BerkeleyLaw
UNIVERSITY OF CALIFORNIA
Berkeley Center for
Law and Business

Berkeley Center for Law and Business
University of California, Berkeley
School of Law
Boalt Hall #7200
Berkeley, CA 94720-7220

India's New Data Localization Regulation Imposes Challenge on Payment Vendors

By: Jiali Yang, LL.M Candidate 2019 | October 24, 2018

An order enacted by the Reserve Bank of India (RBI) regarding data localization went into effect on October 15, 2018. This order allows authorities to have "unfettered access" to data, giving them the power to supervise all payment data happening in India. Under the order, all payment system operators must store "full end-to-end transaction details" involving Indians in India. The foreign element of these transactions can be stored in elsewhere, if required by that foreign country. All system providers must comply with this order within six months.

U.S. credit card companies and other payment service providers are struggling to follow the order. Companies like Visa, American Express, PayPal, and Amazon have pointed to their expansive data processing and fraud detection systems, located throughout the world. The companies have argued they need more time to prepare for the localization. In fact, Visa and Mastercard have allegedly requested "an extension of the deadline and a relaxation of the rules, citing operational difficulties and security concerns."

RBI, however, has ignored these pleas. The agency has made it clear via phone calls and letters that it would impose fines if companies missed the order's deadline. Facebook's WhatsApp messaging service is the only major American company that expressed its ability to comply.

The 21st century is known to be an era of data. Almost everything we do on the Internet can be turned into data, which consequently involves some heated issues like individual privacy and national security. Europe implemented the General Data Protection Regulation (GDPR) to protect privacy rights by requiring companies to request individual's explicit consent before processing data. Apart from this "individual consent" approach, some countries have adopted a "governmental scrutiny" approach. China's data protection law, for example, also requires a security assessment when data gathered inside the country may be transferred outside of China. For critical information infrastructure operators (CIIOs) such as public communication and information service providers, the security assessment will be conducted by regulatory authorities. For non-CIIOs, this assessment will be conducted by companies and monitored by regulatory authorities, unless the transmission of data may harm the public interest or national security.