 19*, 09 May 2019) https://www.article19.org/resources/singapore-new-law-on-online-falsehoods-a-grave-threat-to-freedom-of-expression/.

[112] Ibid.

[113] Aradhana Aravindan, 'Singapore opposition party correct posts under 'fake news' law' (*Reuters*, 16 December 2019) https://in.reuters.com/article/us-singapore-fakenews/singapore-opposition-party-corrects-posts-under-fake-news-law-idINKBN1YK09E.

[114] Charu Bahri, 'Interview: Why police still make arrests under IT Act section 66A, years after it was struck down' (*Scroll.in*, 03 December 2018) https://scroll.in/article/904317/interview-why-police-still-make-arrests-under-it-act-section-66a-years-after-it-was-struck-down.

[115] Ibid.

II. Proposed regulatory interventions

While criminalising misinformation or regulating online speech may seem like a solution that directly tackles the challenge of misinformation, learnings from both the Indian and global experience indicate that any law that empowers internet platforms or even the government to be the arbiters of speech, without adequate legal safeguards, may inadvertently fetter free speech. Therefore, till we better comprehend how to adequately protect speech rights while directly regulating misinformation, India should avoid introducing overarching laws to regulate political speech on internet platforms. Instead, India should adopt regulations that address the complex systems of information flows online and design elements of internet platforms that help propagate misinformation. As a starting point, we propose the following regulatory interventions:

(i) Algorithmic design and auditing

Algorithmic or automated decision-making deployed by internet platforms is known to accelerate the dissemination of misinformation and polarise voters through targeted content, including curated news feeds and advertising.[116] However, information about such algorithms is neither publicly disclosed nor independently scrutinised for any inherent bias or harm.[117] To address the potential harms algorithmic decision-making may cause, such as amplifying the visibility of polarising content and creating filter bubbles and echo chambers, there is a need for algorithmic accountability.

Internet platforms, such as Facebook, have argued that the area of content moderation falls within the ambit of the regulation of free speech, and as a private company, it should not be taking down content that can impinge on this right.[118]

[116] Matthew Crain and Anthony Nadler, 'Political Manipulation and Internet Advertising Infrastructure' Journal of Information Policy (2019) 9 p. 370-410; Taberez Ahmed Neyazi, 'Digital propaganda, political bots and polarized politics in India' Asian Journal of Communication (2020) 30, 39-57.

[117] Ibid.

[118] Byers (n 78).

However, the challenge in the context of internet platforms is perhaps less about taking down the content being posted by users and more about addressing how the design of the algorithm amplifies certain content. Algorithms control what content gets enhanced visibility, driven by the algorithm's objective of enhancing user engagement.

To ensure that such algorithms exercise ethical judgement and operate responsibly (for example, non-discrimination on the grounds of religion or caste), regulators should mandate that internet platforms are subject to independent audits and enhanced transparency requirements. These audits of the algorithms can be by a regulator or third-party auditors and researchers approved by the regulator. To incentivise platforms to be transparent, Indian regulators should develop a public scoring or rating system that indicates the level of compliance with algorithmic transparency and disclosure norms by internet platforms. Such transparency will allow the public to access information regarding how the data collected about users is used to profile and target them, and how these algorithms determine what content should target specific users. Transparency will also allow us to better understand the role internet platforms play in the spread of misinformation.

Through these audits, internet platforms should also be required to demonstrate that their technology does not result in *inter alia* malicious propaganda, voter profiling, and micro-targeting. Globally we have seen some preliminary steps in this direction. For example, the EU's General Data Protection Regulation ('GDPR') requires that organisations be able to explain the logic behind their algorithmic decisions that have a significant impact on individuals.[119] Similarly, the proposed Personal Data Protection Bill, 2019 ('PDP Bill') requires technology companies that collect personal data to undertake data protection impact assessments while deploying new profiling technology.[120] However,

[119] The General Data Protection Regulation 2016/679, art. 13-15.

[120] The Personal Data Protection Bill 2019, s. 33(1).

the PDP Bill fails to provide protection against the specific harms from automated profiling and decision-making. Therefore, any such impact assessments should be designed to include the algorithmic audits and transparency measures proposed above. Additionally, the PDP Bill should provide expanded protections against automated decisions that may cause significant harm to users. It remains to be seen how effective these measures will be in preventing the spread of misinformation by micro-targeting. However, the implementation of these measures and learnings from them will give us useful insight into how to tackle the challenge of misinformation.

(ii) Changing the advertising model from behavioural to contextual

As discussed in this essay, economic incentives associated with behavioural advertising facilitate the proliferation of misinformation on internet platforms.[121] Not only does micro-targeting invade a user's privacy but it also provides them with information intended to polarise them.[122] While banning micro-targeting may not be enough to address the issue of misinformation, Indian regulation should require internet platforms to move away from behavioural advertising and adopt contextual advertising, where advertisements are displayed based on relevance or context of what users are viewing rather than their personal data. Evidence shows that the GDPR has prompted publishers to move from behavioural advertising to contextual advertising and geographical targeting, which has continued to bring in substantial revenue without compromising user privacy.[123] We need to pay close attention to the framing of the PDP Bill to ensure a regulatory nudge is provided to internet platforms to move to a contextual advertising business model.

[121] Crain, Nadler (n 116).

[122] Ibid.

[123] Jessica Davies, 'After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue' (*Digiday*, 16 January 2019) https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue; Natasha Lomas, 'Data from Dutch public broadcaster shows the value of ditching creepy ads' (*TechCrunch*, 24 July 2020) https://techcrunch.com/2020/07/24/data-from-dutch-public-broadcaster-shows-the-value-of-ditching-creepy-ads/?guccounter=2.

(iii) Campaign finance transparency and regulating advertisers of political content

Given the role political parties and their affiliated organisations play in the proliferation of election misinformation on internet platforms, it is important that there be complete transparency around the generation of political content and also political spending on advertising on internet platforms by them. Affiliate organisations and individual supporters/influencers (affiliates) have been found to push out election misinformation in a coordinated manner with political parties.[124] Reports indicate that such affiliates can be traced back to the IT cells of political parties and undertake computational propaganda in the form of spreading misinformation and deploying bots, trolls, and fake accounts.[125]

In the context of political advertisements bought by political parties and candidates, internet platforms have started to maintain public files of such advertisements along with amounts paid for such advertisements and by whom.[126] Political advertisements and content posted by political parties and candidates on internet platforms undergo scrutiny by both the ECI and internet platforms and require disclosures to the ECI around spending on these advertisements.[127] However, while there is some requirement of a self-declaration by affiliates to the ECI when placing advertisements, it is unclear as to what kind of scrutiny this is subject to by the ECI, whether it applies to advertising on internet platforms, and whether all affiliates actually undertake this self-declaration.[128] Given this, there seems to be inadequate scrutiny of political advertisements and content shared by affiliates and a lack of transparency around advertising spending by these affiliates. Hence, to tackle the issue of election misinformation, there needs to be enhanced scrutiny and greater transparency around the political advertisements and content shared by affiliates on internet platforms.

[124] 'Removing Coordinated Inauthentic Behaviour and Spam from India and Pakistan' (*Facebook Newsroom*, 01 April 2019) https://about.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/; Apurva Chaudhry, 'BJP and the 'Silver Touch' of Trending Lies' (*News Click*, 25 October 2017) https://www.newsclick.in/bjp-and-silver-touch-trending-lies; Sreenivasan Jain, Manas Pratap Singh, Rohit Bhan, 'Exclusive: The 'Silver Touch' Behind BJP's Online Dominance' (*NDTV*, 23 October 2017) https://www.ndtv.com/india-news/exclusive-silver-touch-behind-bjps-online-dominance-1766114?pfrom=home-india.

[125] Ibid.

[126] Ad Library (n 75).

[127] Social Media Instructions (n 64).

[128] Application for Certification of Advertisement http://ceodelhi.gov.in/WriteReadData/ByeElection2014/AFC.pdf.

Extending this scrutiny to affiliates will be challenging given the potential for a large pool of affiliates operating across several internet platforms. As a starting point, the ECI should frame criteria to identify key affiliates sharing election misinformation content on platforms and seek to monitor their behaviour. The criterion for identifying affiliates can include the number of followers, level of engagement with the page, and amount of spending on advertising. Identifying these affiliates publicly will help build transparency around their operations and enable internet platforms to declare their spending openly. Such transparency will enable public scrutiny by not only the ECI but also researchers, fact-checkers, and legislators, and be a foundational step towards studying such inauthentic behaviour online and identifying relevant tools to combat misinformation. This will, in turn, provide valuable insights about information flows online and empower stakeholders to formulate effective regulatory solutions to tackle the challenge of election misinformation.

G. Conclusion

These internet platforms enhance the public sphere and bring enormous benefit to public discourse in India. However, election-related misinformation and its impact on democratic systems is an increasingly concerning issue as seen across the 2014 and 2019 General Elections and needs to be addressed effectively. The question is how we can harness the benefits these platforms provide while preserving the effective functioning of Indian democracy. Despite self-regulatory measures adopted by internet platforms to limit the spread of misinformation on their platforms, false content and propaganda continue to polarise voters. Global experience has highlighted that the self-regulatory approach is not enough by itself and needs to be complemented by regulatory and co-regulatory steps. As we have argued, since it is difficult to directly sanction misinformation without impinging on free speech, India should focus on regulatory measures that aim to bring transparency in

political spending on digital advertisements and the design and business models of internet platforms. These steps will address some of the key underlying factors that facilitate the viral flow of misinformation and stem its flow, consequently reducing its negative impact on elections and democracy at large.

Disinformation Campaigns in the Age of Hybrid Warfare

By Shreya Bose**

A. Introduction

***Scenario 1*:** *Imagine global and national actors manufacturing crowd ideology through ratings and videos, and bots purchasing likes and instigating followers to join terrorist groups.*

***Scenario 2*:** *Envision a nationalist leader on a podium influencing an audience with an impassioned speech layered in bigotry and half-truths.*

Do either of these scenarios cause discomfort? As a reader, do you note any difference in the ways in which the two scenarios should be approached, and if yes, are the differences only a question of scale and magnitude or are they a matter of more serious legal and societal consequences? In 2020 parlance, both these scenarios could morph into the phrase 'disinformation campaigns' through rampant misuse of technology. These are just a few instances of what Disinformation today looks like. Disinformation, unlike misinformation and mal-information is false information deliberately created to harm a person, social group, organisation or country.[1] While the definition sounds straightforward, this paper will use illustrations to unpack the layered complexity in its legal and social ramifications.

Disinformation was hardly on the agenda for the framers of the UN Charter or the Geneva Conventions. The hue and cry around it is more recent. The rapid advancement in technology and the increased human dependency on connectivity and cyber space have meant that the use of lethal force and warfare have evolved beyond the traditional conception of International Humanitarian Law (IHL) norms and treatises. While neither the scenarios mentioned above nor the definition of disinformation refers to international armed conflict and/or (internationalized) non-international armed conflict *per se*, understanding

** All opinions in this paper are that of the author and cannot be attributed to any organization that she is currently working with, and/or has been in the past or will be affiliated to in the future. The author is grateful to Professor Steven R. Ratner, Professor David Hess, participants and advisors of the 2019 Salzburg Cutler program, Shrutanjaya Bhardwaj, Amitava Bose, Tilman Rodenhäuser and Sana Sud for their valuable inputs in the development of ideas illustrated in this paper. Any faults that may be found, however, maybe attributed to the author alone. The author can be reached at bosesh@umich.edu.

[1] Council of Europe, *Information Disorder: Towards an Interdisciplinary Framework for Research and Policy-Making* (DGI.09, 2009) p. 20.

disinformation in the context of warfare is relevant as it has the potential to cause immense damage to the civilian population. Though we have not found a way to measure the impact of disinformation and are still grappling with indicators and evaluation standards, examples from Myanmar, Iraq, Ukraine, Syria,[2] and more recently Nagorno-Karabakh[3] have surfaced to demonstrate how our inadequate real-time response has impacted civilian population and the existing conflict in general.

To start with, a few basic questions need to be asked – are the current international and concurrent domestic legal frameworks equipped to deal with disinformation campaigns? Who are the primary and secondary actors involved in disinformation campaigns, what responsibility has been attributed to them, and how are they benefitting from disinformation campaigns? This paper will address these basic questions and will argue that the international community needs to, on a priority basis, define and reach a consensus on the debate on "disinformation campaigns" and "fake news". While operating in ambiguity offers the international community a certain degree of latitude to include concerns of domestic approaches to freedom of speech and expression and cultural relativism, I argue that information and expression has a transnational feature that cannot be overlooked. Factors such as the advancement of military technology, extensive use of social media and the role of sophisticated media outlets have in practice transformed the dynamics of hybrid warfare.

Due to the breadth of the subject, the focus of this paper is solely on disinformation campaigns. The paper will not address cyberwarfare at length, although a brief comparison between cyberwarfare and disinformation will be made to explain how they differ. Additionally, while hate speech will be discussed in the context of warfare, the paper will not address how tech companies are dealing with the complexities of the differential application of Article 19, ICCPR[4] across the world.

[2] Christiane Rexilius, `Syria's social media war (since 2011)' (*The Cyber Law Toolkit*, 19 September 2020) https://cyberlaw.ccdcoe.org/wiki/Syria's_'social_media_war'_(since_2011).

[3] Christopher Giles and Upasana Bhat, 'Nagorno-Karabakh: The Armenian-Azeri information wars' (*BBC News*, 26 October 2020) https://www.bbc.com/news/world-europe-54614392.

[4] The International Covenant on Civil and Political Rights, 1976 (referred to as ICCPR).

B. The Interplay of Disinformation, Propaganda and Psychological Warfare

The legality of disinformation campaigns is not a hotly contested topic as there is nothing to indicate their legality. In fact, disinformation campaigns, state propaganda, and psychological warfare are interconnected in practice and have often been used interchangeably by NATO leaders.[5] Although state propaganda and psychological warfare date to as early as the 17th century, disinformation is more a product of the Cold War. While the two ideas were earlier understood to be one and the same, the current interpretation of disinformation campaigns is very different from its previous versions of propaganda and psychological warfare. However, it is pertinent to examine both psychological warfare and state propaganda as disinformation campaigns are centred around them.

Extensively used during the World Wars, psychological warfare has since been institutionalized in many forms – most prominently as ruses of war, i.e. legitimate acts such as calling people to overthrow their national government or diminish national leadership that induce the adversary to act recklessly while not infringing laws on perfidy or international armed conflict.[6] According to IHL, ruses of war such as use of camouflage, decoys, mock operations and misinformation are not prohibited by rules of war.[7] Interestingly, IHL does not address psychological warfare directly, but military and war manuals from Israel[8], Australia,[9] Nigeria,[10] South Africa,[11] the United States[12] make it permissible. These military strategies operate in a grey zone as there is no concrete definition for the term 'psychological warfare' in the manuals and a notable lack of consistency in its implementation.

Scholars have therefore attempted to define psychological warfare as "*propaganda designed to undermine the adversary's will using nonviolent warfare acts and psychological operations to influence the military discipline of the adversary"*(what is interesting is that the

[5] European Union: European Parliament, *Understanding propaganda and disinformation*, (Briefing European Parliamentary Research Service, 2015), p. 2.

[6] Kalliopi Chainoglou, 'Psychological Warfare' (2016) Oxford Public International Law, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e385.

[7] Hague Regulations 1899, Art 24: Hague Regulations 1907, Art 24; Additional Protocol I 1977, Art 37 (2).

[8] ICRC, 'Practice relating to Rule 57: Ruses of War - Israel's Manual on the Laws of War` (1998), IHL Database, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule57.

[9] ICRC, 'Practice relating to Rule 57: Ruses of War - Australia's LOAC Manual ` (2006), IHL Database, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule5.

[10] ICRC, 'Practice relating to Rule 57: Ruses of War - Nigeria's Military Manual` (1994), IHL Database, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule57.

[11] ICRC, 'Practice relating to Rule 57: Ruses of War - South Africa's LOAC Manual` (1996), IHL Database, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule57.

[12] ICRC, 'Practice relating to Rule 57: Ruses of War - The US Field Manual` (1956), IHL Database, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule57.

adversary in such a scenario could be both the military and the civilian population).[13] While caveats such as "*the attack must not be expected to cause excessive injury to civilians*"[14] are in place, such operations against the civilian population appear to be permissible under state practice and law as long as there is no kinetic damage and the psychological operation does not qualify as an 'attack' as per the Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare[15].

Disinformation campaigns also form the basis of state propaganda used to induce and encourage a certain kind of behaviour and mindset. Historically, we have experienced censorship and State propaganda in full effect during the two World Wars. States engaged in conflict kept the media and information dissemination channels in a tight leash, releasing only specific information which would further the State's interests in the war. During World War II, propaganda radio station such as Lord Haw-Haw was established to broadcast Nazi propaganda to the UK from Germany. Such tactics would effectively imply that the information disseminated would either influence public opinion and sentiment on national, political and social issues or be used as a strategy to discriminate against a certain group of people. It is only if there is kinetic impact of these sentiments can accountability be truly sought. The latter was exceptionally seen during the Rwandan conflict when the radio station Radio Television Libre des Mille Collines (RTLM) supported by leaders of the government were responsible for instigating Hutus against Tutsis. RTLM daily played songs demonizing the Tutsis, using slogans of hate and dehumanizing language describing them as '*cockroaches'*, and encouraging people to "*cut down the tall trees*", referring to their height. RTLM also broadcasted names of people to be killed and information of where they could be found, and government soldiers would use these lists to target moderate Hutu families and Tutsis.[16] The United

[13] Kalliopi Chainoglou, 'Psychological Warfare' (2016), Oxford Public International Law, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e385.

[14] Yoram Dinstein, 'Distinction and Loss of Civilian Protection in International Armed Conflicts', in MD Carsten (ed) *International Law Studies* (Naval War College Newport 2008) Volume 84.

[15] Harvard University, 'Manual on International Law Applicable to Air and Missile Warfare: Rule 21' (2009) Program on Humanitarian Policy and Conflict Research, https://reliefweb.int/sites/reliefweb.int/files/resources/8B2E79FC145BFB3D492576E00021ED34-HPCR-may2009.pdf.

[16] Mia Swart, 'Music to kill to: Rwandan genocide survivors remember RTLM' (*Al-Jazeera*, 07 June 2020) https://www.aljazeera.com/features/2020/6/7/music-to-kill-to-rwandan-genocide-survivors-remember-rtlm.

Nations Residual Mechanism for Criminal Tribunals convicted the founder of RTLM along with two others for genocide, crimes against humanity and incitement to genocide in the famous 'media case'[17], with Judge Pillay stating: "*He was fully aware of the power of words, and he used the radio – the medium of communication with the widest public reach – to disseminate hatred and violence....Without a firearm, machete or any physical weapon, he caused the death of thousands of innocent civilians.*"[18]

Disinformation as defined by the Oxford English Dictionary is the "deliberate dissemination of false information, especially when provided by a government or its agent."[19] Over the years, it has gained exponential importance in different parts of the world and has been used by a wide range of actors who have, through diplomatic and media channels, asserted a much broader influence on the population at large or on a more focussed and targeted population. It is commonly seen as a military strategy to supply false information through political, conventional, cyber and irregular channels. In recent times, however, it is also being used as a means of creating major disharmony and division between communities and religious blocks by divisive forces,[20] including non-state actors[21] and financial interest groups.[22] On a few occasions, state agencies have also been suspected of using disinformation as a means to satisfy narrow political ends.[23]

Of note here is the fact that disinformation campaigns conducted in Myanmar against the Rohingya (persecuted ethnic minority) have had a similar effect of fuelling divisive politics. The difference, however, lies in identifying the source. Admittedly, in the case before the International Court of Justice, Gambia has alleged that the anti-Rohingya narrative and anti-Muslim hate speech has been perpetrated by the Government of Myanmar and that it is a part of genocide committed against Rohingyas. But the obvious difficulties of proving the dissemination of disinformation remain apparent.[24] Facebook was hauled up for the slow uptake

[17] *The Prosecutor v Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze* [2007] ICTR-99-52-A

[18] *The Prosecutor v Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze* [2003], ICTR-99-52-T; United Nations International Residual Mechanism for Criminal Tribunals, 'Three Media Leaders convicted for Genocide' (2003) https://unictr.irmct.org/en/news/three-media-leaders-convicted-genocide.

[19] Oxford Learner's Dictionaries, 'Disinformation' https://www.oxfordlearnersdictionaries.com/definition/american_english/disinformation.

[20] Christiane Rexilius, `Hate speech in India (since 2017)' (*The Cyber Law Toolkit*, 19 September 2020) *https://cyberlaw.ccdcoe.org/wiki/Hate_speech_in_India_(since_2017).*

[21] Anne-Marie Balbi, 'The Influence of Non-State Actors on Global Politics' (*Australian Institute of International Affairs*, 26 August 2016) https://www.internationalaffairs.org.au/the-influence-of-non-state-actors-on-global-politics/.

[22] United States Department of Homeland Security, *Combatting Targeted Disinformation Campaigns: A Whole-of-society-issue*, (Homeland Security Digital Library, 2019), p. 11.

[23] Davey Alba and Adam Satariano, 'At least 70 countries have had disinformation campaigns, study finds', (*The New York Times*, 26 September 2019) https://www.nytimes.com/2019/09/26/technology/government-disinformation-cyber-troops.html.

[24] Christiane Rexilius, `Hate speech in Myanmar (since 2010s)' (*The Cyber Law Toolkit*, 19 September 2020) https://cyberlaw.ccdcoe.org/wiki/Hate_speech_in_Myanmar_(since_early_2010s).

on taking down the pages of individuals and organisations associated with the Myanmar military, including that of the Commander in Chief,[25] revealing the lack of transparency and the ease with which the platform was being used to disseminate hate speech. Given that Facebook is a non-state actor with no clear links to the source of such propaganda, it is harder to seek accountability and penalize its actions. Although Article 25(3) of the Rome Statue provides that a person may be criminally responsible for directly and publicly inciting others to commit genocide,[26] which applies even when the incitement is not successful,[27] it would be hard to locate the source of such provocation unless we have full cooperation from such non-state actors in cases where the provocation is done through audio-visual means shared over platforms provided by such non-State actors (as was done in Myanmar). Therein lies the gravity of the problem, where unlike the cases of RTLM and Lord Haw-Haw, the source of propaganda was easily located to be the radio stations.

[25] United Nations, *Report of the Independent International Fact-Finding Mission on Myanmar*, (UN Doc A/HRC/42/50, 2019) para 72.

[26] Rome Statute of the International Criminal Court (Rome Statute), 2187 UNTS 90.

[27] *Prosecutor v Jean-Paul Akayesu*, [1998] ICTR-96-4-T, para 562.

This leads us to question: how could we measure the effect of psychological warfare or disinformation campaigns in cases where there has been kinetic damage? Also, what domestic and international measures have been put in place whereby we can limit the impact of such campaigns in an age of rapidly developing technology?

C. Disinformation Campaigns on Social Media

State and non-state actors now use social media platforms like Facebook to disseminate their propaganda. The NYU Report on Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation (The NYU Report)[28] notes that Facebook has incorporated an algorithm that assesses reading patterns, subjects and activities of interest, and monitors internet history of the user. The NYU Report mentions that the Facebook algorithm provides the user with a unidimensional take on a conflict based on the

[28] NYU Stern Business School: Center for Business and Human Rights, 'Harmful Content: The Role of Internet Platform Companies in Fighting Terrorist Incitement and Politically Motivated Disinformation ' (2017) https://issuu.com/nyusterncenterforbusinessandhumanri/docs/final.harmful_content._the_role_of_?e=31640827/54951655.

aforementioned criteria (meaning only one kind/side of news or story). This mechanism of continuous filtering and tailoring of information can be misused by actors to only feed one kind of information to the public. This is best evidenced by the extensive usage of Twitter and Facebook by the Islamic State of Iraq and Levant (ISIS) during the Iraqi Civil War (2014-2017). The ISIS shared posts and manufactured videos depicting the government's loss of control. It regularly communicated through different channels to recruit people, including impressionable youth from within Iraq, Syria and around the world using social media platforms and communication applications such as Skype and WhatsApp.[29] Further, the ISIS used various other media channels to disseminate doctored videos and disinformation reports,[30] thereby creating confusion as a pretext to annexing cities like Mosul in Iraq. Over the years, the world has lost count of the number of recruits ISIS has managed to amass through their campaigning. It appears that despite their alleged loss of control[31] they are still able to influence polarized populations across countries through the release of recent videos.[32] Therefore, it is imperative to initiate and pursue a discussion on the legal form of disinformation campaigns and its varied implications and effects on population, global order and international peace and security. This is so especially because there is no specific legal framework that captures the nuances of disinformation campaigns and penalizes the perpetrators.

[29] Shehabat, Ahmad, and Teodor Mitew. 'Black-Boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics' (2018) 12 (1) Perspectives on Terrorism, www.jstor.org/stable/26343748.

[30] Note: ISIS used anonymous sharing portals such as Justpaste.it, Sendvid.com and Dump.to, Ibid.

[31] Ben Wedeman and Lauren Said Moorhouse, 'ISIS has lost its final stronghold in Syria, the Syrian Democratic Forces says' (*CNN World*, 23 March 2019) https://edition.cnn.com/2019/03/23/middleeast/isis-caliphate-end-intl/index.html.

[32] Bianca Britton and Hamdi Alkhshali, 'ISIS leader Abu Bakr al-Baghdadi may have reappeared in new video' (*CNN World*, 29 April 2019) https://edition.cnn.com/2019/04/29/middleeast/isis-leader-abu-bakr-al-baghdadi-video-intl/index.html.

D. Measuring the Impact of Disinformation Through Law

Disinformation campaigns, netwars, information warfare, fake news – whatever term one would like to attribute to this new form of weaponization of information – shares a complex relationship with IHL as it is not directly addressed by customary principles of IHL. Yet, I would argue that it cannot escape the traditional trappings of IHL, as Article 36 of the Additional Protocol I compels new methods of warfare to comply with IHL norms and principles. Admittedly, on

paper, IHL would apply to disinformation campaigns and real assessment of damage to civilian population can only be measured if there is a kinetic impact. A straightforward method would be to evaluate if the disinformation campaigns have instigated or fuelled conflict and/or further exacerbated ongoing genocide or crimes against humanity in a way that has resulted in loss of civilian life and/or caused damage to civilian population. However, gathering testimonies that could substantially and clearly establish links between such warfare and loss would not only be belated but may also be hard to obtain.

One example is the case of the 2015 San Bernardino attack, when a couple pledged their allegiance to the ISIS on Facebook moments before shooting 14 people and injuring over 21 people.[33] These attacks were termed as terrorist attacks, and arguably, they are isolated incidents that do not fall within the framework of IHL. If caught, the couple would have been tried on criminal charges in domestic courts. It could be said that the couple had no direct link with the ISIS and therefore the case did not fall under the 'chain of command' or 'superior responsibility' provisions of the Rome Statute. Nor could they be termed as strict soldiers of an established warring party. However, it is also true that the ISIS has instructed to all those who seek to act in their name to publicly pledge allegiance to the group before carrying out a terror attack. The link between such actors and new recruits is undoubtedly tenuous but often it is the only obvious and visible link that connects the act and the perpetrator, with the actor influencing the perpetrator.[34] For all purposes, it is true that such acts of terror are a human rights violation; however, in a situation of IAC or NIAC, it could prove to be extremely dangerous. The relaying of instructions by the ISIS Caliphate, their connection with 'ISIS soldiers', and the increase in such events demonstrate the power of such disinformation campaigns that not only influence behaviour but can also be used as strategic tools for recruitment and the spread of terror.

[33] Office of the United Nations High Commissioner for Human Rights, *Effects of Terrorism on Enjoyment of Human Rights: ISIS/Daesh and Boko Haram*, (Ewelina Ochab and Kelsey Zorzi, 2016), p. 5.

[34] Michael S Schmidt and Richard Pérez-Peña, 'F.B.I. Treating San Bernardino Attack as Terrorism Case', (*The New York Times*, 4 December 2015) https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html.

To assess other means through which we could discern the impact of disinformation campaigns on civilian population, I propose we encourage research on the following two consequences: (1) impact of disinformation campaigns and children and subsequent recruitment, and (2) the link between threat of terror and migration. Although extensive quantitative research has not emerged for the aforementioned, it could be an entry point to understanding the intersection between disinformation campaigns and laws governing the conduct and means of warfare, and the gaps and challenges presented therein.

Recruitment

The innovative methods employed by ISIS in recruiting people across the world for their cause are not beyond the scope of law. In theory, such recruitment is permissible under IHL if it does not violate the restrictions placed on compulsory recruitment[35] or child recruitment.[36] The soft approach of ISIS in recruiting young persons and local children in Iraq and Syria through propaganda campaigns[37] could potentially cross over to other parts of the world. Non-state actors like the Al-Shabaab have been known to recruit from beyond Somalia, as was seen in the infamous recruitment case of Burhan Hassan and his six Somali-American friends from Minneapolis who were taken to Somalia to join the Al-Shabaab. The person responsible for the recruitment drive was tried in the federal courts of US[38] as IHL's material scope of application is subject to geographical limitations[39] with the rules of war regulating and restricting military operations only in conflicting territories. Using radicalized propaganda to recruit youth is not uncommon for non-state actors.[40] However, the link between radical propaganda available online and recruitment of children and youth, and the applicability of Article 19 and 20 of the ICCPR and the Rabat Plan of Action to this relationship, is an area that is academically massively understudied. State action in such cases is limited and requires urgent focus. Tech companies like YouTube on the other hand have

[35] ICRC, 'Recruitment', Casebook: Glossary, https://casebook.icrc.org/glossary/recruitment.

[36] ICRC, 'Child Soldiers', Casebook: Glossary, https://casebook.icrc.org/glossary/child-soldiers.

[37] Mia Bloom, 'Armed Conflict Survey: Child Soldiers in Armed Conflict' (2018) The International Institute for Strategic Studies, https://www.iiss.org/publications/armed-conflict-survey/2018/armed-conflict-survey-2018/acs2018-03-essay-3.

[38] Dina Temple-Raston, 'Minnesota Case Reopens wounds among Somalis' (*National Public Radio*, 19 October 2012) https://www.npr.org/2012/10/19/163258560/minnesota-case-re-opens-wounds-among-somalis.

[39] Geneva Convention 1949, Art 2.

[40] Jessica Trisko Darden, 'Tackling Terrorists' Exploitation of Youth' (2019) American Enterprise Youth https://www.un.org/sexualviolenceinconflict/wp-content/uploads/2019/05/report/tackling-terrorists-exploitation-of-youth/Tackling-Terrorists-Exploitation-of-Youth.pdf.

responded to such concerns by creating technology that tackles violent recruiting discourses online. Their Redirect Method pilot experiment focuses on 'the slice of ISIS' audience that is most susceptible to its messaging, and redirects them towards curated YouTube videos debunking ISIS recruiting themes.[41]

[41] YouTube, https://redirectmethod.org/; United Nations Educational, Scientific and Cultural Organization, *Youth and Violent Extremism on Social Media* (2017) p. 16.

Threats and Acts of Terror

There exists sufficient data to prove that disinformation campaigns are considered threats of terror. Not only is it widely recognized by states[42] and tech companies[43], but it could also be used as an indicator to evaluate the impact of such campaigns on civilian population during warfare. IHL prohibits all acts or threats of violence that have the primary purpose of spreading terror among civilian population.[44] Connecting disinformation campaigns to the threat of terror could be both qualitatively and quantitatively assessed through subsequent migration. Pertinently, if the legality of such disinformation campaigns is to be questioned, then it should be one that is created with the primary aim of spreading terror. The ensuing *en masse* migration (with a probability of civilian casualties) should be a direct and not an incidental consequence of such campaigns. Though a focussed study has not been conducted on this aspect, researchers have suggested that Mosul in Iraq witnessed a population decline by more than half the numbers post ISIS' declaration of Caliphate in the city.[45] Similarly, in the 1990s when Turkey clashed with its Kurdish insurgents, Yilmaz Simsek explored the relationship between migration patterns and acts of terrorism.[46]

[42] European Union, 'Counter Terrorism and radicalization` (*Migration and Home Affairs*) https://ec.europa.eu/home-affairs/what-we-do/policies/counter-terrorism_en; The United States of America, 'Homeland Threat Assessment' (*Homeland Security*, October 2020) https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf.

[43] Facebook, https://www.facebook.com/communitystandards/credible_violence/.

[44] The Geneva Convention relative to the Protection of Civilian Persons in Time of War 1949, Art 33; Additional Protocol I to the Geneva Conventions 1977, Art 51(2); Additional Protocol II to the Geneva Conventions 1977, Art 13(2).

[45] International Centre for Counter-Terrorism- The Hague, 'Links between Terrorism and Migration: An exploration´ (*Alex P. Schmid*, 2016) http://icct.nl/app/uploads/2016/05/Alex-P.-Schmid-Links-between-Terrorism-and-Migration-1.pdf.

[46] *Ibid*; Yilmaz Simsek, 'Impact of Terrorism on Migration Patterns in Turkey' [2006] VCU

Disinform-ation Campaigns and Cyberlaw

The last few decades have witnessed disinformation campaigns being largely conducted in the cyber domain. Due to the target population's heavy reliance on communication through different devices, there is a rapid makeover in the battlefield landscape. However, the status of disinformation as an "attack" or a means of warfare has been extensively contested and poses a certain degree of uncertainty. This is primarily due to

concerns of anonymity afforded to users, subjective interpretation of scale and magnitude of the campaign, private parties acting as proxies and ensuing complexities in attribution,[47] difficulty in taking precautions,[48] and following the IHL principle of distinction between military and civilian population and objects.[49]

According to *Rule 30 of the Tallinn Manual* on the International Law applicable to Cyber-warfare,[50] non-violent operations such as psychological cyber operations or cyber espionage do not qualify as cyber-attacks under International Law.[51] Cyber operations could amount to an 'attack' under IHL if they directly target tangible or intangible legitimate military targets and infrastructure, producing kinetic damage.[52] However it gets complicated in cases where the cyber operations are directed at civilian infrastructure like hospitals, banks etc. with no easily attributable source. September 2020 witnessed the first concrete instance of direct kinetic damage caused by cyber operations, when a patient in a city hospital in Germany died because the hospital was unable to admit her as their systems had been knocked out by a cyber-attack. The prosecutor and head of the cybercrime unit has opened an investigation into negligent homicide against unknown persons[53] as the source of the cyber-attack is yet to be located. Envision this scenario magnified during an IAC or NIAC. That is why it is extremely crucial to think of hypotheticals and draw clear lines on how to react and identify the law that is applicable, even in instances of disinformation campaigns, as they could potentially also lead to direct or indirect kinetic damage in the near future.

If the aim is to regulate such campaigns both at a domestic and transnational level, then countries must focus on developing appropriate redressal mechanisms and legal frameworks because soft law governing cyber-warfare does not account for disinformation campaigns.

[47] Vishaka Choudhary, 'The Truth under Siege: Does International Humanitarian Law Respond Adequately to Information Warfare?' (2019) GroJIL, https://grojil.org/2019/03/21/the-truth-under-siege-does-international-humanitarian-law-respond-adequately-to-information-warfare/.

[48] Additional Protocol I to the Geneva Conventions 1977, Art 57(2)(a).

[49] Additional Protocol I to the Geneva Conventions 1977, Arts 48, 51, 52; Additional Protocol II to the Geneva Conventions 1977, Art 13(2).

[50] Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (Cambridge University Press 2013).

[51] Federal Ministry of Defence of the Federal Republic of Germany, Humanitarian Law in Armed Conflicts Manual ZDv 15/2, (1992).

[52] Laurent Gisel and Tilman Rodenhauser, ` Cyber operations and international humanitarian law: five key points` (2019) ICRC Humanitarian Law & Policy https://blogs.icrc.org/law-and-policy/2019/11/28/cyber-operations-ihl-five-key-points/.

[53] 'Prosecutors open homicide case after cyber-attack on German hospital', (*The Guardian*, 18 September 2020) https://www.theguardian.com/technology/2020/sep/18/prosecutors-open-homicide-case-after-cyber-attack-on-german-hospital.

E. The Legal Grey-Zone in matters of Transnational Mass Disinformation Campaigns

This section will delve into the measures put in place to discuss the transnational nature of disinformation campaigns and scrutinize the obligations of key actors in further detail. Through certain measures, I will be highlighting the need for a more inclusive approach to addressing the issue of disinformation campaigns. At an international level, the advent of cyber technology, enhanced cyber operations and greater access to media have ensured that disinformation can be used to weaken regional blocs, subvert governments, annex territory, and create pretexts for hostile aggression.[54] In recent times, the most quoted examples would be the Russian annexation of Crimea, the conflict between the Islamic State of Iraq and Syria,[55] and the Israel and the Hezbollah war.[56] Each of these instances are different as some involve only state actors while the other conflicts are between Non-state actors and a state, thereby giving rise to different legal implications.

To understand better the nuances of these different scenarios, consider the following:

1. State A launches a disinformation campaign against the civilian population of State B during war time;

2. Non-state actors acting as agents of State A launch a disinformation attack against State B;

3. State A launches a disinformation campaign on the civilian population of State B during peace time, and thereafter launches a military attack.

Keeping in mind, the aforementioned instances, it is worth deliberating on whether states can claim the ground of "self-defence" and/or they have any other legal recourse under the UN Charter?[57] Under the Westphalian notion of sovereignty, any interference in the internal domestic affairs of a state by an external state would be considered a breach.[58] But as the meaning of 'sovereignty' has evolved over time, and

[54] Rand Corporation, 'Understanding Russian Hybrid warfare and what can be done about it: Testimony presented before the House Armed Services Committee on March 22, 2017' (*Christopher S. Chivvis*, 2017) https://www.rand.org/pubs/testimonies/CT468.html.

[55] David Stupples, `What is Information warfare?` (2015) World Economic Forum, https://www.weforum.org/agenda/2015/12/what-is-information-warfare; Renee Diresta, `How ISIS and Russia won friends and manufactured crowds', (*The Wired*, 3 August 2018); The George Washington University, 'ISIS in America From Retweets to Raqqa ´ (2015) Program on Extremism https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/downloads/ISIS%20in%20America%20%20Full%20Report.pdf; Greg Miller and Soud Mekhennet, 'Inside The Surreal World of ISIS: Propaganda Machine` , (*The Washington Post*, 20 November 2015) https://www.washingtonpost.com/world/national-security/inside-the-islamic-states-propaganda-machine/2015/11/20/051e997a-8ce6-11e5-acff-673ae92ddd2b_story.html.

[56] Human Rights Watch, 'Questions and Answers on Hostilities Between Israel and Hezbollah' (2006) https://www.hrw.org/news/2006/08/01/questions-and-answers-hostilities-between-israel-and-hezbollah; Ron Schleifer, 'Psychological Operations: A New Variation on an Age Old Art: Hezbollah versus Israel' (2007) Studies in Conflict & Terrorism, Taylor & Francis online, https://www.tandfonline.com/doi/abs/10.1080/10576100500351185.

[57] U.N Charter 1945, Art 51: Requires the attack to be an "armed" attack.

[58] 'The Legitimate use of Military of Force: The Just War Tradition and the Customary Law of Armed Conflict' in Howard M. Hensel (ed), (Routledge, 2015).

humanitarian law and human rights law have rapidly developed, disinformation campaigns and information warfare struggle to find a place in the legal framework due to the dearth of a focussed study[59] and the non-kinetic nature of the operations involved.[60]

From our analysis so far, the following aspects are clear:

The *first* scenario would *probably* be considered a ruse of war during war time, and therefore legal, unless there is some kind of kinetic impact such as an act or threat of terrorism against the civilian population or protected persons under IHL.

The *second* scenario highlights the role of non-State actors, but if they are proven to be acting as agents of the State, the disinformation campaigns can easily be attributed to the State. Under International Criminal Law, if the source can be attributed to State A, then both the State and the agent could be penalized for their actions.

In the *third* scenario, it may be argued that under just war, if the governing authority of State B receives unambiguous information that an armed attack by State A is imminent, then a pre-emptive strike designed to neutralize the threat is justified on part of State B.[61]

For the first and second scenarios, the big question remains whether disinformation campaigns will qualify as "attacks" or cyber intrusion under IHL and Cyber Law. Furthermore, with the discussion progressing from the traditional interpretation of Article 2(4) of the UN Charter to a more expanded interpretation of 'use of force' that could evolve to include cyber intrusions depending on the severity of their impact,[62] it would be strategic to think of disinformation campaigns as a cyber intrusion against the territorial integrity or political independence of another state, or in any other manner that is inconsistent with the Purposes of the United Nations.[63]

[59] Kalliopi Chainoglou, 'Psychological Warfare', (2016), Oxford Public International Law, http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e385.

[60] United States of America, 'Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities' Committee on Armed Services: House of Representatives (*One Hundred Fifteenth Congress: First Session*, March 2017) https://www.govinfo.gov/content/pkg/CHRG-115hhrg24680/pdf/CHRG-115hhrg24680.pdf.

[61] 'The Legitimate use of Military of Force: The Just War Tradition and the Customary Law of Armed Conflict' in Howard M. Hensel (ed), (Routledge, 2015).

[62] William C Banks, *Developing norms for cyber conflict, Research Handbook on Remote Warfare*, (Edward Elgar Publishing, 2017).

[63] U.N Charter 1945, Art 2(4).

It has been suggested earlier that disinformation has evolved to be an effective military strategy that goes beyond psychological warfare and the textual interpretation of laws on warfare. But despite these complexities, disinformation strategies do not operate in a legal vacuum. Often, relevant domestic and international human rights law are applicable to the said campaigns with the caveat that the thresholds of attribution and accountability are satisfied. If, in the backdrop of disinformation campaigns, the states also engage in armed conflict then principles of IHL will apply. But the legal difficulty arises if a state solely engages in disinformation campaigns to bring about a domestic change in another state without the manifest use of force that would invoke IHL. The Parliamentary Assembly of the EU argues that in such instances, the actions should be examined in the light of domestic criminal law or international legal instruments on hate speech.[64] But this position is problematic as it would probably encourage states to enact strict and draconian laws on freedom of speech in the name of preserving national security and public order. Moreover, in practical terms, states or non-state actors acting as agents of the state cannot be brought to task in national courts of other states,[65] and therefore states would need to engage in other resolution techniques such a diplomacy channels to tackle disinformation campaigns.

[64] Council of Europe: Parliamentary Assembly, *Legal Challenges related to Hybrid war and Human Rights obligations*, (Doc 14523, 2018).

[65] *Jurisdictional Immunities of the State, Germany v Italy, Judgment*, [2012] ICGJ 434; Geoff Gilbert, 'The Criminal Responsibility of States' (1990) 39 The International and Comparative Law Quarterly 345.

F. Discovering Meaningful Ways to Control Disinformation Campaigns

Prior to understanding the role of disinformation in global warfare and distinguishing between counteractive measures employed at both the domestic and international level, the first question to be raised is what type of information is considered by countries to be illicit and what kind of information would be deemed non-illicit. This is a controversial issue by its very nature as different regimes have differing concerns and priorities, as is noted from the varying approaches to freedom of speech and expression and sedition laws across countries.[66] Moreover, to draw lines categorizing

[66] *Refer* to Hate Speech according to German Constitution and the First Amendment rights under the Constitution of United States of America. The International Covenant on Civil and Political Rights 1976, Art 20.

disinformation, certain criteria can be adopted by both social media platforms, media outlets and judicial institutions. For instance, countries can develop strategies to monitor and review the harmful effects of the disinformation being disseminated and determine if the damage needs to be restricted to kinetic damage only. Other factors can include the nature of information and the background in which it is being conveyed, actors responsible for organizing the disinformation campaigns, and the target groups for/against whom the campaigns are being conducted. Legal institutions can also consider the intent behind such campaigns and whether states have the right to informational sovereignty in an international forum. Although intent behind disinformation campaigns cannot be penalized given its similarity to psychological warfare, it should be noted that the latter is only legal during war time and therefore the law can capture disinformation campaigns being conducted during peace time in attempts to instigate war.

Disinformation tactics often exhibit general characteristics of hybrid warfare by being non-linear and legally asymmetrical, but the persistence and degree of intensity of the strategy may differ. In fact, the global phenomenon of "fake news" and creative social media posts[67] that resulted in the Arab Spring uprising, drastic political transitions, growing nationalism, and apathy towards refugees – all fall under the broad umbrella of disinformation. Any individual or terrorist outfit responsible for disinformation campaigns through computer systems within the borders of the state and without any state sponsorship falls solely under the domain of domestic criminal law. At an international level, such individuals or terrorist organizations would be addressed in the Council of Europe Convention on Cybercrime, which now serves as a model law for 63 states that are not just members of such Council.[68] This distinction between individuals and non-state actors responsible for disinformation campaigns at the

[67] Moonyati Yatid, `Disinformation: Economic Loss and Short-run Gains`, (*Institute of Strategic and International studies (ISIS) Malaysia*, 2019 https://www.isis.org.my/2019/01/08/disinformation-economic-loss-and-short-run-gains/.

[68] Johann-Christoph Woltag, 'Cyber Warfare', (2015) Oxford Public International Law https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e280?prd=EPIL; Council of Europe, *Convention on Cybercrime*, (ETS No.185, 2004).

domestic and international levels is critical as the legal frameworks applicable to both are vastly different. Further, the Convention was drafted as a model domestic law, but due to the variance in perspectives and approaches on the framing of freedom of speech and expression and digital rights in different countries, often members of the Convention find it difficult to harmonize it with their domestic laws.

In addition to the above, one the biggest challenges in designing accountability for individuals and non-state actors who are not aligned with any state is creating the balancing act between individual rights and the preservation of public order and national security. The obligation to respect freedom of speech and expression of individuals is binding on every state party as a whole,[69] and state parties are required to ensure that the aforementioned right is given effect to in the State's domestic laws. Though states are permitted to impose restrictions on the exercise of the right based on national security, public order, morals, and, etc., they may not jeopardize the right itself.[70] Therefore, monitoring disinformation at a domestic level is the duty of the state itself and is relative to their legal system and values. For instance, Malaysia recently followed in the footsteps of Germany[71] and introduced the Anti-Fake News Act in the interest of maintaining public order and national security, but despite a efficacious legislation, the Act failed to provide a clear definition of "false information".[72] This has long term consequences as any kind of propagation of "false information" can be penalized under the aforesaid law. Thereby, causing widescale uncertainty and anxiety about the Act itself.

[69] The International Covenant on Civil and Political Rights 1976.

[70] The International Covenant on Civil and Political Rights 1976, Art 19: General Comment No. 34, (HRC 102 Session CCPR/C/GC/34, 2011).

[71] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) 2017.

[72] Anti-Fake News Act 2018; Gulizar Haciyakupogly, `Malaysia's Elections and the Anti-Fake News Act` (*The Diplomat*, 26 April 2018), https://thediplomat.com/2018/04/malaysias-elections-and-the-anti-fake-news-act/.

G. Conclusion: Possible Solutions and the Need of the Hour

An informal way to resolve this issue is to create a multi-stakeholder initiative among regional blocs/countries, non-governmental organizations and social media platforms. In recent times, the European Union ('EU') is leading by example. In order to protect its

its democratic systems and shared values, the EU has set out common concrete measures to tackle disinformation through a Rapid Alert System and close observance of the Code of Practice signed by online platforms such as Facebook, Twitter, Google as well as trade associations representing them and the advertising industry. The Rapid Alert System is said to facilitate data sharing on disinformation threats and assessment of disinformation campaigns, especially during European Parliament elections in 2019.[73]

A multi stakeholder initiative could also be formed among different governments and big and small tech companies. In 2018, the UK Home office claimed to have developed a new technology that automatically detects terrorist content on any platform.[74] To ensure real and integrated progress, such technology should be shared with other countries, big tech companies with a large user base, and also with smaller platforms that are increasingly targeted by non-state actors like ISIS but do not have the same capacity or resources to manage the onslaught of disinformation campaigns.

Although the primary responsibility of dealing with disinformation campaigns lies with the state, private actors like tech companies and businesses also have a secondary obligation to respect human rights, i.e., to avoid infringing human rights of others and address the human rights impacts in which they are involved.[75] This stems from the soft law of UN Guiding Principles on Business and Human Rights. These days, conscious consumerism is gaining the requisite momentum to drive change as consumers, investors, shareholders, governments, regulatory bodies and industry bodies are now more socially conscious of their actions. Therefore, companies like Facebook should step up and assume accountability for the information disseminated on their platforms. After severe backlash on their recent policies, Facebook has stated that it will make political advertising on the platform more transparent by

[73] European Union, 'A Europe that Protects: The EU steps up action against disinformation` (European Commission, 2018) http://europa.eu/rapid/press-release_IP-18-6647_en.html.

[74] United Kingdom, 'New technology revealed to help fight terrorist content online` (Home Office and the Ty Hon Amber Rudd, 2018) https://www.gov.uk/government/news/new-technology-revealed-to-help-fight-terrorist-content-online.

[75] UN Guiding Principles on Business and Human Rights, Principle 11.

requiring advertisements to identify the Facebook page, which has paid for them. It is my understanding that by expanding their services to such options, Facebook is creating space for rampant misuse and overreaching its initial goal of connecting people. To maintain profits, social platforms including Facebook are introducing new features on a daily basis. If that is to be then companies should also ensure that appropriate due diligence and risk assessment tests on such features are conducted regularly.[76] The Oversight Board created in the wake of such backlash is not sufficient. The best way to counter disinformation is to supplement the work of the Oversight Board with active dissemination of neutral information.

A UNESCO report on countering online hate speech stated that "*Counter-speech is generally preferable to suppression of speech. And any response that limits speech needs to be very carefully weighed to ensure that this remains wholly exceptional, and that legitimate robust debate is not curtailed.*"[77] While States can invest in countering online hate speech by presenting an alternative narrative (as USAID is investing in many parts of the world),[78] tech companies can apply the same analogy in their work. Although obscure and non-transparent algorithm facilitates companies to understand their consumers better, with regards to certain sensitive topics such as 'politics', 'international affairs', 'religion' (and other preidentified categories by Facebook), there should be an algorithm created that provides holistic information from the spectrum rather than reinforcing biases.

The need of the hour is to carry forward this discourse both through informal policy and formalised legal channels.

The starting point should therefore be attempts to clearly define and characterize disinformation campaigns in the context of domestic politics and hybrid warfare, as this will enable us to frame laws and/or policies that can limit the damage caused. The

[76] UN Guiding Principles on Business and Human Rights, Principle 15; UN Guiding Principles on Business and Human Rights, Principle 17.

[77] United Nations Educational, Scientific and Cultural Organization, *Countering Online Hate Speech*, (2015).

[78] US Aids, 'Accounting For Risks: A Need For Safeguarding In Digital Ecosystems' (2020) https://www.usaid.gov/usaid-digital-strategy/02-accounting-for-risks.

first point of analysis should centre around the definition of illicit information. As noted above, this is controversial given the different concerns and priorities of different regimes; yet, I propose that social media platforms, media outlets and judicial institutions must adopt certain criteria to enable themselves to categorize disinformation, such as strategies to appraise the harmful effects of the dissemination information (including but not limited to kinetic damage), the nature of information, the context in which information is conveyed, actors responsible for organizing disinformation campaigns, and the target groups for/against whom the campaigns are conducted. Further, states may explore the possibility of invoking the idea of informational sovereignty and punishing the intent behind disinformation campaigns; this may be achieved by equating disinformation campaigns with psychological warfare which is permissible only during war time.

Informally, a few countries are also educating their population to detect doctored videos and fact check. Schools in Finland, Denmark, Netherlands, etc. is taking this fight to classrooms where they are shaping minds to be resilient to fake news by improving news literacy[79] and equip them with tools to critically fact check and interpret all information they receive.[80] Specific companies and networks have also mushroomed tools that fact check and train users to utilize the tools at their disposal such as the google search bar to do basic fact checking.[81] Educating the civilian population is vital as we share the onus of being vigilant with information sharing and critically interpreting the information we receive.

After all, in this age of hybrid warfare, countries may temporarily win the battle on the ground but, if not cautious, could lose the long-lasting information warfare.

[79] Emma Charlton, ` How Finland is fighting fake news - in the classroom` (2019) World Economic Forum, https://www.weforum.org/agenda/2019/05/how-finland-is-fighting-fake-news-in-the-classroom/.

[80] 'How Finland starts its fight against fake news in primary schools', *The Guardian*, (29 January 2020) https://www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news.

[81] International Fact-Checking Network, Poynter Institute https://ifcncodeofprinciples.poynter.org/.

Facial Recognition: Why We Should Worry the Use of Big Tech for Law Enforcement

By Vrinda Bhandari[1]

A. Introduction

In September 2020, the Telangana State Election Commission decided to introduce facial recognition software on a pilot basis in the elections to the Greater Hyderabad Municipal Corporation, by using it in one polling station in each of the 150 wards.[2]
Facial recognition technology ('FRT') has also been introduced in the Hyderabad airport since 2019,[3] and is being used by the Telangana police to track a suspect against the Crime and Criminal Tracking Network and System ('CCTNS') database.[4]
The Telangana Police is also using Artificial Intelligence ('AI')-based systems, through CCTV cameras and FRT, to establish who has not been wearing a mask during the COVID-19 pandemic.[5]

Telangana is not alone. Different agencies and police departments across the country have begun deploying FRT on the premise that it enhances *"efficiency, transparency and accountability in the entire process."*[6] In Chennai, it is *"used to identify suspicious looking people"*; in Delhi, to identify "habitual protestors" and "rowdy elements"; and in Punjab, to gather intelligence in real time.[7]

The terrain of the privacy battle is changing.[8] What was once a subject of cinematic fiction in Minority Report has now become reality, powered by improvements in computational power and artificial intelligence.[9] FRT and Live Facial Recognition Technology have entered our lives – through collaborations between private entities and the State – and are here to stay. As I will show in this piece, rather than improving transparency or efficiency, FRTs end up threatening democracy. Although the use of FRT across different sectors such as education, retail, and travel is increasing,[10] in this piece I will focus primarily on the use of FRT by law

[1] Vrinda Bhandari is a lawyer who works on a variety of digital rights and privacy issues. She can be reached at vrindabhandari89@gmail.com.

[2] 'Facial recognition software in each ward, says SEC' (*The Hindu*, 29 September 2020) https://www.thehindu.com/news/cities/Hyderabad/facial-recognition-software-in-each-ward-says-sec/article32726739.ece; Soumyendra Barik, 'Telangana to use facial recognition on voters in upcoming civic elections' (*MediaNama*, 20 January 2020) https://www.medianama.com/2020/01/223-telangana-facial-recognition-voter-verification/.

[3] 'Hyderabad airport launches Face Recognition system for entry on pilot basis' (*LiveMint*, 02 July 2019) https://www.livemint.com/news/india/hyderabad-airport-launches-face-recognition-system-for-entry-on-pilot-basis-1562059587608.html.

[4] Venkat Ananth, 'In tech-driven Telangana, the eyes have it' (*The Economic Times*, 16 March 2020) https://economictimes.indiatimes.com/technology/in-tech-driven-telangana-the-eyes-have-it/articleshow/74644565.cms.

[5] Aneesha Bedi, 'Geo-mapping, CCTV cameras, AI — how Telangana Police is using tech to enforce Covid safety' (*The Print*, 02 June 2020) https://theprint.in/india/geo-mapping-cctv-cameras-ai-how-telangana-police-is-using-tech-to-enforce-covid-safety/433856/.

[6] 'Introduction to Facial Recognition Projects in India' (*Internet Freedom Foundation*, 17 February 2020) https://internetfreedom.in/facial-recognition-in-india-part-i/; *The Hindu* (n 1).

[7] Vidushi Marda, 'From Protests to Chai, Facial Recognition is Creeping up on us' (*The Economic Times*, 07 January 2020), https://carnegieindia.org/2020/01/07/view-from-protests-to-chai-facial-recognition-is-creeping-up-on-us-pub-80708; https://theprint.in/india/geo-mapping-cctv-cameras-ai-how-telangana-police-is-using-tech-to-enforce-covid-safety/433856/; Jay Mazoomdar, 'Delhi Police film protests, run its images through face recognition software to screen crowd' (The Indian Express, 28 December 2019) https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/.

[8] Jake Goldenfein, 'Facial Recognition is the Only Beginning' (*Public Books*, 27 January 2020) https://www.publicbooks.org/facial-recognition-is-only-the-beginning/#fn-33473-1.

enforcement agencies. In a relationship characterised by lack of consent, the existence of concentrated and centralised State power (including the power to arrest, convict, and sentence a person), and the significant nature of harms caused by the exercise of such power, the use of FRT by law enforcement agencies merits special attention.[11]

For the purpose of this paper, I adopt the Future of Privacy Forum's definition of facial recognition as a *"type of biometric technology that measures and analyses the unique mix of a person's identifiable biometric facial characteristics"* to help in facial detection, classification, authentication, verification, or individual identification.[12]

Part B of the paper will sketch out the privacy and fundamental rights concerns, which arise due to the use of FRT and necessitate the application of the proportionality test. Part C will adopt the four-pronged proportionality test, as laid out in *K.S. Puttaswamy vs Union of India* (*'Puttaswamy'*),[13] and crystalised in *K.S. Puttaswamy vs Union of India (II)* (*'Aadhaar judgment'*),[14] to evaluate the constitutionality of the use of FRT. This involves a specific consideration of the legality, suitability, necessity, and procedural guarantees surrounding the deployment of FRT by law enforcement agencies. Part D will conclude with certain recommendations on the way forward for the use of FRT in India.

While this piece is about FRT and law enforcement, the analysis also has relevance for other emerging areas of AI, machine learning, and augmented reality used by the State, which collectively represent what American Civil Liberties Union ('ACLU') has termed a "phase shift" from *"collection-and-storage surveillance to mass automated real-time monitoring"*.[15]

[9] Sangh Rakshita, 'The Proliferating Eyes of Argus: State Use of Facial Recognition Technology' (*Centre for Communication Governance*, 23 September 2020) https://ccgnludelhi.wordpress.com/2020/09/23/the-proliferating-eyes-of-argus-state-use-of-facial-recognition-technology/.

[10] R. Ravikanth Reddy, 'Facial recognition system introduced in Degree admissions' (*The Hindu*, 22 June 2020) https://www.thehindu.com/news/national/telangana/facial-recognition-system-introduced-in-degree-admissions/article31892709.ece; 'Indian Railways to Use Facial Recognition by 2020 End Despite Warnings Against Privacy Breach' (*Tech2*, 16 November 2020) https://www.firstpost.com/tech/news-analysis/indian-railways-to-use-facial-recognition-by-2020-end-despite-warnings-against-privacy-breach-7982211.html; Soumyendra Barik 'Face recognition systems active at Chaayos outlets without opt-out feature; some questions' (*MediaNama*, 20 November 2019) https://www.medianama.com/2019/11/223-chaayos-face-recognition/; Vijayata Lalwani, 'Facial recognition: As airports in India start using the technology, how will it be regulated?' (*The Scroll*, July 23 2019) https://scroll.in/article/929851/facial-recognition-as-airports-in-india-start-using-the-technology-how-will-it-be-regulated.

[11] Vrinda Bhandari and Renuka Sane, 'Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018' (2018) 14(2) Socio Legal Review 143; Laurent Sacharoff, 'The Relational Nature of Privacy', (2012) 16(4) Lewis & Clark Law Review 1249.

[12] 'Privacy Principles for Facial Recognition' (*Future of Privacy Forum*, December 2015) https://fpf.org/wp-content/uploads/2015/12/Dec9Working-Paper-FacialRecognitionPrivacyPrinciples-For-Web.pdf.

[13] (2017) 10 SCC 1 ('*Puttaswamy*').

[14] (2019) 1 SCC 1 ('*Aadhaar judgment*').

[15] Jay Stanley, 'The Dawn of Robotic Surveillance' (*ACLU*, June 2019) https://www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf.

B. Privacy, Free Speech and Free Assembly: Fundamental Rights and FRT

FRTs capture people's facial features as well as their entire face, often without their consent. This biometric data constitutes sensitive personal information, given the expectation of confidentiality associated with such data; the immutability of the data as part of an individual's identity; and the risk of significant harm that may be caused by its use and misuse.[16]

Large scale deployment of FRT by law enforcement agencies will capture and store people's identities, associations, locations, and even emotions *en masse*, thereby creating a fear of surveillance.[17] It will also systematically monitor, record, and process biometric data of individuals in a public place for identification purposes, raising serious privacy concerns.[18] In addition, the photo stored in the facial recognition system may be linked to other databases (such as social networking profiles or a driving licenses database) that provide contextual personally identifying information and remove any element of anonymity. In this manner, the use of FRT can connect an otherwise anonymous face in a protest to a name, and to all the information available on the public database associated with that name.[19] Researchers at Carnegie Mellon University found that simply combining publicly available online photos (such as a campus photo or a Facebook profile picture) with FRT allowed large-scale, automated, real time individual re-identification online; and inference of additional personal data, and in some cases, sensitive personal data.[20]

These factors cumulatively create a chilling effect on the free speech and expression and the freedom of assembly of people and can serve as a mechanism for social control. Moreover, the continued surveillance through FRT creates a "psychological restraint" in the minds of people that induces fear and psychological harm.[21] Consider for example, the use of FRT and the automated facial recognition systems ('AFRS') by the Delhi Police and the Uttar Pradesh Police during the

[16] Personal Data Protection Bill, 2019, s 15(1).

[17] Stanley (n 14); AI Now Institute, *AI Now 2019 Report* (2019) ch 2.

[18] *P.G. and J.H. v The United Kingdom* [2001] Po LR 325 [57]; *Reklos and Davourlis v Greece* [2009] ECHR 200 [40].

[19] Yana Weilder, 'A Face Tells More Than A Thousand Posts: Developing Face Recognition Privacy in Social Networks' (2012) 26(1) Harvard J of L and Tech 166.

[20] Alessandro Acquisti, Ralph Gross, Frederic D. Stutzman, 'Face Recognition and Privacy in the Age of Augmented Reality' (2014) 6(2) J of Privacy and Confidentiality 1.

[21] *Kharak Singh v State of Uttar Pradesh* 1964 SCR (1) 332; Kaleigh Rogers 'What Constant Surveillance Does to Your Brain' (*Vice*, 14 November 2020) https://www.vice.com/en/article/pa5d9g/what-constant-surveillance-does-to-your-brain.

anti-Citizenship Amendment Act protests in 2019 to identify over 19,000 faces for allegedly inciting violence during the protests.[22] In this process, the police ended up capturing the images of people engaged in a legitimate exercise of their right to free speech (and protest). Worryingly, we have no clarity on whether these images may have ended up on a police database. The reversal of the presumption of innocence by treating every participant in a protest as a potential criminal will create a fear amongst individuals from exercising their democratic rights by receiving and imparting information that may *"offend, shock or disturb the State or any sector of the population"*.[23]

The use of FRT to screen "law and order suspects",[24] is akin to the creation of a national fingerprint database of all citizens for the future prevention or detection of crime, which is a clearly disproportionate means of achieving a State aim.[25] As Spurrier notes, *"When people lose faith that they can be in public space in that free way, you have put arsenic in the water of democracy and that's not easy to come back from."*[26]

Separate claims for violation of fundamental rights under Article(s) 19(1)(a) and 21 of the Constitution of India ('Constitution') arise at the stage of collection, storage, and sharing of facial biometric data. Facial recognition cameras are a biometric system of identification that capture one of the most intimate characteristics of an individual, often without their consent, which may then be verified against a reference dataset that provides additional identifying information.[27] These datasets may contain millions of images, which are often included without the knowledge or consent of the individuals concerned, raising separate privacy concerns.[28]

[22] 'Delhi, UP Police use facial recognition tech at anti-CAA protests, others may soon catch up' (*India Today*, 18 February 2020), https://www.indiatoday.in/india/story/delhi-up-police-use-facial-recognition-tech-at-anti-caa-protests-others-may-soon-catch-up-1647470-2020-02-18.

[23] *Handyside v UK* [1976] 5493/72 [49].

[24] Mazoomdar (n 6).

[25] *M.K. v France* (2013) ECHR 341 [37]; *S & Marper v United Kingdom* [2008] ECHR 1581 [112].

[26] Ian Sample, 'Facial recognition tech is arsenic in the water of democracy, says Liberty' (*The Guardian*, 7 June 2019) https://www.theguardian.com/technology/2019/jun/07/facial-recognition-technology-liberty-says-england-wales-police-use-should-be-banned.

[27] United States Government Accountability Office, *Facial Recognition Technology: Privacy and Accuracy Issues Related to Commercial Uses* (GAO-20-522, July 2020) https://www.gao.gov/assets/710/708045.pdf.

[28] Olivia Solon, 'Facial recognition's 'dirty little secret': Millions of online photos scraped without consent' (*NBC News*, 12 March 2019) https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921; Antoaneta Roussi, 'Resisting the rise of facial recognition' (*Nature*, 18 November 2020) https://www.nature.com/articles/d41586-020-03188-2.

The method and period of storage of such sensitive personal data as well as protocols around sharing such data are left to the complete discretion of the individual private or state entity. For instance, the nation-wide AFRS proposed to be rolled out by the National Crime Records Bureau ('NCRB') envisages a "centralised web application" hosted at the NCRB Data Centre. This national level database of facial images will be "made available for access" to "all police stations" across the country and to all "relevant stakeholders" in order to facilitate "criminal identification and verification".[29] The NCRB has not provided further information on the safeguards to be adopted to ensure purpose limitation and privacy protection.

In addition to these privacy concerns, FRT suffers from a bias and discrimination problem, as I discuss later, which also raises the prospect of the violation of the right to equality guaranteed under Article 14 of the Constitution.

[29] National Crime Records Bureau, *Request For Proposal to Procure National Automated Facial Recognition System (AFRS)* (02/001 Revised) https://drive.google.com/file/d/1KgnURYsFLBqOhLidW28nrbugI--SnKx5/view; Soumyendra Barik, 'NCRB drops CCTV integration clause from updated facial recognition tender, eases bid qualification criteria for vendors' (*MediaNama*, July 02 2020) https://www.medianama.com/2020/07/223-afrs-revised-tender-ncrb/.

C. The Constitutionality of FRT Deployment: A Proportionality Analysis

The collection of highly sensitive forms of personal data such as facial data/biometric data must be accorded the highest degree of protection. The use of FRT infringes the right to privacy, while also creating a chilling effect on the free exercise of speech, expression, and assembly. This raises a claim on the violation of fundamental rights under Articles 19 and 21 of the Constitution. To pass muster, any restriction on fundamental rights must pass the test of proportionality articulated by the Supreme Court in *Puttaswamy* and the *Aadhaar judgment*, which means the restrictions must be (a) imposed by law (legality); (b) a suitable means of achieving a legitimate aim (rational connection); (c) necessary and balanced (necessity), i.e. they should be the least restrictive alternative available to achieve the said goal and on balance, must not disproportionately impact the rights of citizens; and (d) have sufficient procedural guarantees to check abuse against state interference.[30]

[30] *Puttaswamy* (n 12) [311] [314] (Chandrachud J), [638] (Kaul J); *Aadhaar judgment* (n 13) [158], [319], [494], [511.5] (Sikri J).

In this section, I evaluate the legality of FRT from the lens of proportionality. Instead of taking a specific case study where FRT has been challenged, I provide a framework which can be used to evaluate the legality of any future use case of FRT, especially for law enforcement purposes.

I. Legality

The principle of legality requires that all executive action, which operates to the prejudice of any person and violates their fundamental rights, must have the authority of law to support it. It cannot rely solely on executive instructions.[31]

However, the use of FRT, whether by law enforcement agencies or private actors, currently lacks any statutory basis. The Telangana State Election Commission has relied on Article 243ZA of the Constitution, which tasks the State Election Commission with being in charge of all matters relating to the conduct of Municipality elections, as the legal basis for using FRT for voter verification in urban local body elections.[32] The NCRB cites a cabinet note of 2009 as the source of power for authorising the use of AFRS technology.[33] The Delhi Police has justified its use of FRT by citing the Delhi High Court order in *Sadhan Haldar v State of NCT of Delhi*[34] that permitted the use of FRT for the express purpose of tracking and reuniting missing children.[35]

However, all these justifications fail the legality standard. A provision of the Constitution or a cabinet note is not a *specific* authorisation for the infringement of fundamental rights. The restrictions on fundamental rights must be grounded in specific legal provisions that set out the circumstances under which the right can be infringed, and the procedural and substantive safeguards against unconstitutional rights violations.[36] For example, the authorisation of targeted electronic surveillance, the use of Aadhaar for welfare linkage, or the imposition of an internet shutdown are all backed by specific laws or legal regulations.[37] In contrast, a cabinet

[31] *State of Madhya Pradesh v Thakur Bharat Singh* [1967] (2) SCR 454; *Gainda Ram v MCD* [2010] 10 SCC 715; *Kharak Singh* (n 20).

[32] 'Illegal use of Facial Recognition for Voter Verification in Telangana #ProjectPanoptic' (*Internet Freedom Foundation*, 17 March 2020) https://internetfreedom.in/the-telangana-ec/.

[33] NCRB's Response on the Legal Notice received from Internet Freedom Foundation, https://drive.google.com/file/d/0B3J0iAyRzCGxRXViUWcya3RXS0hXb3cxeDJYQU5DWnZKZnhj/view.

[34] *Sadhan Haldar v State of NCT of Delhi* [2017] WP (Crl) No. 1560/2017.

[35] 'Is the illegal use of facial recognition technology by the Delhi Police akin to mass surveillance? You decide. #Project Panoptic' (*Internet Freedom Foundation*, 3 July 2020), https://internetfreedom.in/is-the-illegal-use-of-facial-recognition-technology-by-the-delhi-police-akin-to-mass-surveillance-you-decide-project-panoptic/.

[36] *Malone v United Kingdom* [1984] ECHR 10.

[37] Information Technology Act, 2000, s 69; The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, s 7; The Telecom Suspension Rules 2007; The Indian Telegraph Act, 1885, s 5(2).

note is a record of proceedings and decisions taken at a particular cabinet meeting. It is similar to an executive instruction in that it can be *"amended, altered or withdrawn at the whims and caprice of the executive for the party in power"*,[38] and hence, does not have the status of law. Thus, there can be no *implied limitations* upon fundamental rights through Article 243ZA of the Constitution or the cabinet note of 2009.

[38] *State of Uttar Pradesh v Johri Mal* [2004] 4 SCC 714.

The Delhi Police's reliance on the Delhi High Court order also falls foul of the legality standard, inasmuch as it is well-settled that an order passed by a Court does not have the status of law.[39] Additionally, the High Court order in *Sadhan Haldar* permitted the use of FRT only to track missing children,[40] and an extension of such purpose for deployment in law enforcement is an unwarranted and impermissible function creep.
It is therefore clear that FRT is being implemented in a legal vacuum in India, both in terms of an enabling legislation or a national privacy law, which is contrary to the decision of the Supreme Court in *Puttaswamy,*[41] and is thus, unconstitutional.

[39] *Gainda Ram v MCD* [2010] 10 SCC 715 [67]; *N.R. Mirajkar v State of Maharashtra* [1967] AIR 1967 SC 1; *Puttaswamy* n (11) [502].

[40] *Sadhan Haldar v State of NCT of Delhi*, WP (Crl) No. 1560/2017, order dated 23 August 2019.

[41] *Puttaswamy* n (12).

However, as the recent UK Court of Appeals judgment in *Ed Bridges*[42] demonstrates, having a legal framework is a necessary, but not sufficient condition. A law that authorises the use of FRT must be clear and lay down sufficient safeguards to check the exercise of discretion by law enforcement agencies. Striking down the use of FRT by the South West police as unlawful, the Court of Appeal elaborated on the "fundamental deficiencies" in UK's FRT legal framework (comprising the Data Protection Act of 2018, the Surveillance Camera Code of Practice, and local policies of South Wales Police) in the following manner:

[42] R (*on the application of Edward Bridges*) *v Chief Constable of South Wales Police*, [2020] EWCA Civ 1058.

> *The first is what was called the "who question" at the hearing before us. The second is the "where question". In relation to both of those questions too much discretion is currently left to individual police officers. It is not*

clear who can be placed on the watch-list nor is it clear that there are any criteria for determining where AFR can be deployed.[43]

The Court ruled that the use of automated facial recognition technology by the police breached Ed Bridge's privacy rights, since the legal framework did not sufficiently set out the terms of exercise of the police's discretionary powers and thus, lacked the "necessary quality of law."[44]

[43] ibid [91].

[44] ibid [94].

II. Legitimate Aim and Rational Connection

The second prong of proportionality test requires that the means used for restricting fundamental rights must bear a rational connection with the stated legitimate purpose of the government.[45]

FRT is currently being deployed by law enforcement agencies for a variety of unstated, open-ended, and vague purposes ranging from crime prevention (through tracking of "suspicious", "rowdy" people or "habitual protestors"), criminal profiling and identification (to catch persons not wearing marks during the COVID-19 pandemic), and crime solving (through "smart policing").[46] An anchoring legislation that governs the use of FRT would help limit such vague and over-broad purposes, and prevent a function creep by ensuring accountability over the use of FRT to its stated purpose.

More importantly, the deployment of FRT for law enforcement purpose fails the rational connection test, since facial recognition is not a suitable means of achieving the State's goals of crime prevention or investigation. There are serious doubts about the efficacy and efficiency of the use of FRTs and the direct and indirect discriminatory effects they perpetuate.

It is well documented that FRT and facial analysis systems are not accurate, and suffer from bias, especially while dealing with women, persons of colour, trans persons, and ethnic minorities.[47] A famous study

[45] *Puttaswamy* (n 12) [329] (Chandrachud J); *Aadhaar judgment* (n 13) [319.2], [331], [495.2] (Sikri J). For instance, in the *Aadhaar judgment*, the Supreme Court held that the making of Aadhaar mandatory for bank accounts had no rational nexus with the State goal of controlling black money, since the government had failed to provide any explanation "as to how mandatory linking of every bank account will eradicate/reduce the problems of "money laundering" and "black money".

[46] Bedi (n 4).

[47] Pete Fussey and Dr. Daragh Murrey, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' (2019) University of Essex 10, https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf; Patrick Grother et al, 'Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects', (2019) National Institute of Standards and Technology 1, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; Os Keyes, 'The Misgendering Machines: Trans/HCI Implications of Automatic Gender Recognition' (2018) 88(2) Proceedings of the ACM on Human-Computer Interaction 88, https://ironholds.org/resources/papers/agr_paper.pdf#page=19&zoom=100,0,710.

in 2018 demonstrated that the AI systems being used by private companies were unable to correctly identify the gender of a person in 34% of cases under review.[48] An independent review of London's Metropolitan police facial recognition technology found that it incorrectly flagged a possible innocent person as a suspect 81% of the time, i.e. in 4 out of every 5 cases.[49] In the U.S., 28 members of Congress were incorrectly matched by Amazon's facial recognition software, "Rekognition", to the mug-shot images of people who had been arrested.[50] In India, with our poor data collection, data quality, and storage practices,[51] the error rate is likely to be significant. In such a case, relying on FRT for criminal identification and verification fails the suitable/ rational connection test.

Ironically, such a system of being "perfectly imperfect"[52] is better than a system of perfect accuracy. Marda and Narayan argue that decisions made on a system of predictive policing suffer from historical, representational, and measurement biases in the data collection and creation process that replicates biased policing practices.[53] This causes a vicious cycle where the probability of crime is marked higher in a marginalised or slum area (rather than more privileged socio-economic areas), leading to higher scrutiny and police intervention in such areas, resulting in more arrests and crime reports emerging from these areas.[54] Perfect accuracy would reproduce these biases. This has far-reaching implications when it used for making decisions around arrest and trial in law enforcement context, given that the bias in the algorithm disproportionately impacts vulnerable and marginalised groups, particularly gender, sexual, religious, and caste minorities, whether in India or the U.S.[55] Therefore, it is clear that the discrimination and socio-economic disadvantage that is further entrenched and perpetrated by FRTs cannot be considered a neutral technological choice even in an "accurate" FRT systems.

[48] Joy Boulamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' (Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81, New York, 2018) http://gendershades.org/. This MIT led study found that the IBM Watson gender classification product had an error rate of 34.4% between lighter males and darker females.

[49] Fussey and Murrey (n 46); Rowland Manthorpe and Alexander J Martin, '81% of 'suspects' flagged by Met's police facial recognition technology innocent, independent report says' (*Sky News*, 04 July 2019) https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941.

[50] Jacob Snow, Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots (*ACLU*, 26 July 2018) https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[51] Sonalde Desai, 'Minding the gaps in India's data infrastructure' (*The Hindu*, 24 October 2019) https://www.thehindu.com/opinion/lead/minding-the-gaps-in-indias-data-infrastructure/article29779725.ece; Neetu Chandra Sharma, 'Why India lacks quality in its demographic and health data' (*The Livemint*, 25 July 2019) https://www.livemint.com/news/india/why-india-lacks-quality-in-its-demographic-and-health-data-1564048796002.html; Ankush Agrawal and Vikas Kumar, 'Data deficit and India's peripheral states' (*Hindu Businessline*, 15 November 2020) https://www.thehindubusinessline.com/opinion/data-deficit-and-indias-peripheral-states/article33102887.ece.

[52] Irina Ivanova, 'Why face-recognition technology has a bias problem' (*CBS News*, 12 June 2020) https://www.cbsnews.com/news/facial-recognition-systems-racism-protests-police-bias/.

[53] Vidushi Marda and Shivangi Narayan, 'Data in New Delhi's Predictive Policing System' (*Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, January 2020) https://dl.acm.org/doi/abs/10.1145/3351095.3372865.

[54] Ibid.

[55] Ibid; Shivangi Narayan, 'Predictive Policing and the Construction of the Criminal' (*The Polis Project*, 30 January 2020) https://thepolisproject.com/predictive-policing-and-the-construction-of-the-criminal/; *(citation contd. on next page)*

Thus, both when it works, and when it does not, FRT fails the rational connection test.

III. Necessity

The necessity stage of the proportionality test requires that the government adopt the "least restrictive alternative" that can adequately serve the legitimate state purpose; and that such a measure does not disproportionately impact the fundamental rights of citizens.[56]

Citizens are subject to FRTs deployed by law enforcement agencies, without their choice and consent. Such a measure of compulsion can only be exercised by the State under certain circumstances and under certain limits. For instance, citizens may be forcibly imprisoned upon their conviction as a punishment for law breaking, although, proportionality requires that the law does not sentence a person convicted for an offence of theft to the death penalty.[57] Similarly, a person accused of committing an offence may be forced to give fingerprints, specimen signatures, or blood samples as an aid to police investigation,[58] but cannot be subject to narco-analysis.[59] Finally, under extraordinary circumstances, compulsion may be used by the State to prevent law breaking, as in the case of preventive detention laws. Given the life and liberty interests involved of persons who have neither been accused nor convicted of any crime, such power can only be exercised in exceptional circumstances, circumscribed by procedural safeguards.[60]

However, the compulsion inherent in the use of FRT as a law enforcement tool to police protests goes beyond these narrow limitations described above. When used as crime prevention measure, such as to screen potential miscreants or "habitual protestors" in a crowd or protest, FRT targets *all* citizens. Law enforcement agencies do not have to satisfy any reasonable belief, much less require a judicial determination, to demonstrate that a person attending a protest might be

[55] Sandra Mayson, 'Bias In, Bias Out' (2019) 128 Yale Law Journal 2218; Anja Kovacs, 'When Our Bodies Become Data Where Does That Leave Us' (*Deep Dives*, 28 May 2020) https://deepdives.in/when-our-bodies-become-data-where-does-that-leave-us-906674f6a969.

[56] *IAMAI v Union of India* [2020] SCC Online 275 and *Puttaswamy* (n 12).

[57] The Indian Penal Code, 1860, s 379.

[58] The Code of Criminal Procedure, 1973, s 53 and 311A; *State of Bombay v Kathi Kalu Ogad* [1962] 3 SCR 10 [10], [11].

[59] *Selvi v State of Karnataka* [2010] 7 SCC 263.

[60] *State of Tamil Nadu v Nabila* [2015] 12 SCC 127 [12], [13].

planning to disrupt public order or even be accused of committing an earlier crime. Treating all citizens as potential criminals is disproportionate and arbitrary, creates a risk of stigmatisation,[61] and based on the principles enunciated in the *Aadhaar judgment*, will likely be struck down. As the Court held

> *"…. Under the garb of prevention of money-laundering or black money, there cannot be such a sweeping provision which targets every resident of the country as a suspicious person. Presumption of criminality is treated as disproportionate and arbitrary."*[62]

The necessity standard also requires an analysis of the kind of information collected (biometric data and metadata to facilitate identification); the data minimisation and collection limitation practices adopted; where, how, and how long such information is stored for; the procedures for its deletion; and the effectiveness of the grievance redress mechanism. Courts will also have to evaluate whether the FRT is being deployed covertly or overtly; how the sensitive information is being used and shared; whether there is a likelihood of function creep (such as through integration with other national databases to help create a 360-degree profile of a citizen); and why existing CCTV systems, if any, have been ineffective, necessitating the use of FRT.

Finally, courts will have to consider the source of the database against which a facial recognition search will be conducted, and whether consent was taken before an individual's photo was added to the facial recognition database. For instance, the AFRS proposes to create *"a repository of image/visual database of criminals in the country"*.[63] However, the NCRB does not explain how these "criminals" will be identified or if/when their photographs will be removed. Based on the specific use of FRT, courts will have to analyse these factors to determine whether there is a less invasive, but equally effective, alternative to achieve the stated aim.

[61] *S & Marper* (n 24) [122].

[62] *Aadhaar judgment* (n 13) [491].

[63] National Crime Records Bureau (n 28).

IV. Procedural Guarantees

Kaul J. in *Puttaswamy* focused on the need for procedural guarantees in any law that restricted the right to privacy so as to prevent against arbitrariness in state action.[64]

[64] *Puttaswamy* (n 12) [638] (Kaul J).

Any evaluation of the use FRT for law enforcement purposes will have to consider the transparency in the deployment of FRT by the State and the means of holding it accountable. This can be done through parliamentary oversight (e.g., over the expenditure incurred by the State while deploying the FRT) and/or judicial oversight (e.g. over the prosecution of an individual based on identification through the government's facial recognition software). Citizens must be clearly provided with the technical specifications of the particular FRT being deployed and a clear assessment of the error rates so that a cost benefit analysis can be conducted.[65]

[65] Bedi (n 4).

Second, the State must ensure that there are safeguards against the lack of consent in collecting facial data or having one's photograph being made part of a facial recognition database, such that individual rights are protected. In case of a creation of a national facial recognition database such as AFRS, individual police officers should not have complete discretion in deciding who to place on the database. Instead, their discretion should be regulated through narrowly tailored guidelines.

Third, courts will evaluate the adjudication process, the practice of law enforcement agencies in using FRT, and the ability of an individual to contest an automated decision-making process in court or before a regulatory authority. Courts will also have to assess whether there is any clear Code of Conduct or Standard Operating Procedure ('SOP') that guides the deployment of FRT at a specific location; the extent to which AI systems running facial recognition can be used in investigations; and the extent to which data can be shared between different government agencies.[66]

[66] Smriti Parsheera, 'Adoption and Regulation of Facial Recognition Technologies in India' (2019) DGN Working Paper 05, 59, https://datagovernance.org/report/adoption-and-regulation-of-facial-recognition-technologies-in-india.

Fourth, the use of FRT must be accompanied by an accessible and efficient grievance redress procedure where individuals have a clearly defined right against data theft, unauthorised or negligent disclosure, breach of privacy, or erroneous decision making.
Finally, there must be an assessment of the contextual factors that may affect the performance of the FRT and the procedural guarantees and mitigation measures put in place to deal with the error rate of FRT systems.

D. Way Forward

The use of facial recognition technologies in India is almost entirely unregulated. There are no statutory protections, either from data protection legislation or specific facial recognition codes of conduct or protocols (as in the UK).[67] The only option left for citizens aggrieved by state action is to engage in expensive and time-consuming litigation by approaching the constitutional courts in the country. Remedies against private, corporate use of facial recognition is even more limited, given the documented inadequacies of the Information Technology Act, 2000.[68]

While courts play an important role in protecting our fundamental rights, they are not ideally suited to issue guidelines to govern the varied uses of FRTs across diverse fields, ranging from unlocking an iPhone, to airport passenger screening, to law enforcement and predictive policing. It is the Parliament, the embodiment of deliberative democracy in our country, that has to decide the form and limits of regulation of FRTs across different sectors.

Any law that enables the use of FRT must incorporate the following four elements, in addition to being preceded by meaningful stakeholder consultation: First, it must be accessible, precise, and foreseeable so as to provide certainty about the basis for collecting biometric data; the procedures and time limits for storage of such data; the procedures for deletion; and the disclosure or use of such data by the data fiduciary (whether State or private entity) and by third parties.[69]

[67] Surveillance Camera Commissioner, 'The Police Use of Automated Facial Recognition Technology with Surveillance Camera Systems' (2019) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786392/AFR_police_guidance_of_PoFA_V1_March_2019.pdf. This guidance is produced by the Surveillance Camera Commissioner to assist 'relevant authorities' in complying with their statutory obligations arising from Protection of Freedoms Act 2012, s 31(1) and the Surveillance Camera Code of Practice, when operating surveillance camera systems in public places overtly in England and Wales, including those which make use of FRT.

[68] Vrinda Bhandari and Renuka Sane, 'Towards a Privacy Framework for India in the Age of the Internet' (2016) NIPFP Working Paper No. 179. See also Satya Prakash, 'Information Technology legislation 'falls far short'' (*Tribune India*, 05 January 2020) https://www.tribuneindia.com/news/features/information-technology-legislation-%E2%80%98falls-far-short%E2%80%99-21652; Amlan Mohanty, 'Grievance Officer in the IT Rules – An Invisible Man?' (*Spicy IP*, 10 November 2012) https://spicyip.com/2012/11/guest-post-grievance-officer-in-it.html.

[69] Vrinda Bhandari and Renuka Sane, A Critique of the Aadhaar Legal Framework (2019) 31 NSLIR Review 1-23; *Huvig v France* [1990] 1 EHRR 528; *Kruslin v France*, [1990] 12 EHRR 547.

Second, the use of FRT under the law must be governed by a notice about the privacy practices, choice, and specific opt-in consent. Individuals must be provided information about suitable alternatives and the interlinking of their facial data with other databases, if any. The risks and harms associated with processing such sensitive biometric data must also be carefully explained.[70] Special care has to be taken while collecting or storing children's data.

Third, the law must implement the data protection principles of data minimisation, collection and purpose limitation, storage limitation, privacy by design, transparency, security, and accountability. For instance, purpose limitation requires that the images captured through the use of FRT cannot be combined with any other database so as to create a 360-degree profile of a citizen. In addition, any large-scale deployment of FRT must be preceded by an algorithmic impact assessment, a data protection impact assessment, and periodic data audits.[71] An effective grievance redress and enforcement mechanism must be built so that it is easy for aggrieved individuals to file complaints and hold the concerned state agency or private organisation responsible for any privacy or security violation.[72]

Fourth, the law must build in principles of necessity, proportionality, and procedural guarantees to strictly regulate the use of FRT. It should not adopt the proposed Data Protection Bill, 2019's wide-ranging exemptions granted to government agencies for any law-enforcement related activities, which will undermine the very privacy protections intended to be introduced through the law.[73] Similarly, if FRT is being deployed for law enforcement purpose, it must be accompanied by judicial oversight and courts should be prohibited from admitting evidence that is illegally obtained through a violation of the prescribed legal safeguards.[74]

[70] Yana Weilder (n 18).

[71] AI Now Institute, *AI Now 2018 Report* (2018); Clare Garvie, Alvaro Bedoya and Johnathan Frankle, 'Unregulated Police Face Recognition in America' (*The Perpetual Line-Up*, 18 October, 2016) https://www.perpetuallineup.org/.

[72] Bhandari and Sane (n 67).

[73] Vrinda Bhandari, 'New data bill gives sweeping powers to govt' (*The Telegraph*, 13 December 2019) https://www.telegraphindia.com/opinion/new-data-bill-gives-sweeping-powers-to-govt/cid/1726583.

[74] *Pooran Mal v Director of Inspection (Investigation)* [1974] 1 SCC 345; RM *Malkani v State of Maharashtra* [1973] 1 SCC 471; *Navjot Singh Sandhu v Union of India* [2005] 11 SCC 600.

However, at the moment, I propose a moratorium or prohibition on the use of facial recognition technology, AFRS, and Live Facial Recognition Technology for any law enforcement purpose. Apart from the absence of any governing legal framework that regulates the use of FRT in the manner described above, there are problems associated with the lack of consent and privacy in the deployment of FRT, the documented biases of FRTs and the resulting profiling, as well as the risk of mass surveillance. Incorrect identification by facial recognition systems can lead to wrongful arrests, long periods of pre-trial detention, and consequent loss of liberty and opportunity, given India's low state capacity and delayed justice delivery system.[75] Currently, the police use of FRT is governed by the out-dated position under Indian law where evidence obtained illegally by law enforcement agencies can still be admitted in trial and surveillance can be authorised by the government without judicial oversight; although as I have argued elsewhere, this position does not hold good post-*Puttaswamy*.[76] These factors cumulatively render the use of FRT by law enforcement extremely problematic.

A moratorium is not a radical solution. Rather, it would follow in the footsteps of cities, states, and countries such as Boston, California, and New York; San Francisco, Oregon, and New Hampshire; and Belgium that have banned the use of FRT by the police, or banned the police from using FRT in body cameras.[77] Companies such as Microsoft, Amazon, and IBM have also temporarily decided to halt the sale of their facial recognition systems to police departments across the U.S.[78]

Based on a better understanding of the dangers of facial recognition, an emerging trend is developing in parts of the world that calls for regulations or restrictions on the use of FRT.[79] In India, unfortunately, we seem to moving in the opposite direction – ramping up the use of FRT,

[75] Vrinda Bhandari, Pretrial Detention in India: An Examination of the Causes and Possible Solutions (2016) 11(2) Asian Journal of Criminology. As per the latest figures, National Crime Records Bureau, *Prison Statistics in India 2019* (Ministry of Home Affairs, 2019), the proportion of under trial prisoners is 69.05% of the total prison population.

[76] Vrinda Bhandari and Karan Lahiri, The Surveillance State: Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World, (2020) 3(2) Univ. of Oxford Human Rights Hub Journal 15.

[77] Alex Najibi, 'Racial Discrimination in Face Recognition Technology' (*Harvard University STIN Blog*, 24 October 2020) http://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/; Halsey Samsel, 'California Becomes Third State to Ban Facial Recognition Software in Police Body Cameras' (*Security Today*,08 October 2019) https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx; Elena Nicholas, 'Pandemic speeds calls for ban on facial recognition' (*EUobserver*, 18 May 2020) https://euobserver.com/coronavirus/148387.

[78] Jay Greene, 'Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM' (*Washington Post*, 12 June 2020) https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

[79] In 2019, three biometric bills were proposed by members of the US Congress, including The Commercial Facial Recognition Privacy Act, 2019; The Facial Recognition Technology Warrant Act, 2019; The No Biometric Barriers Act of 2019; AI Now Institute (n 16); 'Peru telcos challenge biometric ID rule' (*BNAmericas*, 02 December 2016) https://www.bnamericas.com/en/news/ict/peru-telcos-challenge-biometric-id-rule/.

without enacting either an anchoring facial recognition legislation or even a data protection law. We need to reclaim our public spaces. Unless corrective measures are undertaken, facial recognition will *normalise* and expand the face of surveillance as we know it in India, and forever imperil our democracy.

The IoT-loaded Smart City and its Democratic Discontents

By Malavika Prasad[1]

A. Introduction

The Smart City Mission ('SCM'), a centrally sponsored scheme launched in 2015, was envisioned as a vehicle to improve quality of life and attract investments for sustainable and inclusive development of the city.[2] Globally, the smart city's earliest definitions revolved around a technology-centric efficient urban management system,[3] capable of branding and marketing itself to invite investment and innovation.[4] Later definitions take a more holistic view of the smart city – as a sustainable, knowledge-based and community-driven urban management system.[5] The SCM Guidelines also lay down similar standards, but do not define the smart city.[6]

Around the same time as the start of the SCM, the Draft Internet of Things ('IOT') policy was also published, in keeping with the Indian government's vision for a smart, "digital India", stating India's aims to promote research and development in the IoT sector. One of the key objectives of the IoT policy is to create an IoT industry in India of USD 15 billion by 2020.[7] This was to be realized, in part, through the domain of the smart city in smart lighting, smart traffic management, smart building, smart health, smart parking, Wi-Fi access, solid waste management, smart metering, water quality, and city surveillance.[8] Other domains included smart water monitoring, smart alarms for CO2 emissions and pollution, smart health monitoring, smart waste management, smart agriculture for precision farming, smart safety for women, children, senior citizens, persons with mental illness or physical disability, smart supply chain and logistics, etc.[9]

An empirical study of successful Smart City Proposals ('SCPs') in India has revealed that a fifth of the total investment in smart cities is directed at smart

[1] The author is a lawyer and Doctoral Candidate at Nalsar University of Law, Hyderabad. She can be reached at malavika.prasad@nalsar.ac.in. The author would like to thank Kritika B for her helpful comments on the draft, and Vidushi Marda in conversation with whom several of these ideas initially took form.

[2] Smart City Mission Statement and Guidelines (Ministry of Urban Development, 2015) para 1.1, 2.3. ("SCM Guidelines").

[3] See for instance the vision for an "instrumented, interconnected, and intelligent" system propounded by IBM. C. Harrison and others, 'Foundations for Smarter Cities' [2010] 54(4) IBM Journal of Research and Development 1-16.

[4] See for a brief literature review on point, Sarbeswar Praharaj, Hoon Han, 'Cutting through the clutter of smart city definitions: A reading into the smart city perceptions in India' [2019] 18 City, Culture and Society 100289.

[5] Ibid.

[6] SCM Guidelines para 2.1-2.2. Two elements are key to the SCM's view of "smart cities" : first, ensuring a "decent quality of life to its citizens" with "core infrastructure", "clean and sustainable environment" and the application of "smart solutions," and second, that no single definition of a smart city can be imposed on a city or a state. Sama Khan, Persis Taraporevala, Marie-Helene Zerah, 'Mission Impossible Defining Indian Smart Cities' [2018] 53 (49) The Economic and Political Weekly 80.

[7] Draft Policy on Internet of Things (Department of Electronics & Information Technology 2015) 5 https://www.meity.gov.in/writereaddata/files/Revised-Draft-IoT-Policy_0.pdf .

[8] Ibid 6-7.

[9] Ibid 7-8.

technological solutions.[10] Of this, smart sanitation, smart transport, energy and water take 15%, 25%, 35% and 40% respectively of the investments.[11] Technological solutions in sanitation, water, transport and energy are envisioned by the SCM to improve infrastructure and services.[12] For this reason, the "smartness" of the city – embodied in its IoT features – is assumed to favour citizen-centric solutions and collaborative and participative governance.[13] In this article, I attempt to interrogate this assumption, through a case study of the Pune smart sanitation project.

Pune ranks as one of India's top smart cities.[14] The Pune smart sanitation project ('PSSP'), the first of its kind in the world, lies at the intersection of the Smart City Mission and the Swachh Bharat Mission – a campaign to improve solid waste management.[15] The PSSP is helmed by the Pune Municipal Corporation in collaboration with the Toilet Board Coalition – a coalition of sanitation businesses. With Dalit women workers being confined to sanitation work and excluded from other occupational opportunities,[16] this effort to smarten sanitation is an instructive case study on the democratic discontents of smart cities.

This article examines the smart city from a constitutional lens, with a particular focus on the IoT solutions being developed and deployed for the PSSP. The central argument is that the Indian smart city, by prioritizing efficiency over self-government, not only fails to meet the structural requirements of democratic city government mandated under the Constitution of India, but can also be exclusionary on caste, class, and gendered lines.

To make this argument, I draw from the work of public policy and public administration scholars and build on a case study of the smart sanitation solution deployed in the PSSP.[17] While I am mindful that a single "canonical example" without fieldwork on cities' smart solutions

[10] Persis Taraporevala, 'Demystifying the Indian smart city: An Empirical reading of the smart cities mission' [2018] Center for Policy Research Working Papers, https://www.cprindia.org/research/papers/demystifying-indian-smart-city-empirical-reading-smart-cities-mission.

[11] Sama Khan and others (n 5) 85.

[12] SCM Guidelines paras 2.4- 2.6.

[13] KPMG, 'Internet of Things in Smart Cities' (2019) 11, https://assets.kpmg/content/dam/kpmg/in/pdf/2019/05/urban-transformation-smart-cities-iot.pdf.

[14] 'Pune Smart City improves its ranking to 13th in country' (*The Indian Express*, 17 October 2020) https://indianexpress.com/article/cities/pune/pune-smart-city-improves-its-ranking-to-13th-in-country-6758157/.

[15] 'PMC partners with TBC to become 'Smart Sanitation City'' (*The Indian Express*, 1 September 2017) https://indianexpress.com/article/india/pmc-partners-with-tbc-to-become-smart-sanitation-city-4823309/.

[16] In the words of B R Ambedkar: "... it is clear that according to the Hindu Shastras and the Hindu notions, even if a Brahmin did scavenging, he would never be subject to the disabilities of one who is born a scavenger. In India, a man is not a scavenger because of his work. He is a scavenger because of his birth irrespective of the question whether he does scavenging or not." See B R Ambedkar, *What Congress and Gandhi have Done to the Untouchables* (Thacker and Co. Bombay 1945) 303-4.

[17] Malavika Prasad and Vidushi Marda, 'Interrogating "smartness": A case study on the caste and gender blind spots of the smart sanitation project in Pune, India' in Alan Finlay (ed), *Global Information Society Watch 2019*, (Association for Progressive Communications 2019) 145-151 ("the Report").

cannot lead to a one-size fits all narrative on the democratic deficit of smart cities,[18] my hope is for this article to trigger further questions and research on IoT in smart cities against the existing constitutional framework for city governance.

[18] See Rob Kitchin, 'Making sense of smart cities: addressing present shortcomings' [2015] 8(1) Cambridge Journal of Regions, Economy and Society 131-136.

B. The Self-Government Deficit in City Government

The constitutional mandate for self-governance in villages and cities was introduced in the Indian Constitution by the 73rd and 74th amendments in 1992 respectively. Prior to these amendments, the structure of city governments was laid down by state legislatures – if at all – in exercise of their power over "local government... and other local authorities for the purpose of local self-government..."[19] Thus, although city governments were elected, their executive powers were vested in unelected bureaucrats[20] or distributed such that the power was ultimately exercisable by "the State Government through a Minister in charge of municipalities...with his veto power".[21] This executive authority has effectively hollowed out electoral accountability.

[19] Constitution of India, art 245 read with Entry 5, List II, Seventh Schedule ("COI"): Local government, that is to say, the constitution and powers of municipal corporations, improvement trusts, districts boards, mining settlement authorities and other local authorities for the purpose of local self-government or village administration

[20] See on this question, *Lok Sabha Debates* 1 December 1992, speech of Kashiram Rana 733.

[21] *Lok Sabha Debates* 1 December 1992, speech of Pawan Kumar Bansal 743.

After the 74th amendment, municipalities were constitutionally required to be institutions of "self-government", elected by popular vote. Three parameters are laid down for the structure of municipal government in the Constitution itself. The first structural parameter is that the "Municipality" will be an "*institution of self-government*..."[22] To that end, municipal governments are to be elected from municipal areas that are subdivided into territorial constituencies or "wards,"[23] and the legal relationship between citizen and State is one of "self-government."[24] Even the powers and authority that state legislatures may endow on Municipalities are those that "may be necessary to enable them to function as institutions of self-government."[25]Therefore, the entire apparatus of the 74th amendment is towards enabling the Municipality to function as an institution of self-government.

[22] COI, art 243-P(e): "(e) Municipality means an institution of self-government constituted under Article 243Q."

[23] COI, art 243-R(1).

[24] Establishing democratically governed municipalities was one of the chief objectives of the 74th amendment to the Indian Constitution. See *Lok Sabha Debates* 1 December 1992 speech of Kashiram Rana 732-733; speech of Pawan Kumar Bansal 747-748; Report of the Joint Parliamentary The Constitution (Seventy-Third) Amendment Bill, 1991 (Insertion of New Part IXA and Addition of Twelfth Schedule) Committee 14 July 1992 paras 1.34-36.

[25] COI, art 243W.

The second is that the Municipality shall be a politically representative institution of city government.[26] Representation of Dalits and Scheduled Tribes is guaranteed through seats reserved in proportion to the populations of the respective communities within the municipal areas.[27] A third of the seats reserved for the two communities are to be reserved for women candidates from those communities,[28] and a third of the total number of seats (including those reserved for women who identify as Dalit and Scheduled Tribes) are reserved for women generally, with each of the seats being allotted by rotation to various constituencies.[29]

The final structural parameter is the term of the Municipality.[30] To the extent that "processes that produce character development, deliberation, reflection, and consent…" all unfold over time on a stipulated schedule,[31] the fixed term of the Municipality is the period for which it is assumed to hold democratic mandate. Thus, the fixed term of five years ensures accountability of the Municipality to its constituents.

However, the Constitution states that the State legislature *"may, by law"* provide for the representation of various persons in Municipalities.[32] In the same vein, although the functions that may be assigned to Municipalities is constitutionally stipulated in the Twelfth Schedule,[33] the Constitution states that State legislatures "*may, by law"* endow powers and authority on municipal governments that are "*necessary to enable them to function as institutions of self-government…"*[34] If such a law were to be enacted, the law is not required to assign any powers and authority on the municipal government; rather, such law *"may contain provisions for the devolution of powers and responsibilities…"* upon the Municipality.[35] Likewise, the State "may" by law authorise the municipal government to levy, collect and appropriate taxes,[36] and it "may", by law, assign to Municipalities, taxes, duties etc., make grants in aid to

[26] Representation of Dalits and Scheduled Tribes is guaranteed through seats reserved in proportion to the populations of the respective communities within the municipal areas. COI, art 243-T stipulates the constitution of Municipalities in respect of representation. A third of the seats reserved for the two communities are to be reserved for women candidates from those communities per COI, art 243-T(2) and a third of the total number of seats (including those reserved for women who identify as Dalit and Scheduled Tribes) are reserved for women generally, with each of the seats being allotted by rotation to various constituencies per COI, art 243-T(3).

[27] COI, art 243-T stipulates the constitution of Municipalities in respect of representation.

[28] COI, art 243-T(2).

[29] COI, art 243-T(3).

[30] COI, art 243-U stipulates that the maximum term of a municipal government is five years, subject to its prior dissolution per the law of the state.

[31] Elizabeth Cohen, *The Political Value of Time Citizenship Duration and Democratic Justice* (Cambridge University Press 2018) 66.

[32] COI, art 243-R(2).

[33] COI, art 243W(a)(i).

[34] COI, art 243-W(a). Concerns were expressed by some framers, that the amendments do not confer powers and responsibilities on such authorities, or mandate functions for them to discharge. See *Lok Sabha Debates* 2 December 1992 speech of V Dhananjaya Kumar 734-735.

[35] COI, art 243-W(a).

[36] COI, art 243-X(a). See also objections to the proposal raised by the framers of this amendment in *Lok Sabha Debates* 1 December 1992, speech of Kashiram Rana, 737-742; speech of Anil Basu, 757-760; *Lok Sabha Debates* 2 December 1992 speech of Debi Prosad Pal, 691-694; *Lok Sabha Debates* 4 December 1992 speech of Shobanadreeswara Rao Vadde, 639-640; speech of Laeta Umbrey, 641-2.

Municipalities, and create funds collected by or on behalf of Municipalities and allow withdrawals f rom them.[37]

State legislatures take these provisions to imply a plenary power to decide the composition, powers, functions, and even finances of the Municipality. They continue to exercise their legislative power to constitute Municipalities over which they retain administrative oversight, by vesting executive power in the Commissioner, an unelected, bureaucratic head.[38] They also use their legislative power to not only deprive Municipalities of financial autonomy, but also control their financial capacities. Consequently, far from being financially self-sufficient, Municipalities are "among the weakest, globally, in terms of fiscal capacity and autonomy," wholly due to State recalcitrance.[39] "While State Finance Commissions were created to safeguard against a mismatch between the revenue and expenses of municipalities,[40] many states have failed to equip their Finance Commissions to discharge these functions.[41]

Furthermore, states have also used their legislative powers to constitute unelected, unrepresentative, permanent parastatal bodies at the city and state level.[42] The reasons for doing so ranged from the need for a single point authority, for "co-ordinated development" where two or more municipal functions vested in different bodies,[43] and for independence and autonomy from government and its inefficiencies, where the funding agency required it,[44] particularly for large-scale infrastructural works.[45] Consequently, parastatal bodies carried out "development and capital works", while Municipalities were left with "operation and maintenance of services".[46]

These authorities were either constituted under state law[47] or as government corporations,[48] and comprise members from the permanent and political executive. Being entrusted with functions that are constitutionally

[37] COI, art 243X(b)-(c).

[38] Mathew Idiculla, 'Unpacking Local Self Government' 53(1) Verfassung und Recht in Übersee 30, 46. See Karnataka Municipal Corporations Act, 1976, ss 64, 95, 96.

[39] No major central or state tax is shared with municipalities in India". See COI, arts 268 – 275 for the divisible pool of tax resources between the Center and States. P K Mohanty, *Financing Cities in India: Municipal Reforms, Fiscal Accountability and Urban Infrastructure* (SAGE Publications India 2016) Chapter 7. There is in fact no "divisible pool of tax resources" between the state and municipalities (unlike between the Centre and states).

[40] SFC are to lay down the basis for devolution of state funds to the Municipality, determine the funds that Municipalities may themselves raise, and advice the Central Finance Commission on augmenting the state's exchequer to supplement the municipalities' resources. See COI, art 243-I read with art 243-Y; COI, art 280(3)(c).

[41] M A Oommen, 'Have the State Finance Commissions Fulfilled Their Constitutional Mandates' [2010] 45(30) The Economic and Political Weekly 39-44.

[42] For instance, the Bangalore Metropolitan Transport Corporation is a wholly owned corporation of the State Government constituted by the Road Transport Corporation Act, 1950 in 1997, while the Bengaluru Metro Rail Corporation Limited was incorporated under the Companies Act, 1956 as a joint venture between the Central and state government in 2011.

[43] See the Statement of Objects and Reasons, Bangalore Development Authority Act, 1976. Act 12 of 1976. http://dpal.kar.nic.in/pdf_files/12%20of%201976%20%28E%29.pdf; See the Statement of Objects and Reasons, Bangalore Water Supply and Sewerage Act, 1964. Act 36 of 1964, http://dpal.kar.nic.in/.%5C36%20of%201964%20(E).pdf.

[44] See the Statement of Objects and Reasons, Bangalore Water Supply and Sewerage Act, 1964. Act 36 of 1964. http://dpal.kar.nic.in/.%5C36%20of%201964%20(E).pdf.

[45] Mathew Idiculla, 'Who Governs the City? The Powerlessness of City Governments and the Transformation of Governance in Bangalore' presented at the RC21 International Conference on "The Ideal City: between myth and reality. Representations, policies, contradictions and challenges for tomorrow's urban life" Urbino (Italy) 27-29 August 2015 14, https://www.rc21.org/en/wp-content/uploads/2014/12/G5.2-Idiculla.pdf.pdf.

[46] Om Prakash Mathur, 'Governing Cities: Facing up to the Challenges of Poverty and Globalization' 17 in Om Prakash Mathur (ed.), *India: The challenge of urban governance* (National Institute of Public Finance and Policy 1999); Solomon Benjamin, 'Governance,

envisioned for municipalities,[49] parastatal bodies undertake planning consistent with the interests of those with social and economic capital, having connections to the bureaucrat and political classes.[50] Consequently, state political parties are able to "subvert local political opposition" (that they would otherwise face in democratically elected Municipalities[51]) by carrying out works through parastatal bodies. Poor groups are left to negotiate with the elected Municipality through "class, caste and bureaucratic alliances", using their social connections with lower level bureaucrats and municipality officials.[52] Further, funding on the terms of international agencies[53] and private investment[54] is received for infrastructure projects.[55]

State legislatures have been afforded such a wide latitude because courts have engaged in solely literal readings of the text of the Constitution.[56] Since State legislatures have a power to legislate on local governments coupled with a discretion to enact laws constituting them, the reasoning goes, that the *Court cannot direct the legislature* to exercise its powers in any particular manner.[57] Likewise, in the case of parastatal bodies, the Court has approved their creation holding that they are not – and indeed do not purport to be – Municipalities,[58] and thus need not adhere to the constitutional framework for city governance.[59] Thus, courts neglect to consider the text in context of the structure of municipal government laid down.

A structural interpretation of the Constitution's provisions on city government indicate that self-government, political representativeness, and the term length together realise the constitutional principle of democratic self-governance. It is well understood that the structure of government and its relationship with citizens, as gleaned from constitutional text, can lend itself to inferences about constitutional principles. [60] Although smaller benches and minority opinions have taken such a structural approach to interpret the constitutional text on Municipalities,[61] it is yet to become the law of the land.

economic settings and poverty in Bangalore' [2000] 12(1) Environment & Urbanization 35-56, 51.

[47] For instance, the Bangalore Development Authority and the Bangalore Water Supply and Sewerage Board were constituted by the Bangalore Development Authority Act, 1976 and the Bangalore Water Supply and Sewerage Board Act, 1964.

[48] For instance, the Karnataka Urban Infrastructure Development and Finance Corporation was incorporated as a public company under the Companies Act, 1956, in November 1993 just a few months after the 74th amendment came into force (in June).

[49] Mathew Idiculla (n 37) 47.

[50] Solomon Benjamin (n 45) 45-46.

[51] Ibid.

[52] Ibid 54-56.

[53] Mathew Idiculla (n 44) 16.

[54] See Mathew Idiculla (n 44) 17-18; Vinay Baindur and Lalitha Kamath, 'Reengineering Urban Infrastructure: How the World Bank and Asian Development Bank Shape Urban infrastructure Finance and Governance in India' (Bank Information Center 2009). Ultimately, however, public grants dominantly funded both the JNNURM and the SCM programs. Ashwathy Anand, Ajai Sreevatsan and Persis Taraporevala, 'An Overview of the Smart Cities Mission in India' (Centre for Policy Research, New Delhi 2018) 6, https://cprindia.org/system/tdf/policy-briefs/SCM%20POLICY%20BRIEF%2028th%20Aug.pdf?file=1%26type=node%26id=7162.

[55] Thus, financial institutions were set up by states to act as intermediaries for channelling these funds towards the projects. Karnataka Urban Infrastructure Development and Finance Corporation was set up in 1991, for instance, to act as an intermediary to receive funds for the construction of ring roads, flyovers, promote four new satellite cities to decongest Bangalore. See Solomon Benjamin (n 45) 35-56, 37-38.

[56] *Charan Singh v. State of Maharashtra* (2012) 4 Bom CR 40; *Bondu Ramaswamy v Bangalore Development Authority* (2010) 7 SCC 129; *Bhim Singh v Union of India*, (2010) 5 SCC 538; *Shanti G Patel v State of Maharashtra*, (2006) 2 SCC 505; *Ranga Reddy District Sarpanches Assn v Government of AP*, 2004 (1) ALT 659; *Forum for a Better Hyderabad v Government of Andhra Pradesh*, 2002 (4) ALD 84 (DB).

[57] *Ranga Reddy District Sarpanches' Association* (n 55) para 20.

[58] *Bondu Ramaswamy* (n 55) para 20-24.

[59] Parastatal bodies are better placed than self-governing ULBs to "fulfil the requirements of a specialist agency executing development schemes...", the

Court reasoned. What required "self-government" was "overall development" under the Twelfth Schedule including the "...plans for economic and social justice, planning for economic and social development, slum improvement and upgradation, urban poverty alleviation, and providing several urban amenities and facilities...." *Bondu Ramaswamy* (n 55) paras 25-27.

With Municipalities answering to State governments rather than their own electorates, and permanent parastatal bodies performing functions reserved for Municipalities, the Indian landscape for city governance fails to realise democratic self-government under the 74th amendment. In short, city governance was already in democratic deficit before the SCM.

C. The Smart City Aggravation

Atop this framework of city governance was laid the smart city. The SCM is to be implemented, not through the Municipality, but through a "Special Purpose Vehicle" ('SPV')—a limited company incorporated under the Companies Act, 2013,[62] whose board comprises nominees of the Central Government, State Government and the city government.[63] The State and the Municipality are to hold shares in the SPV in equal parts, and jointly ought to hold a majority stake in the SPV.[64] Given their financial capacities, Municipalities are permitted to use Central Government's grants under the SCM as their equity contribution to the SPV.[65] As a result, while the SCM compels states to disburse funds (by mandating that they match the shareholding of the Municipality in the SPV), it condones states depriving Municipalities of financial autonomy and capacity (by permitting the latter to use Central grants towards their own shareholding in the SPV).

The structure of the SPV as an incorporated company combined with the lack of functional and financial autonomy in Municipalities, as shown in Section 1, together ensure that the SPV is incapable of even a modicum of democratic self-governance. Even the SCM does not expect SPVs to engage in self-governance. For instance, the only role envisioned for the Municipality is to ensure (along with the State) that the smart city has "*a dedicated and substantial revenue stream*", is capable of sustaining itself and raising more funds in the market, while also ensuring that the government's funds are used "*only to create infrastructure that has public benefit*

[60] Charles L Black, *Structure and Relationship in Constitutional Law* (Louisiana State University Press 1969).

[61] See dissent of Goda Raghuram, J. in *Ranga Reddy District Sarpanches' Association* (n 55); *Rajendra Shankar Shukla v State of Chattisgarh and Ors.* (2015) 10 SCC 400.

[62] SCM Guidelines para 10.2.

[63] Ibid.

[64] SCM Guidelines para 10.2 Annexure 5.

[65] SCM Guidelines Annexure 5.

outcomes.[66] Furthermore, SPVs are permitted to appoint "Project Management Consultants" from a list of vetted consulting firms and handholding agencies, for "designing, developing, managing and implementing" smart city projects.[67] Thus, smart cities were planned under the stewardship of management consultants, with limited public participation, and a total neglect of "municipal capacity-building."[68]

The SCM defends the SPV as necessary for "operational independence and autonomy in decision making and mission implementation."[69] But this is precisely the import of "self-governance" entrusted to elected Municipalities under the Constitution of India. Yet, the SCM requires the Municipality to delegate its rights and obligations in respect of smart city projects to the SPV, and its executive authority to the CEO of the SPV.[70] Effectively, the SCM commands a handover of all rights, obligations and powers of Municipalities to the SPV without guaranteeing any electoral accountability from SPVs.[71]

It is not clear what about the governance of a smart city was thought to merit a departure from the constitutional framework for city governance on the principle of democratic self-government. The purpose of this SPV is to "plan, appraise, approve, release funds, implement, manage, operate, monitor and evaluate the Smart City development projects".[72] Of these functions of SPVs, it is unclear how the "planning" function is different from the planning function of the Municipality at the level of the city,[73] and of the "District Planning Committee"[74] ('DPC') and "Metropolitan Planning Committee"[75] ('MPC'), at the level of the district and metropolitan area under the Constitution. Indeed, the DPC and MPC are entrusted with "co-ordinated spatial planning of the area, sharing of water and other physical and natural resources, the integrated development of infrastructure and environmental conservation" and all other matters

[66] Ibid.

[67] SCM Guidelines para 10.6.

[68] Sama Khan and others (n 5) 84.

[69] SCM Guidelines para 4.1 Annexure 5,

[70] SCM Guidelines para 4.1.1-2 Annexure 5.

[71] Indeed, the SPV, being a company and not an elected unit of government, is structurally incapable of embodying subsidiarity, self-government, political representativeness and term limits.

[72] SCM Guidelines para 10.1; SCM Guidelines, para 5, Annexure 5 which are to be included in the Articles of Association of the SPV.

[73] COI, art 243W(a)(i) and Twelfth Schedule.

[74] See COI, art 243-ZD.

[75] See COI, art 243-ZE.

of common interest between Municipalities in cities and Panchayats in rural areas.[76] Likewise, it is unclear how the remaining functions of the SPV, especially of implementation, management, operation and monitoring of projects, differ from the functions entrusted to Municipalities under the Constitution, viz. performance of Twelfth Schedule functions and the "implementation of schemes in relation to the Twelfth Schedule".[77]

[76] COI, arts 243ZD(3) and 243ZE(3).

[77] COI, art 243W(a)(ii).

Moreover, the SCM itself does not lay down any special prerequisites for a city to qualify as smart,[78] over and above a regular city. The "*core infrastructure elements*" for smart cities laid down in the SCM are worth examining. They are "i. adequate water supply, ii. assured electricity supply, iii. sanitation, including solid waste management iv. efficient urban mobility and public transport v. affordable housing, especially for the poor, vi. robust IT connectivity and digitalization, vii. good governance, especially e-Governance and citizen participation, viii. sustainable environment, ix. safety and security of citizens, particularly women, children and the elderly, and x. health and education."[79] These requirements are in the nature of standards, not rules,[80] and thus do not offer useful definitional boundaries or particular prerequisites for a city to qualify as "smart". Moreover, they are merely standards for improving urban infrastructure and governance, all but one of which are already laid down as functions of Municipalities in the Constitution of India.[81]

[78] Sama Khan and others (n 5) 80.

[79] SCM Guidelines para 2.4.

[80] See Pierre J. Schlag, 'Rules and Standards' [1985] 33 UCLA L. Rev 379 for a review of the distinction between the two in legal theory and practice.

[81] See art 243W read with the Twelfth Schedule, COI.

The following "smart" features are recommended for SCPs to qualify under the SCM:

> *6.2 Essential features of SCP : It may be noted that even though a particular model is not being prescribed, it is expected that the SCPs will include a large number of infrastructure services and smart solutions highlighted in paras 2.4 and 2.5. In particular, the elements that must form part of a SCP are assured electricity supply*

with at least 10% of the Smart City's energy requirement coming from solar, adequate water supply including waste water recycling and storm water reuse, sanitation including solid waste management, rain water harvesting, smart metering, robust IT connectivity and digitalization, pedestrian friendly pathways, encouragement to non-motorised transport (e.g. walking and cycling), intelligent traffic management, non-vehicle streets/zones, smart parking, energy efficient street lighting, innovative use of open spaces, visible improvement in the Area (e.g. replacing overhead electric wiring with underground wiring, encroachment-free public areas, and ensuring safety of citizens especially children, women and elderly). Cities will have to add more 'smart' applications to this list in order to improve their SCP ...It must be emphasized that, since cities are competing with each other for selection under the Smart Cities Mission, the SCPs have to be prepared with great care and the proposed Smart City made 'smart' enough."

However, an empirical examination of winning SCPs finds that the Indian smart city remains heavily committed to improving public services, not unlike prior urban renewal missions.[82] Thus, a bulk of smart city investments was made towards transport, energy, water, sanitation, and housing.[83] In the absence of any rules mandating special requirements for a city to qualify as "smart", the requirement that the SCM be implemented through an SPV and not through the Municipality begs the question.

The empirical study of successful SCPs has revealed the unstated objective of SPVs is to move towards increased efficiency through "corporate methods of functioning,"[84] to be realized along three axes. First, a stable leadership and institutional memory through the permanent office of the CEO; second, collaborative work replacing the silos of departmental functioning in municipal government; and third, financial credibility by way of

[82] Persis Taraporevala (n 9) 2; See also, Russel M Smith and others, 'India's 'Smart' Cities Mission: A Preliminary Examination into India's Newest Urban Development Policy' [2019] 41(4) Journal of Urban Affairs 518-534. 52.5% of all projects in smart cities were for basic urban infrastructure ranging form the delivery of water, sewer, electricity, roads etc. 12.2% of projects were devoted to public health and safety. On the contrary, the smart city globally was devoted to deploying data-based technologies for efficient urban management. See Yirang Lim and others, 'Identifying the results of smart city development: Findings from systematic literature review' (2019) 95 Cities 102397.

[83] Persis Taraporevala (n 9) 18.

[84] Persis Taraporevala (n 9) 10.

[85] Persis Taraporevala (n 9) 20.

access to the debt market.[85] However, these supposed virtues of SPVs are afforded only by derogating from constitutionally mandated requirements for the structure of city government – such as electoral accountability enforced through term limits, political representativeness and self-government. In other words, the absence of democratic self-government in the SPV's structure and relationship to citizens is a feature and not a bug of the SCM.

Atop this framework of smart cities is laid the IoT based layer of technological solutions.

D. The Pune Case Study : A "The Democracy of Consumers"?

[86] Toilet Board Coalition India Roundtable, 15 November 2017, https://www.youtube.com/watch?v=VUKB1WDJBjQ.

The case study of the PSSP revealed that its goal is to reduce the cost of providing sanitation by tapping into a nascent market of healthcare and allied sanitation services.[86] It proposes to do this through three mutually reinforcing economies. The first is the Smart Sanitation Economy comprising businesses that digitize sanitation systems to "optimise data for operating efficiencies, maintenance" while deriving "consumer use and health information insights". The second is the Toilet Economy comprising businesses innovating in toilet products and services. The last is the Circular Sanitation Economy comprising businesses capturing toilet resources like human waste to recover "nutrients and water, creating value-adding products such as renewable energy, organic fertilisers, proteins".[87]

[87] Toilet Board Coalition, 'The Sanitation Economy in India, Market Estimates and Insights November' [2017] https://www.toiletboard.org/media/35-The_Sanitation_Economy_in_India.pdf.

[88] See the Report 148-150.

In the PSSP case study, three findings were key.[88] First, sensors (at toilets to capture footfall, in toilets to detect pathogens and other health data, and in treatment plants to capture flow and quality of toilet resources)are being deployed in the PSSP for "the collection of new data, feeding new insights, and creating Sanitation Intelligence". Second, the data collected by these sensors will be transferred to a one-stop control center for their assimilation and analytics to facilitate data-driven decision-making. Third, two kinds of intelligence are predicted to follow from such data: at the city level, for the Municipality to adjust stockage and improve toilet maintenance, and at the business level,

for the toilet-operating businesses to optimize service levels and improve consumer communication.

These findings reveal that the PSSP is interested in capturing data only on one component of human experience - *usage*. Assimilation and analysis of data of only citizen-consumers by design excludes the data of citizen-labourers and citizens in other capacities. Since sanitation workers[89] in India are largely Dalit women,[90] the resulting datasets will be unrepresentative.

Further, insights drawn from and decisions made based on the data will embed the caste, class, and gender based exclusions inherent in the dataset. Take the specific instance of smart toilets in the PSSP. Sensors in these toilets are designed to capture data on the "operational status of toilets", to "trigger" maintenance and cleaning[91] and "optimize service levels."[92] This data will drive decisions to realise the larger vision of the PSSP - to "ensure optimised operations, maintenance and hygiene, keeping toilets clean, safe, healthy and ready to use."[93] Since maintenance and cleaning will continue to be done by sanitation workers, this data will be used to manage and discipline their movement and work.[94] Thus, we may reasonably conclude that decisions based on this data will bear down on the sanitation workers without obtaining any data regarding their labour conditions, contexts and experiences in servicing and maintaining the smart toilets.

The solution, however, does not lie in making datasets representative alone. Datasets – even if representative - are used to drive decisions to realise the predetermined end[95] of the PSSP - improved efficiency. It is unclear how data will be analyzed to conclude that an improvement in efficiency is called for, who decides how to carry out the improvement, and whether such an outcome will come at the cost of the conditions of labour of citizen-sanitation workers. Efficiency is hardly a neutral objective. As Ben Green argues, what is efficient is political.[96] For instance, *why* someone chose not to use a

[89] Sanitation work refers to all cleaning work from sweeping streets, collecting and transporting garbage to cleaning sewers. Their work is marked by precarity, being hired on contract (even despite Supreme Court orders to the contrary) through a contractor and thus outside the purview of labour laws that govern permanent employment and resulting benefits. See Order dated 07 April 2017 in *Municipal Corporation of Greater Mumbai v Kachara Vahtuk Shramik Sangh*, Civil Appeal no 4929/2017 (SLP (C) no. 6202/2017). "Manual scavenging" is one form of sanitation work that is forbidden in India – whether on contract or through employment. Under the Prohibition of Employment as Manual Scavengers and their Rehabilitation Act, 2013, "manual scavenging" is defined as the manual "cleaning, carrying, disposing of, or otherwise handling in any manner, human excreta" in any insanitary latrine, open drain, pit, railway track or other space notified by the Central/State Government. However, the prohibition on hiring labourers for manual scavenging does not apply if protective gear is provided. See ss 2(g) and 5 of the Act. As we note in the Report, it goes without saying that "protective gear does not eliminate the stigma associated with manual scavenging or cleaning labour, which continues to be the only occupational opportunity available to 1.3 million Dalits in India."

[90] See Hemangi Kadlak and others, 'Intersectionality of Caste, Gender and Occupation: A Study of *Safai Karmachari* Women in Maharashtra.' [2019] 11(2) Contemporary Voice of Dalit 132-138.

[91] Toilet Board Coalition, 'Smart Sanitation City, A Thought Piece from the Toilet Board Coalition in Partnership with the Pune Municipal Corporation and Pune Smart City, India' [2018] 11, https://www.toiletboard.org/media/45-TBC_2018PuneReport_11202018.pdf?v=1.0.1.

[92] Ibid 13.

[93] Ibid 17.

[94] Thus, all parties who can access the city level and business level intelligence - including the toilet operator, the toilet business, the contractor, the governing SPV and the Municipality – will now have a share in the dispersed power to manage and discipline workers. This may even lend itself to a perennial surveillance of sanitation workers contracted for cleaning and maintenance of toilets. See the Report 149.

[95] Eric Gordon and Stephen Walter argue that civic technology extracts the labour of individual citizens to generate data for servicing the system on its terms to improve the efficiency of the system for predetermined political ends. In contrast, the PSSP marshals data on citizens' use patterns (and not their individual labour) towards improving the efficiency of predetermined systems. Yet, Gordon and Water's critique holds as I go on to show in the subsequent part of this section. See Eric Gordon and Stephen

smart toilet, access needs for those who were faced with a barrier to entering the toilet and such other data will not be collected by the PSSP. Answers to questions like "what should be made efficient?", "who gets to decide?", and "by what means should efficiency be attained?" indicate the priorities of a society.[97] What may be efficient need not necessarily make cities more inclusive and participatory, or even improve governance.[98]

It may be tempting to argue that efficiency is the very determinant for the principle of subsidiarity, at least on its economic theory foundations.[99] That is to say, whether the city can provide a public service is determined by whether it can do so efficiently – by keeping its externalities to a minimum.[100] However, the measure of efficiency is a political question. In the words of Yishai Blank:

> *"...what constitutes "efficient" management of immigration or climate change is a profound question, and the power to set the parameters for measuring it is what the principle of subsidiarity is actually trying to decide. For subsidiarity to be able to scientifically balance the advantages of smallness with the requirements of economic integration, there needs to be a scientific answer determining which externalities need to be internalized (and which should be ignored), the costs of each activity, and other political questions. In other words, in the most important cases, subsidiarity does not provide the answer to the basic political dilemma: who should decide what?"*[101]

Moreover, prioritising efficiency can mask "political decisions as objective, technical ones."[102] For instance, the casteism inherent in the Swachh Bharat Mission[103] is occluded entirely by the pursuit of efficiency in the PSSP. This teaches that technological solutions cannot solve social problems.

Walter, Meaningful Inefficiencies: Resisting the Logic of Technological Efficiency in the Design of Civic Systems in Imar de Vries and others (eds.), *The Playful Citizen*, (Amsterdam University Press 2019) 318-19, https://www.degruyter.tools/document/doi/10.1515/9789048535200-019/html.

[96] Ben Green, *The Smart Enough City*, (MIT Press 2019) Chapter 2, 17, https://smartenoughcity.mitpress.mit.edu/pub/8dthlkrx/release/1.

[97] Ibid.

[98] Ibid Chapter 3, 12-13, https://smartenoughcity.mitpress.mit.edu/pub/d90vaiya/release/1.

[99] The origins of subsidiarity are broadly located in economic theory and, perhaps counterintuitively, in social theory. In economic theory, the level of government that offers a public service is that level of government that can fully absorb the externalities (or indirect benefits and costs) of its provision. On the other hand, the social theory foundations of subsidiarity sets store by the unique capacity and purpose of social associations to service individual human well-being. It requires that functions be assigned to that unit of social association that is distinctly suited to contribute to the common good, in its "nature and essence", or its capacity, ability and potential. In their philosophical origins, these social associations can range from the parish, household, workplace, or NGO to the city, or state. In its Catholic articulation, each social association should be permitted to make its contribution without intervention from other associations – thus rendering this interpretation of subsidiarity contrary to contemporary legal and political understandings. Yishai Blank, 'Federalism, Subsidiarity, and the Role of Local Governments in an Age of Global Multilevel Governance' [2010] 37 Fordham Urb. L.J. 509, 540- 3; Otfried Höffe, 'Subsidiarity as a principle in the philosophy of government' [1996] 6(3) Regional & Federal Studies, 56-73, 58-67.

[100] The Twelfth Schedule of the Constitution of India, which lays down functions that may be vested in the Municipality, broadly coheres with the economic logic of subsidiarity along three categories. See COI, art 243W read with the Twelfth Schedule; See also Table 2.5, Typology of 12th Schedule Municipal Functions in P K Mohanty (n 38) Chapter 2. "Essentially municipal functions" are for the(contd) provision of those public services whose externalities can be totally absorbed by the governing municipality. They include urban planning and town-planning, regulation of land use and construction of buildings, public health, sanitation conservancy and solid waste management, provision of urban amenities and facilities such as parks, gardens, playgrounds, public amenities including street lighting, parking lots, bus stops and public conveniences, burials and burial grounds; cremations, cremation grounds and electric crematoriums, regulation of slaughter houses and tanneries, cattle pounds; prevention of cruelty to animals, and vital statistics including registration of births and

deaths." Agency functions" are for the provision of those public services whose planning, funding and regulation are done by higher levels of government, but whose implementation is done by the municipality, acting as the agent of a higher level of government, for considerations of efficient management. They include broadly redistributive Schedule functions such as safeguarding the interests of weaker sections of society, including the handicapped and mentally retarded, slum improvement and upgradation, urban poverty alleviation. Finally, "shared functions" are for the provision of those public services whose execution requires a partnership between higher levels of government and the municipality, reckoning with "benefit spillovers, scale economies, need for resource pooling, and promotion of national interest. They include preparation of plans for "economic development and social justice", roads and bridges, water supply for domestic, industrial and commercial purposes, fire services, urban forestry, protection of the environment and promotion of ecological aspects, promotion of cultural, educational and aesthetic aspects.

[101] Yishai Blank (n 98) 537.

[102] Ben Green (n 95) Chapter 2 20-21.

[103] "Eradication of manual scavenging" was stated as a policy imperative in the Swacch Bharat Mission guidelines. However, no details on how or by when this would be done were forthcoming. In 2017, the Revised Guidelines for SBM (Urban), 2017 make cursory protections (such as the upgrading of insanitary toilets to sanitary toilets) for manual scavengers. Likewise, the Revised Guidelines for SBM (Gramin), 2017 merely forbid the construction of insanitary latrines and mandate conversion of existing ones to sanitary latrines. See also Updated Guidelines for SBM (Gramin), 2019. However, the Mission has nothing to say on the varieties of sanitation work outside manual scavenging. See Anand Teltumbde, 'No Swacch Bharat Without Annihilation of Caste' [2014] 49(45) Economic and Political Weekly 11-12; Subhash Gatade, 'Silencing Caste, Sanitising Oppression Understanding Swachh Bharat Abhiyan' [2015] 50 (44) Economic and Political Weekly.

[104] Ben Green (n 95) Chapter 2 18.

What ought to be done instead is that political priorities be first laid down through a democratic and inclusive process. Technological solutions to facilitate their realization must be designed only thereafter.[104] To do so, elected governments must set the political agenda at the level of the city, and technological solutions must be innovated – even if at the hands of private players – only towards achieving them. A more inclusive PSSP would steer citizens into collectively improving the *design* of the system itself, towards the ends of their choosing, instead of reducing them into components of an efficiency enhancing system.[105] While the PSSP compels citizens to sustain the power structure of caste, gender and labour, a more inclusively planned system carries the potential of allowing citizens to reshape power structures.[106]

No doubt any 'agency' or 'instrumentality' of the State, including the SPV governing the Pune Smart City, is to be held to the standards of just, fair and reasonable state action encoded in Part III of the Constitution of India.[107] However, that is beside the point. External limits on the power of a state agency (in the form of Part III's fundamental rights) cannot substitute the need for internal limits (in this case, prescribed in the Twelfth Schedule) and process limits (prescribed in Part IX-A's parameters on who should make these decisions and how) on state power. Thus, an entity entrusted with governance of a whole or part of a city – such as the SPV in the Pune Smart City - ought to be democratic in its structure and accountable in the relationship it shares with its electorate.

E. Good Care is Inefficient: In Lieu of a Conclusion

In this article, I have argued that the absence of electoral accountability of the Indian smart city is a feature and not a bug of the SCM. Thus, the SCM compounds the democratic deficit already inherent in city governments created by states. Over and above this, the technological solutions being innovated in the Indian smart city – by prioritizing efficiency and optimization of the public

[105] Gordon and Walter (n 94) 318.

[106] Ibid, 319.

[107] See the law on making agencies and instrumentalities of the State liable to the State's obligations under Part III in *Ajay Hasia v Khalid Murjib Sehravardi* 1981 SCR (2) 79.

service for the citizen-user – are exclusionary to and further marginalize classes of citizens who do not qualify as users. Drawing from the PSSP case study, I show that datasets built from sensors at toilets and treatment plants effects a virtual segregation between citizen-users and citizen-workers. Therefore, the business-driven smart city agenda of efficiency splinters citizenship along class, caste and gendered lines.[108] Furthermore, solutions towards improving the deeper issue of public service provision, driven by such unrepresentative datasets, will not only entrench the structural democratic deficit of cities under the Indian Constitution but can also be exclusionary on caste, class and gendered lines.

The PSSP case study reveals that the SCM places the cart before the horse by first funding the innovation of technological solutions, and then foisting efficiency and optimization on the city government as if they are neutral or worthy goals. Instead, the Indian smart cities must pursue political agendas laid down by elected governments, and then finance and innovate technological solutions towards realizing them.

Of course, the question is whether "efficiency" itself can meaningfully be a political agenda for elected governments. At least in the realm of care work – public welfare, safety, sanitation and healthcare – I would suggest no. Good care is inherently inefficient.[109] The provision of good care, through deliberation and democracy, is also inherently inefficient. In the words of Eric Gordon,

> *"Deliberation is a great example of a meaningful inefficiency within a democratic process. The quickest way for a group to make a democratic decision would be to vote. But the process of deliberation where there is dialogue that builds over time where multiple stakeholders are involved, and the positionality of those stakeholders matters.*

[108] I borrow the term from Susan E Clarke, 'Splintering Citizenship and the Prospects for Democratic Inclusion' in Christina Wolbrecht and others (eds.), *The Politics of Democratic Inclusion* (Temple University Press 2005).

[109] In the words of Rutger Bregman: *"In our race against the machine, it's only logical that we'll continue to spend less on products that can be easily made more efficiently and more on labor-intensive services and amenities such as art, healthcare, education, and safety. It's no accident that countries that score high on well-being, like Denmark, Sweden, and Finland, have a large public sector. Their governments subsidize the domains where productivity can't be leveraged. Unlike the manufacture of a fridge or a car, history lessons and "doctor's checkups can't simply be made "more efficient. ...When you're obsessed with efficiency and productivity, it's difficult to see the real value of education and care."* Rutger Bregman, *Utopia for Realists* (The Correspondent 2016).

That very process is a process that people engage in not because it is efficient, but because it is inefficient. ....”[110]

Therefore, restoring self-government, political representativeness, and electoral accountability through a finite term limit to city governments requires a commitment to political agendas other than efficiency. Perhaps the SCM and the project of urban renewal might gain from taking up Gordon’s invitation to exploring “meaningful inefficiencies” in government.[111]

[110] Angel Quicksey, Eric Gordon on Valuing the Inefficiencies of Civic Life *Civic Hall* (10 July 2017) https://civichall.org/civicist/valuing-inefficiencies-civic-life/.

[111] See also Eric Gordon and Gabriel Mugar, *Meaningful Inefficiencies* (Oxford University Press 2020).

Centre for Communication Governance at
National Law University Delhi, Sector 14,
Dwarka, New Delhi, 110078, India
ccgdelhi.org | @CCGNLUD
Email: ccg@nludelhi.ac.in