To Delete or Not to #DeleteFacebook, That is the Question

There are no easy answers beyond ensuring that we as citizens do not surrender our privacy to darker forces until a global internet governance regime is in place.
As individuals we have become data points for commercial gain, and perhaps far more dangerously, political gain—without the remotest pretense of permission. Credit: Reuters/Dado Ruvic

Maya Mirchandani
For the last few days, I’ve been grappling with an unexpected existential crisis over whether or not to delete my Facebook. While the harvesting of data of 50 million Facebook users in America for political gain, without consent, is unconscionable, the issues the Cambridge Analytica scandal has raised — of privacy, consent and data security — highlight perhaps the biggest challenge of the 21st century — that of governing the internet.

Since joining Facebook a decade ago, I’ve found it fun and extremely serendipitous — finding people I had long lost contact with, school friends, or making new friends, courtesy conversations on other’s pages. It is also useful in allowing me maximum contact with a vast family with minimum effort. All these reasons that made so many of us join Facebook dulled us into complacent comfort, consenting without reading the fineprint or understanding the ramifications of giving up so much of ourselves each time we voluntarily tagged photos, did random personality quizzes and checked into different places.

In the absence of clearly spelt out rules of governance, we didn’t see that this seamless syncing of our virtual world with the real world was creating a Frankenstein’s monster that could turn on us. We had no way of knowing that those fun quizzes telling us whether Rome was the perfect city to live in, or yellow was our aura colour, or which 1980s’ popstar we would be born again were fodder for political analysts, tasked with profiling us to either influence our politics or reinforce our biases — sometimes with violent consequences. The privacy settings we checked off perhaps ensured safety from criminals, but each time we took and allowed these quizzes to access our friends’ list and photographs in order to proceed, we surrendered a little more of ourselves.

It is this heady addiction to Facebook — logged in 24/7 on our computers and phones — that has brought us to this pass. As individuals we have become data points for commercial gain, and perhaps far more
dangerously, political gain — without the remotest pretense of permission. The developers of these quizzes mapped our food habits, book choices, political ideologies and concerns and monetised that information by selling it to the highest bidder. In the case of the political consulting company, Cambridge Analytica, members of Donald Trump’s Presidential campaign management bought and used the information of 50 million Facebook users to send targeted political messaging aimed to influence voters during the contentious 2016 American Presidential race.

Several reports indicate that it was Trump’s predecessor, former President Barack Obama whose campaign team first discovered the immense possibilities of using Facebook for political gain in 2012. It is also true that if it weren’t for the fact that liberal America is still reeling with shock since Trump’s win, perhaps such a scandal may never have come to light, nor would we be having a global conversation on fake news, even though so many of us in India have been voicing concerns over the spread of unchecked propaganda and fake news on social media for the last few years.
It is now time to recognise that as enraged as we might be over the Cambridge Analytica scandal, this is only one of several alarming realities to contend with in our social media-driven world — most importantly, as concerned citizens who follow the rule of law, our own roles in surrendering ourselves to tech giants. Our smartphones are loaded with all kinds of personal data — phone numbers and photographs, financial information, travel, reading and shopping preferences. Facebook, Google, Amazon and Apple together know everything there is to know about us through our online habits — a reality that makes it imperative for us to seek ways of plugging the damage since these companies, irrespective of the outrage, are probably here to stay.

But like everything else in our technology-dependent universe, all attempts to plug the damage come with their own dilemmas. The European Union is prioritising privacy concerns over fears of political misuse — misinformation and attack that can pose threats to democratic functioning as we know it. Germany, on the other side, has already passed legislation warning social networks like Facebook, Twitter and Google against fomenting hate speech. The law demands that networks remove illegal content as defined in Germany’s criminal code promptly, else face fines of up to Euro 50 million each time they fail to act.

Social networks became popular because they allowed individuals to exercise absolute freedom of speech. Unless their broad community standards are breached and reported as abusive, these networks have provided an uninterrupted, unfiltered flow of information and ideas to a vast global population that feels empowered to challenge the relevance of mainstream media in today’s polarised world. Last year, Facebook
itself said it took down an average of 288,000 posts a month based on reports of hate speech and violent content.

On March 12, ten days before the scandal over Facebook’s data breach for political gains broke, Mazurki Darusman, chairperson of the United Nations Independent Fact Finding Mission on Myanmar, blamed Facebook for playing a key role in what the UN Human Rights Commissioner called the possible genocide of Rohingya Muslims last year. Darusman said Facebook was a huge part of public, civil and private life in Myanmar, used both by citizens and government, but it had “substantively contributed to the level of acrimony and conflict within the public…Ultra-nationalist Buddhists, through their own pages were inciting violence against Rohingya and other ethnic minorities.”

Facebook, under fire globally for the spread of hate speech well before this latest scandal, has been proactively trying to promote what it calls “counter speech” through various initiatives engaging young people, civil society organisations and celebrities in efforts to promote narratives of tolerance, diversity and acceptance on the platform. Whether these efforts are noble, or simply geared towards taking the heat off from growing accusations of fomenting hate worldwide is debatable, but the initiatives have yet to see any substantive results.

In India, where Facebook crossed 240 million users last July, (over 10% of the platform’s global user base) efforts are further complicated by the fact that fake news, propaganda and hate speech all exist and circulate within the same ecosystem of political and religious polarisation. Many more, especially rural and older populations who cannot or will not go through the complications of logging on via email, simply use their smartphones to access the now encrypted instant messaging service WhatsApp, acquired by Facebook for $16 billion in 2014.

Today, WhatsApp’s co-founder Brian Acton is one of the biggest names leading the #deletefacebook campaign, urging us all to care about
privacy, as we well should. But WhatsApp in India is fast becoming a bigger concern. Its encryption may well protect our privacy, but examples abound of its inability to prevent the spread of fake news and incitement to violence. WhatsApp’s ease and falling prices of both smartphones and data has meant we are flooded with unverified, unfiltered, often uninformed communication, even misinformation. In an extreme comparison, some have even voiced concerns over the potential of WhatsApp in India to become that of the radio in Rwanda where 800,000 Tutsis were killed in three months in 1994. The radio became the trigger that incited and mobilised the Hutus.

Perhaps that’s a stretch, but in December 2010, Google’s Eric Schmidt and Jared Cohen wrote in Foreign Affairs magazine that the rise of “‘interconnected estate’ where any person with access to the internet regardless of living standards or nationality is given a voice and has the power to affect change” will create both opportunities and challenges to established institutions as we know them and warned of the potential of these connection technologies for both good and evil. Given the potential for abuse and manipulation in charged political times, there is no question of state control or regulation of social networks by those in power. The fact that social networks like Facebook must be accountable for galloping roughshod over our rights is equally unquestionable.

Under these circumstances, can these platforms self-regulate? More importantly, given this massive breach of faith by Facebook, its unclear how long it will take to re-establish trust in their motives even if companies pledge to improve their data security systems and guidelines. As we ponder these challenges, there are no easy answers at the moment, beyond perhaps ensuring that we as citizens of the internet educate and empower ourselves enough not to surrender our freedoms of privacy and expression to darker forces, until a global ‘internet governance’ regime is agreed upon with the involvement of all stakeholders — tech giants, civil society and governments.
Meanwhile, whatever we have already put out there on social media exists somewhere in the ether. Deleting or not deleting accounts today doesn’t change the fact that our metadata is already secured on their servers somewhere. A download of ones Facebook archive will give a sense of just how much about us they know, both with and without our active consent. Therefore, my existential dilemma continues. Perhaps it’s a question I will pose to my friends on Facebook, who from the number of people I continue to see online, are grappling with the same questions.

Maya Mirchandani is a Senior Fellow at Observer Research Foundation and an independent journalist.