THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

July 13, 2021

WhatsApp in India

A Tale of Big Tech, Privacy Violation and Government Control

By: Vidya Subramanian

The ongoing tussle between the Indian government and social media companies has compromised the data integrity & privacy of citizens. We need an ecosystem of innovation and regulation to keep in check the unrestricted data powers of Silicon Valley giants.

Facebook (which owns WhatsApp)— that big bad Silicon Valley giant that harvests your data and sells it to advertisers — is fighting the government of India in court to protect the privacy of its users? What is going on?

The new IT Rules of 2021 —officially, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021— have brought sweeping new changes to the way that digital media (including messaging applications, social media sites, digital news sites, over-the-top (OTT) platforms) is administered in India.

Among other things, the rules require digital intermediaries (such as WhatsApp, Facebook, and Twitter) to allow a tracing of the origin of messages to the first sender, as a means of curbing the spread of misinformation and fake news. The government has said that they do not expect every single message to be traced, only the ones that spread misinformation, and on orders from a "competent authority." In response, WhatsApp has filed a case in the Delhi High Court pointing out that tracing some messages would mean that it will then be possible to trace all messages. This will mean breaking the much vaunted encryption WhatsApp boasts of.

> [I]f companies such as WhatsApp are forced to break encryption, then even the messages exchanged will not be private anymore, becoming vulnerable to snoopers of all hues – government, hackers, etc.

Of course, the encryption on the message only keeps the content of the message unreadable. WhatsApp collects a lot of other data from the use of its app, even as the messages themselves remain encrypted: who sent it, who received it, the locations of the sender and receiver, the devices used to send and receive messages (their unique device IDs), the length and type (text, image, or video) of message sent, financial information, purchases, diagnostics, contacts. These other things, the ‘data exhaust’ or the metadata of our online behaviour is what has been made monetisable (more on that in a bit). But if companies such as WhatsApp are forced to break encryption, then even the messages exchanged will not be private anymore, becoming vulnerable to snoopers of all hues, including governments and hackers.

The other problem, of course, is what does it mean to be an ‘originator’ of a message. If I see a piece of inflammatory misinformation on, say, Twitter, and I copy it to WhatsApp and send it, and it goes viral from there, am I the originator of the message? If the person who created the message is the originator, then there is no way for anyone to know who that person is by tracing the source of the message on WhatsApp. The Twitter user I copied it from may have got it on email, or seen it on a pamphlet slid under her door. How then is this traceability of messages on WhatsApp helping find misinformation spreaders?

Playing both sides

But it really is not as though WhatsApp has become the torchbearer of privacy rights by arguing for it in this case. Ironically, there is another case in the courts right now in which both WhatsApp and the Government of India are currently arguing from opposite positions. WhatsApp appealed last March to the Delhi High Court against a Competition Commission of India order that it was unfair that WhatsApp’s new privacy policy required all its users to agree to allow WhatsApp to share user data with other Facebook-owned companies. The government is arguing that the new privacy policy violates the informational privacy of Indian citizens (WhatsApp told the court in early July that it would not compel users in India to accept the policy until India’s planned data protection law comes into effect. However, millions of users have already accepted the policy on their apps when prompted.)

The government’s case here is that WhatsApp violates privacy norms by failing to specify exactly what data it collects, failing to notify users about the kinds of data it will collect, and failing to provide the exact purpose for its collection. The government has also raised

the issue of withdrawal of consent. This means that a user should be able to withdraw consent for data collection and sharing, even if they have agreed to share data in the past.

> Users … are caught between privacy violations by the government and by private companies; and neither is without its dangers.

Another wrinkle for WhatsApp in this case is that while this update gives WhatsApp the right to share user data of all Indian users with Facebook group companies, it permits European users to opt out of the policy. This is because the General Data Protection Rules in Europe have been quite stringent about large monopolistic tech companies collecting data about people in its jurisdiction. This opt out provision had not been made available to Indian users, who have had to accept these provisions in order to keep using the app.

The Indian government in this case has argued that the informational privacy and user choice of Indian users is "sacrosanct," while in the other case it has argued for every message sent via WhatsApp to be traceable with scant regard for the informational privacy of the same Indians.

It is these double standards on the part of both WhatsApp and the government that give cause for worry. Users, in the meanwhile, are caught between privacy violations by the government and by private companies, neither of which is without its dangers.

The power of metadata

This brings us to the problem of metadata. Simply put, metadata is everything except the content of your communications. And many times it is enough to track the intimate details of a person's life. For instance, if you have the Facebook app on your phone, Facebook knows where you are at all times because it can access the location information. Even if you think you turned off that setting, it still has access to your mobile network and knows which cell tower you are connected to.

If you meet someone who also has any of the apps of Facebook group companies on their phone, and they are allowed to share user data with each other, Facebook now knows you have both been in the same space because it has both your location information. It is possible to identify if it was a business meeting, a date, a gathering of friends, or a fixed appointment, simply by knowing the duration of time you spent, where it was, who you called immediately after, where you went next, and other such details, even if the app was not eavesdropping on the contents of your conversation.

Similarly, through tracking people's online behaviour — what links you clicked, what products you checked out, what articles you read, what photos you liked, what cat videos you watched, which groups you engage with — companies such as Facebook, Google, and Amazon have built a profile of each of their users. They leverage this profile with advertisers, who can be selling anything from soap to a political ideology to make sure you – specifically you – see their message.

The problem is not just that we are all being constantly monitored and surveilled, which is a huge problem by itself. What makes it worse is that such intimate surveillance of all humans at this planetary scale makes it possible to influence the collective behaviour of large groups of people, for any means— nefarious or otherwise. We already know that it was the use of Facebook metadata by Cambridge Analytica that allowed them to target specific voters with specific messaging that had been created to fit their ideological profiles. It was this that eventually led to Donald Trump being elected in the US and even the Brexit vote in the UK.

> [T]hrough tracking people's online behaviour: what links you clicked, what products you checked out, what articles you read … companies such as Facebook, Google, and Amazon, have built a profile of each of their users.

Large tech companies with many fingers in many pies have the ability to know a lot more about us than simply where we are and who our friends are. (To be sure, this by itself is enough to endanger the lives of several people,political activists living under oppressive regimes, whistle blowers, even victims of domestic and other forms of intimate abuse; the list is long and painful.) Large monopolistic tech giants that own several different companies that collect data about many different parts of our lives and then have the capacity to put it all together and make predictions of our future behaviour, have too much information about each and every single one of us. Having all of this data about all of these people is giving private, for-profit companies a whole lot of power over a whole lot of people.

Living in a neo-Panopticon

The 18th century British philosopher Jeremy Bentham came up with an interesting idea for a circular prison building called the Panopticon. Essentially, it was a building where one guard could keep an eye on several prisoners, each in their own separate prison cell. It was supposed to be designed in such a way that no prisoner would know if they were being seen at any moment or not; but because the possibility always existed, it would serve to model their behaviour as though they were under constant scrutiny. A starker version of surveillance was imagined by George Orwell in his novel *1984*, where all citizens were constantly under surveillance by agents of the totalitarian head of state known as Big Brother.

The point is we are now living in a surveillance society, even though we may think we have more freedoms than ever before. There is no longer any doubt that our every move is being watched. Not just watched; collected, recorded, collated and analysed to explain and predict our behaviour. We live even our intimate lives in full view of large technology companies and governments. And the worst part is there is no longer a need for Bentham's prison guard. We happily carry our monitors in our pockets.

> Instead of the state needing to use coercion to find out the innermost secrets of its citizens, all of our secrets can now be known from our phones, social media and online shopping patterns.

Contemporary philosopher Byung-Chul Han has suggested in *Psychopolitics: Neoliberalism and New Technologies of Power* that the surveillance society we now live in is similar to those visions of Bentham and Orwell, only far more seductive and entirely voluntary. He argues that the smartphone has replaced the torture chamber and forced confessions have been replaced with voluntary confession on social media. Instead of the state needing to use coercion to find out the innermost secrets of its citizens, all of our secrets can now be known from our phones, social media, and online shopping patterns.

All of this, he argues, is in service of the engines of capitalism — the ideology that moves with profit as its only driving force, exploiting people, governments, and nature to make more and then even more money. This system is built to let us think we have freedom, while making us cogs in a wheel of an ever more exploitative set-up. And using the smartphone — the zeitgeist of this generation — this ideology has really almost taken over the world, without coercion, without punishment, and without making us feel exploited. "Instead of forbidding and depriving it works through pleasing and fulfilling. Instead of making people compliant, it seeks to make them dependent," writes Han.

Companies or governments?

But these are the problems of large companies owning our data. What of the government? If the new 2021 IT Rules are any indication, there is a clear shift in the Indian government's policy towards technology companies: this is a movement from regulation to control.

Regulation of tech giants should be about allowing the government to oversee their activities and put in place checks and balances that would protect the rights of their users and consumers, while at the same time encouraging innovation and new ideas to keep growing, all the while ensuring that large companies do not misuse their power and smaller players have room to grow.

> If the new 2021 IT Rules are any indication, there is a clear shift in the Indian government's policy towards technology companies: this is a movement from regulation to control.

Instead, now having control over tech companies is for the government to have the power to manipulate the power of large tech companies for its own purposes, without necessarily putting in place policies that either encourage smaller players or protect the rights of users and citizens. It is as dangerous as large swathes of individual data in the hands of for-profit corporations. Governments that control tech companies can leverage them to their own advantage, and put in place means of censorship and control of content that directly affects fundamental freedoms of speech, and expression. (A good way to understand this difference is to compare the GDPR of Europe to the great firewall of China.)

While there are several cases in court right now questioning different sections of the new IT rules, , the WhatsApp cases are important tests by themselves. Given how ubiquitous WhatsApp has become and how central it has been to communication strategies (for election messaging and otherwise) pioneered in India by the current ruling party, the manner in which the WhatsApp cases are resolved will show clearly the direction in which government oversight and regulation will go.

> Making private communication more visible to the government will create a nightmare even more Orwellian than the one we live in now.

If the government ensures that every message a WhatsApp user sends is readable, it becomes that much easier to find and punish — using the entire might of the state — people who disagree with it, challenge its narrative, or in any way question its activities. Making private communication more visible to the government will create a nightmare even more Orwellian than the one we live in now.

The flimsy excuse of preventing the spread of misinformation does not require such drastic measures. Misinformation, fake news and propaganda far predate technologies such as WhatsApp and social media and likely will outlast them. Technological tools themselves are never neutral. In this case, they have served as conduits for faster and wider spread of malicious misinformation, mostly by design.

What we need in India is an ecosystem of innovation and regulation that can bring to heel the untrammelled data powers of large Silicon Valley giants, such as Facebook that owns several companies such as WhatsApp, without compromising on the data integrity and privacy concerns of Indian citizens. Resolving the conflicting positions that the Indian government has taken in the two WhatsApp cases will be a litmus test for the new IT rules.