

Protecting our data

After the Cambridge Analytica crisis exploded, Union Law Minister Ravi Shankar Prasad warned Facebook against the misuse of Indians' data and any attempt to influence the electoral processes of this country. Unsurprisingly, the issue subsequently took on a partisan hue after the Bharatiya Janata Party and the Congress started trading accusations about hiring the services of Cambridge Analytica. Regardless, the fact remains that a clear mention was made by representatives of that company, which stands accused of misusing the data of 50 million users stored on Facebook and rigging multiple elections worldwide, of political involvement in India.

In a sense the data of Indians has been ripe for the plucking for some time now. Statista, an online data portal, estimates that India had 281.81 million mobile phone Internet users in 2016 and would have an estimated 492.68 million mobile phone Internet users by 2022. In 2019, there would be around 258.27 million social network users in India, up from 168.1 million in 2016. Facebook is projected to reach close to 319 million users in India by 2021. This proliferation of digital networking has provided an incredible platform for people to communicate, but its flip side is that individual users are increasingly viewed as legitimate targets for mining personal and metadata. As elsewhere, data mined from Indian users of social media may prima facie be used for relatively innocuous purposes such as targeted cross-platform advertising, but analysed in bulk, such data can provide an intimate psychological profile including ideological preferences that together help campaign managers target communications and forecast voter behaviour.

Further, certain risks to the very health of democracy stem from the dominance of social media platforms, which not only deliver personalised content to users, but in many cases privilege content based on engagement rather than quality. This limits users' access to information, which in turn leads to political polarisation and the spread of fake news. And fake news, as we know, has had a considerable impact on electoral politics to the point where it is being investigated by authorities in the U.S.

All of this raises a red flag on the question of data protection laws, which are virtually non-existent in India. It was only in 2017 that the Ministry of Electronics and Information Technology released a White Paper by a committee of experts led by former Supreme Court judge, Justice B.N. Srikrishna, on a data protection framework for India. Until that consultative process agrees upon basic principles to guide data protection laws, India will continue to suffer the existing regulatory framework under the Information Technology Act, 2000, which only identifies six types of "sensitive personal data" and requires entities handling such data to have "reasonable security practices and procedures" in place before collecting the information. The fact that the contracting parties can agree on their own rules governing the use of such data, and what security standards or privacy policies are applied, tells us all we need to know about the strength of data protection in the country.

The India-Japan economic relationship remains underwhelming in relation to strategic ties

END

Downloaded from crackIAS.com

© **Zuccess App** by crackIAS.com