NUS National University of Singapore | ISAS Institute of South Asian Studies

ISAS Brief

No. 949 – 22 July 2022

Gaps and Mishaps in India's Digital Economy

Karthik Nachiappan and Shavinyaa Vijaykumarr

Summary

RazorPay's submission of privately held customer data to the Indian government reveals the perils of operating in India's digital economy.

Following the ongoing spat between Twitter and the Indian government, the RazorPay-Indian government episode has served as another blow to the operational environment for digital outlets in India. RazorPay, an eight-year-old Bengaluru payment gateway start-up, found itself in the spotlight after it was revealed that the company had released Alt News' donor data to Indian authorities to cooperate with an ongoing police investigation involving Alt News.

This impasse began when one of Alt News co-founders – Mohammed Zubair – was arrested for allegedly hurting religious sentiments through a tweet he made four years ago. Things went awry when the charges against Zubair were expanded to include the violation of India's Foreign Contribution (Regulation) Act, which curtails foreign donations to non-profit organisations. Authorities allege that Alt News has accepted donations "through RazorPay from Pakistan, Syria, Australia, Singapore, UAE [United Arab Emirates]".

Alt News stated that RazorPay failed to inform it that the data of their patrons would be shared with the police. While the specificities of the content of data shared with the authorities remain concealed, Alt News has accused RazorPay of sharing all its users' payment data, including phone numbers, email addresses and tax identities, with the authorities. Alt News added that it did not enable international payments on its RazorPay account, only linked to Indian payment instruments like bank accounts, digital wallets and credit cards. RazorPay, in response, released a statement clarifying its actions, stating that the firm had received a written order from the legal authorities under Section 91 Criminal Procedure Code and [that it is] mandated to comply with the same as per the regulation under the provisions of the Indian law".

RazorPay's response and statement fundamentally revealed the difficulties small digital firms and organisations experience operating in India, attempting to uphold high standards of data security to protect customer information while adhering to government decrees to hand the data over with limited recourse. In fact, RazorPay had little choice but hand over the data. Police authorities have sweeping powers under the Indian law to request and obtain information that could be deemed as contributing to anti-national or sensitive activities. Had RazorPay refused, it could have risked shutting down operations. Resisting the government would have also opened the doors for endless rounds of litigation for RazorPay.

Critics, however, claim that RazorPay acquiesced to the government's demands without sufficiently questioning the validity of these requests. RazorPay maintained that the data was shared with the authorities only after comprehensive consultations with "policy experts and legal counsels" and that "the specific data [it] shared was only restricted to what was within the scope of [the] investigation". That said, RazorPay users are well within their rights to seek answers as to why their proprietary data was provided, potentially opening them to government questioning.

The increasing frequency of such requests to digital businesses and outlets by the Indian government testifies to the dire need for a comprehensive data protection law to govern and manage such issues. Indian citizens and internet users demand to be protected from being caught in the crossfire between the government and technology firms. This situation also applies to digital payment businesses like RazorPay. A robust and transparent law covering data and privacy would establish guidelines under which firms are expected to hand over user data, and the powers and limits of the power government authorities possess, especially in such situations. Undeniably, digital payment services like RazorPay require additional protections given the nature of their businesses and transactions; undoubtedly, these outlets should also provide information on how they use and manage customer data collected from Indian users.

The Indian government will likely have some exceptions carved into the final data protection bill that will exempt it from certain requirements on the grounds of national security or public order, as evidenced in this case. The implications of such carve-outs are worth understanding. Giving the government unchecked power to request and obtain critical data, like payments, could have a ripple effect, deterring users and consumers from transacting and communicating freely online that could undermine trust and security in India's digital economy.

It would also make regulatory compliance onerous for small digital firms, increasing their costs and overheads should they fear dealing with recurring government requests that they cannot challenge or defy legally, given a law that tilts power to the government. What these digital businesses require instead are clear rules vis-à-vis user data they collect online, how to keep that data secure and intact and assurances to internet users who would place their faith and personal data in their hands. The future of small digital firms and the digital rights of internet users in India rests on these provisions being added to the final Personal Data Protection Bill.

. . . . .

Dr Karthik Nachiappan is a Research Fellow at the Institute of South Asian Studies (ISAS), an autonomous research institute at the National University of Singapore (NUS). He can be contacted at isaskn@nus.edu.sg. Ms. Shavinyaa Vijaykumarr is a Research Analyst at the same institute. She can be contacted at shav@nus.edu.sg. The authors bear full responsibility for the facts cited and opinions expressed in this paper.