Is Big Data a threat to free democratic choice?

The 1928 US presidential elections were a lively affair. Democratic Party nominee Alfred Smith may well have wished they were less so. Backers of Republican nominee Herbert Hoover accused Smith, among other smears, of indulging in “card-playing, cocktail drinking, poodle dogs, divorces, novels, stuffy rooms, evolution . . . nude art, prize-fighting, actors, greyhound racing and modernism”. It was apparently an effective if eccentric bit of calumny. Hoover went on to win.

It is a useful oddity to bear in mind when considering the ongoing Cambridge Analytica scandal. Electoral dirty tricks are a regrettably time-honoured tradition. That Donald Trump’s presidential campaign may have used underhand means to target voters is thus not the central issue. Nor is it that Facebook betrayed user trust, although it certainly had its share of lapses. The heart of the matter is the nature of the bargain users have made with tech companies like Facebook and Google.

When The Guardian reported the story last week, it presented Cambridge Analytica’s alleged use of data from some 50 million Facebook users to target US voters as a data breach. Facebook is contesting that it was a breach. But this is about more than semantics.

A breach would imply a failure in Facebook’s security, and thus liability on its part. Facebook is thus trying to push a different narrative: that academic Aleksandr Kogan, who collected the data via his app, thisisyourdigitallife, did so according to Facebook guidelines. When he then passed on that data to Cambridge Analytica, however, he was in contravention of the guidelines and Facebook took appropriate action.

Facebook is right in claiming that the data was collected as per its guidelines but wrong in claiming due diligence thereafter. The Guardian revealed the Cambridge Analytica angle in 2015. Facebook’s lawyers moved swiftly, demanding that Kogan and Analytica delete the user data. But the paperwork took two years to complete. Facebook neglected any auditing to confirm that the data had actually been deleted. It also failed to publicly reveal the leak, possibly violating a 2011 agreement about making it clear how user data was used.

These are all lapses for which Facebook should be held to account. Indeed, with the US Federal Trade Commission gearing up to hold its feet to the fire, and the threat of a hefty fine if it is found to have violated the 2011 agreement, Facebook is starting to feel the heat. It has also earned negative publicity and taken a hit to its market value.

But the fact that such vast amounts of data were so easily collected in the first place—and without breaking the rules —points to the larger issues to do with the economics of the internet. Since its inception in 2004, Facebook, more than any other company, has propagated the norm of digital businesses fuelled by private data that users sign over willingly in exchange for notionally free services. Certainly, privacy advocates have helped put some guardrails in place. For instance, in 2015, Facebook altered the rules that allowed apps like Kogan’s to collect data not just on individuals who signed in but also of people on their friends’ lists. However, the core model has remained unchanged.

Can regulatory action change this? To an extent, yes. Data localization conditions can ensure that user data collected within a country must be kept within it. Regulations can also compel businesses to adopt privacy by design principles that foreground user choice and consent. The European Union’s General Data Protection Regulation (GDPR), which takes effect from 25 May this year, has adopted this approach. Perhaps the most stringent data protection regime globally, it will be a litmus test for companies’ ability and willingness to comply. US lawmakers, protective of

Silicon Valley champions until not too long ago, are also starting to lose patience.

Regulations cannot, however, alter the fundamental economic value of user data or the business models they fuel. Besides, the regulatory approach often hinges on user consent as the GDPR does—and the growth of social media companies over the past decade is fair evidence that consent is not hard to obtain, even with the knowledge of private data being signed over. This has political implications as well. Cambridge Analytica and other such firms have boasted of the merits of psychographic targeting based on user data. This is currently a dubious proposition with little proof to back it up. But that might change as algorithms grow more sophisticated. The current controversy may seem far removed from India, but political parties here are also embracing Big Data analytics to understand voter behaviour—and perhaps alter it.

Whether privacy concerns will compel a change in digital business models will depend in the end on the market and consumer choice. If users prioritize privacy enough to opt for currently nascent technologies such as blockchain-based self-sovereign identity systems, Facebook and its ilk's heyday will be a blip in the arc of the digital economy. If not, scandals such as Cambridge Analytica will remain mere speed bumps.

Should the scraping of user data from social media be regulated? Tell us at views@livemint.com

END