INTRODUCTION

PRATIK KANJILAL

In contemporary India, the most dangerous communication is: 'Forwarded as received'. Prefacing millions of social media messages, the phrase institutionalises herd behaviour. It absolves the sender of moral guilt, transferring all responsibility to the hive mind of the Internet. It is a heavy responsibility, since the effects of messages forwarded as received include murder. In Digital India, 30 people were attacked by mobs last year as a consequence of fake news forwarded as received, which raised the bogies of child lifters and organ harvesters. The tools used in this brutal project were also deployed to delegitimise the press in India and the United States. The Internet does not respect national borders, and the dark side of the communications revolution is visible everywhere. A study commissioned by *The Guardian* and published in early March showed that in 40 countries the incidence of populist rhetoric has doubled since the year 2000, altering the political landscape worldwide in nations as diverse as the United States, Turkey and India.

This issue of the *IIC Quarterly* focuses on the Internet in a crisis of confidence, as the very technology that was hailed as a force of freedom, progress and transparency. Eight years ago, when Arab Spring broke out, it was revealed to have been used to vacuum up psychological and behavioural data on tens of millions of social media users, which was allegedly used to influence elections and a referendum in two of the world's most important democracies. As Kiran Karnik writes, this two-faced perception of the Internet has created a 'schizophrenia' between interest groups which want it to remain open, and those who demand privacy and controls.

Winter 2018–Spring 2019, Volume 45, Numbers 3 & 4

About the time this issue was planned, in response to privacy concerns, the Supreme Court restricted the use of Aadhaar data to welfare delivery. As the Journal went to press, Brexit loomed, without the stakeholders having any idea of the extent to which the referendum in the United Kingdom had been influenced by overseas entities. A decade ago, there was public concern that harvested data was being used to condition individual consumer choices (see Prabir Purkayastha for a lucid explanation of how things—including you, at the keyboard—are sold on the Net). Now, we know that aggregate choice can be tinkered with to delegitimise elections, the very basis of democracy. In the last few years, concerted social media campaigns have been used to mislead voters and subvert elections, to undermine the institutions on which democracy stands, including educational institutions, and to demonise minority communities and vocal dissenters.

In this issue, Vinton Cerf, the creator of the TCP/IP protocol on which the World Wide Web runs, points out that, as always, money is at the bottom of the problem. The Achilles' heel of the World Wide Web (and the social media that rides on it) is its business model:

> ...Metrics were offered to the generators of content: 'likes' on Facebook, followers on Twitter and views on YouTube. Users were rewarded by these metrics and this feedback loop led to behaviours that may not have been anticipated by the new media creators. To achieve higher metric scores, users were given incentives to produce more and more extreme content. Extremism gets attention.

Jyoti Panday investigates the WhatsApp pandemic, which leverages modern technology to resurrect old anxieties, and which has become the most visible of the issues that the mature phase of the digital age is raising. It is also analysed, along with international influence operations, by Samir Saran and Bedavyasa Mohanty. Tobby Simon presents a subhead of that story—information warfare—whose threat level Indians have not completely appreciated. It is generally seen in stories buried in the inside pages of newspapers, reporting cyberattacks from overseas on domestic infrastructure and government networks. It makes the front pages only when dramatic malware goes online, like ransomware, or the Stuxnet worm,

which temporarily crippled a national nuclear programme: in 2010, Stuxnet infected Iranian centrifuges used to purify nuclear fuel, and caused them to tear themselves apart.

Simon also makes two points which are often lost in the discourse. Quantum computers, which could be commercially available within a decade, would make present cryptographic and password-based network security redundant. With superfast computing and easy access to very large prime numbers, cracking them would be trivial for both governments and non-state actors. It is not clear how the Internet would address this watershed event, but it can be hazarded that biometrics would become the new norm, adding a new twist to the debate about the countervailing needs for privacy and unique IDs like Aadhaar. Secondly, Simon points out that hacking is no longer purely technical. Usually, it depends on social engineering, because human stupidity is easier to exploit than network vulnerabilities. As the old chestnut goes, 'The vulnerability is the idiot at the keyboard.' That idiot will always be around to let the hacker in.

Amber Sinha notes that increased smartphone penetration and computer access have not created an aware population, and that people are generally unable to evaluate the credibility and provenance of the electronic news that they receive. Scarcely surprising. No one ever claimed that access to schooling guarantees education. But while people generally swallow the news on the cell phone without complaint, there is disquiet about the digital frontier. An industry which values disruption above all else must cause unease among people who wish to lead the quiet life, and some new technologies inspire more alarm than hope. Foremost among them are artificial intelligence (AI) and Bitcoin/Blockchain, which Shashi Shekhar Vempati and Debjani Mohanty, respectively, investigate in detail. Here, let us contrast these technologies to see how problems raised by new technology sometimes resolve themselves.

Bitcoin is done and dusted, because all the fears about it came true. A currency floating free, without the intervention of a central bank, is too volatile to be relied on either as a store of value or as an investment. Its use for offshoring funds and making illegal or non-transparent transactions attracts unfavourable government attention. But Blockchain, the distributed ledger system which underlies Bitcoin, has been embraced by at least five national

governments, apart from numerous banks and service providers. It is the most reliable bookkeeping system because the record cannot be altered by a single player. Every stakeholder in a transaction must agree to change the record. This means that the Blockchain record would eliminate much of civil litigation, which is a result of false or unverifiable claims. Blockchain holds the promise of streamlining every activity in which bookkeeping figures, from property transactions to inventory management. A rock-solid accounting system has risen from the ashes of a failed currency.

That's already an old story, while AI is a future technology. Apocalyptic fears about insufficient regulation have been raised by Elon Musk and Stephen Hawking, who presumably know what they are talking about. The popular fear is of independent systems, which achieve the ability to replicate themselves and outstrip humans in intelligence, to the extent that the human race loses control over its fate. But in the immediate future, such a 'singularity' is not anticipated, and a lot of the anxiety about AI owes to a misunderstanding. AIs in operation today generally excel at one task, but do not know what the task is, or its place in the human universe. A computer may well beat you at chess, but it does not know that it is playing chess, while you do. It's impressive when you tell Alexa what you'd like to eat and it books you a table at a restaurant, but all that its AI has done is to convert your speech to text, which is fed into search engines and booking services. Apart from the voice recognition function, you have been doing the very same thing, from your keyboard. Most importantly, neither Alexa nor the chess computer know that they exist. From this, to extrapolate to an autonomous, Terminator-like military machine, or HAL 9000 in 2001, which killed because of a guilt complex, takes a leap of the imagination.

Similarly, the marketing catchphrase 'new media' means nothing except a new mode of distribution. The content of new media is actually old media—text, pictures, sound, moving pictures—which are distributed over TCP/IP networks. It is the distribution that confuses us. We are living in the age of 'convergence', the Holy Grail of digital capitalism in the 1990s. We are finding it incomprehensible, because fake news is travelling to us down the same pipe, to reach the same phone, as formal news, delivered by journalistic organisations which work with checks

and balances developed over decades of experience. The grain and the chaff are available at the same counter, and you can take your pick. If you choose unwisely, or if you instinctively seek bubbles which confirm your prejudices, you could become disconnected from reality. The 'wisdom of crowds' powers Wikipedia and makes informed consumer choice possible in online retail; but in clever hands, it enables political 'astroturfing', in which small but vocal groups appear to be as weighty as the mainstream, altering perceptions and electoral outcomes. This is the no-man's-land of botnets and fake accounts, which repeat a single message until it looks like a tide in the affairs of men. Concerns about the effects of technological black magic can only intensify as candidates are sold to the public by the very gimmicks that are used to sell instant noodles.

The new asset in the salesman's arsenal is Big Data, which Vrinda Bhandari investigates in the course of her analysis of the right to privacy in the age of analytics and the Internet of Things, when huge volumes of raw data can be stored and manipulated quite cheaply. Even if storage of primary data is restricted by privacy laws, metadata in large volumes can profile a person very accurately. At the crudest level, without tapping a phone but merely looking at the call record, agencies can deduce a lot about the owner's relationships. Our own government had proposed a social media monitoring tool which would have collected both data and metadata of users to generate a '360 degree view' of voices on the Internet, which can lead or swing conversations. The proposal was met with public uproar and quietly shelved.

Ironically, not only would this tool have identified the change-makers in social media, but also the leading purveyors and amplifiers of fake news. Vibodh Parthasarathi and Andreas Mattsson, and Govindraj Ethiraj, examine the most visible disease of the Internet: Ethiraj focuses on photoshoppery in India, while Parthasarathi and Mattsson look at fake news through the lens of the Swedish general elections, and the *sanningssägare,* or people who tell you what they think the truth should be.

Problems invite solutions, which sometimes become problematic themselves. Back in the 1990s, the pioneering citizens of the Internet conceived of it as a haven of free and anonymous speech. But virtual speech has real consequences. Women journalists in India have suffered violent online abuse for years, and are just

beginning to talk about it. Death threats are commonplace. Apar Gupta follows the government and the law as it grappled with the issue: the introduction of Section 66A in the Information Technology (IT) Act, in 2008, which criminalised the sending of offensive messages, followed by misuse by governments to curb its freedom of speech, followed by the landmark judgement of the Supreme Court in *Shreya Singhal vs Union of India*, in which the provision was struck down. The question of freedom of speech versus the right not to be harassed remains a work in progress.

Section 69 of the IT Act, which requires communications platforms to supply unencrypted data to the government on pain of imprisonment, is another point on which perceptions differ. India is one of a few countries to demand that encrypted services like WhatsApp provide access to their communications. The rationale is national security, but in unscrupulous hands this provision could be misused to invade the privacy of citizens. The corporate response to increasing state surveillance is also interesting. Mark Zuckerberg of Facebook, which owns WhatsApp, now plans to focus on promoting private conversations rather than the free-to-air multicasting model that turned his company into a giant. As government surveillance increases, the monetary value of privacy will appreciate. Elsewhere, Purkayastha raises a question which is giving headaches to institutions and organisations everywhere: When an employee tweets a personal opinion, is the communication private or public? And Mahima Kaul of Twitter India lists the hashtags that have helped dispersed interest groups to connect and push for social change. Most memorable, of course, was the Indian chapter of #MeToo, which brought down a minister of the central government.

Osama Manzar and Udita Chaturvedi point out that despite the smartphone boom, the digital divide persists. Their focus is poor connectivity among civil society organisations, because of which we do not get the real picture of the public will. Amit Sen speaks of the growing addiction to devices and networks among young children, and reveals that the phenomenon follows the same chemical pathways as drug addiction. The result is a set of symptoms akin to ADHD, and the child affected is unable to either learn or socialise properly. Strangely, this problem is generally left to parents to deal with (who are as addicted to the screen as their children),

though governments should be concerned about an impending social crisis as present generations of children grow up.

But perhaps we must not rely too much on governments. The future of digital capitalism, whose most powerful corporations are located in the United States, may be unassailable for reasons of geopolitical expediency. Attempts to break up corporations, such as Facebook and Google, which own multiple properties and platforms, under antitrust law would be resisted on the plea that they project US interests globally, and contribute to its perceived power. Sadly, the technology that was created to undermine traditional hierarchies has created a hierarchy of its own. At present, the future of this new hierarchy is assured.

◆