Banking with Google

Regulators need to be watchful about sensitive financial data

Reports that Google intends to enter the consumer banking space through a partnership with Citibank did not cause any surprise, because many tech firms are looking at the consumer finance market. However, there are genuine concerns about the implications for data security and data sovereignty if this happens. The search engine giant would gain access to vast, new, highly sensitive datasets if it became a banking service provider. It is unclear what it intends to do with that data. Recent revelations that Google had discreetly gained access to the health data of at least 50 million Americans have added to the apprehensions.

Consumer finance is a new focus area for tech majors. Apple has launched credit cards in partnership with Goldman Sachs. Facebook is trying to create a cryptocurrency with its Libra initiative. Facebook's subsidiaries, WhatsApp and Instagram, are setting up payment systems within the respective apps. Amazon is said to be seeking a partnership to provide banking services. Google Pay is already a very successful payment app. It has around 67 million users in India, and it is said to be generating over 50 per cent of all Unified Payments Interface (UPI) transactions and also doing well elsewhere around the world.

The Citibank-Google partnership would provide checking accounts tied to Google Pay accounts, with backup support from a credit-rating agency. This initiative could be launched in 2020. Citi's checking accounts are typically fee-based, with charges payable for overdrafts, and for withdrawals from non-Citi ATMs. Google may opt that model. On Citi's part, gaining access to Google's massive user-base makes the partnership an attractive proposition.

However, even if the bank accounts are fee-based, Google is unlikely to be interested in just generating some revenue from consumers. This would be small change for the company, which had over $136 billion in global revenues in 2018. The real area of interest would be the new data generated in a banking operation. When consumers are paid, how much they spend on discretionary purchases, where they spend it, and so on - these are the sorts of information Google would become privy to as a banking service provider. It could potentially tie the new information fields to data it already possesses about the search practices of users, their video-watching habits, reading and musical tastes, e-mail usage, video-calling patterns, and the ads they watch.

This would enable the creation of a formidably complete profile of users, which could enable the company to micro-target consumers in multiple ways. Would Google share that data with other companies? Would it use that data to drive some new initiatives of its own? Obviously, these things are unclear. But consumers and the regulatory authorities could justifiably be apprehensive about one private company gaining access to so much information about so many individuals. Questions may also arise about the storage and security of any such data, and the privacy laws that would be applicable. This is over and above regulators wanting compliance with local KYC and regulations.

The Reserve Bank of India (RBI), for instance, wants financial service providers to store data pertaining to Indian citizens on servers located within the country. The EU has also started thinking about data localisation. Google Pay has agreed in principle to comply with the RBI's data localisation rules but it has not done so yet, even though the rules were announced about a year ago. All this means that there is a trust deficit where many consumers are concerned. There are over 5.5 billion searches on Google every day, and 1.4 billion Gmail accounts in operation. Indeed, there are over 100 million users of Google Pay across the world. But many of those users may not be comfortable with Google having access to sensitive financial data as well. And regulators certainly need to review Google's plans carefully, given the chance that something could go very wrong.

India and its Brics dilemmas

The five-country group faces challenges arising from bilateral differences and diverse political systems

PHOTO: PTI

Prime Minister Narendra Modi (second from right) with, from left to right, Chinese President Xi Jinping, Russian President Vladimir Putin, Brazilian President Jair Bolsonaro and South African President Cyril Ramaphosa at the 11th BRICS emerging economies summit in Brasilia, Brazil

HARSH V PANT & RAJ KUMAR SHARMA

The 11th BRICS summit concluded in Brazil on Friday with customary calls for strengthening multilateralism and reforming global institutions such as the UN Security Council (UNSC), World Trade Organisation, World Bank (WB) and International Monetary Fund (IMF). Initially, BRICS mainly had an economic agenda but gradually, the scope has widened to include security, health, science and technology, culture and civil society. Under the chairmanship of Brazil, more than a hundred meetings relating to BRICS were held in 2019.

From an Indian perspective, two major developments happened at the summit. One, the grouping decided to open a regional office of the New Development Bank (NDB) in India. This hopefully will give impetus to financing of projects in India's priority areas. Second, terrorism was one of the priority areas for BRICS 2019, set by Brazilian President Jair Bolsonaro. The BRICS joint working group on counter-terrorism decided to constitute five sub working groups — one each focusing on terrorist financing, use of the internet for terrorist purposes, countering radicalisation, the issue of foreign terrorist fighters, and capacity-building.

In 2012, India, as the chair of BRICS, introduced security on the agenda, as the theme of the New Delhi summit was "BRICS Partnership for Global Stability, Security and Prosperity". Terrorism is now a key concern of all member states, and India made good use of this opportunity as Prime Minister Narendra Modi highlighted the fact that the world loses $1 trillion due to terrorism each year. India has been facing state-sponsored cross-border terrorism from Pakistan for decades now but in BRICS, China has been shielding Pakistan and has been uneasy discussing the issue of terrorism on this platform. India hopes to continue to work with other BRICS countries to reach an understanding with China on the issue of cross-border terrorism.

Overall, while the BRICS grouping may have completed a decade, it continues to face the challenges of the lack of a binding ideology, bilateral differences, diversity in terms of socio-cultural and political systems, and China's overwhelming presence, which reduces the space for other countries in the grouping. Given these challenges, New Delhi's continuing engagement with BRICS has generated mixed responses.

As China rises and positions itself as the sole challenger to American hegemony, there is a growing discussion about the possible Kindleberger Trap, a situation where China may fail to provide global public goods like a clean environment and financial stability, despite being a superpower. Small countries have little incentive to contribute to global public goods and it is generally the responsibility of great powers to provide global governance. The idea of the Kindleberger Trap is also applicable to rising powers like India, which have global ambitions.

A close examination of India's record in BRICS reveals that New Delhi has used its membership to make a substantial contribution to the international financial architecture, while also making efforts to address glaring gaps in areas such as counter-terrorism, the fight against climate change and UNSC reform. India is not a free-rider in a system of global governance dominated by the West, and continues to provide a vision of global governance.

BRICS allows India to send out messages about its foreign policy priorities, underscoring its desire to be part of issue-based coalitions

India was the main BRICS country behind the establishment of the NDB and proposed the idea at the fourth BRICS summit in New Delhi. The NDB was established in 2014 with all five BRICS members contributing equal amounts of economic capital and having equal voting rights, with no provision of veto power. The NDB also intends to provide non-conditional financing, unlike the WB and IMF. This reflects true equality in a global financial institution, and the NDB attempts to rectify the North-South divide that exists in the governance of the WB and IMF to make it more inclusive.

While it might be tempting to position the NDB as a challenge to the West, New Delhi seeks reforms in global governance through BRICS and does not have an anti-West agenda. As External Affairs Minister S Jaishankar recently suggested, India could be viewed as a south-western power, a blend of the West and the developing world. Through BRICS, India seems to be mediating between the two identities.

India's efforts to seek changes in international financial governance through BRICS have been successful, as China also shares this objective with India. The story has been one of missed opportunity in areas like UNSC reform, counter-terrorism and the fight against climate change. BRICS may have raised the issue of UNSC reform but this is more declaratory in nature than a serious attempt to overhaul the UNSC. This reflects that BRICS is interested in selective reform of the system, as its members have developed vested interests in the existing system. That is why the grouping seeks to reform global financial governance but is divided over UNSC reform. On the issue of terrorism, India has tried to project its unique approach, in which New Delhi is not selective and does not differentiate between good terrorists and bad terrorists, since they all pose a threat to humanity.

Climate governance too has been highlighted as an area where BRICS members have a lot of potential to contribute, but so far, that has not happened. Russia has been ambivalent towards climate change and has recently joined the Paris Agreement. India has taken initiatives outside the grouping to project itself as a leader in the fight against climate change, such as the launch of the International Solar Alliance in 2015 with France. Apart from the global agenda, BRICS allows New Delhi to send out messages about its foreign policy priorities, underscoring its desire to be part of issue-based coalitions.

At a different level, BRICS membership elevates India's global profile. China may still not be interested in de-hyphenating India and Pakistan, but India's BRICS membership automatically de-hyphenates India and Pakistan, while it casts India and China as equals. So, even as challenges abound in the BRICS trajectory, the grouping will continue to be of some instrumental value to India in the years ahead.

Harsh V Pant is director research at Observer Research Foundation, New Delhi, and professor of International Relations, King's College London.

Raj Kumar Sharma is a consultant at Faculty of Political Science, IGNOU, New Delhi

How secure are social media messaging apps?

ATANU BISWAS

Did we think that our social media messaging devices are so safe that they cannot be hacked or snooped? If so, then we were silly. We now know that a bug in WhatsApp's audio call feature allowed hackers to install a commercial spyware of Israeli company NSO Group on Android and iOS phones just by calling the target.

No doubt, most messaging apps are not easy to crack. In an opinion piece in *The Daily Telegraph* in July 2017, the then UK Home Secretary Amber Rudd opined that "real people" are not really interested in security features that stop the government and criminals from reading their messages. Her claim has been called "dangerous and misleading" by many critics. However, the idea somehow persists.

This October, US Attorney General William Barr, acting US Homeland Security Secretary Kevin McAleenan, UK Home Secretary Priti Patel and Australia's minister for home affairs, Peter Dutton, co-signed an open letter to Facebook, urging it to halt its plan to roll out end-to-end encryption across its suite of messaging products. Such demands, however, completely ignore the choices of billions of "real people" who are present and future users of such messaging apps. And, the recent outrage following the episode involving the spyware Pegasus shows that real people do care about their security.

'Encryption' has become a buzzword that is widely used to emphasise the security of messaging apps and attract more users

In April 2016, the Facebook-owned messaging service, WhatsApp, rolled out end-to-end encryption across all devices supporting the platforms: "WhatsApp's end-to-end encryption ensures only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp." This is because all messages are secured with a lock, and only the recipient and sender have the special key needed to unlock and read them. But, that security is certainly not absolute. And Pegasus has also exposed WhatApp's limitations around its end-to-end encryption. If the spyware is installed, it can access the targeted users' private data, including passwords, contact lists, calendar events, text messages, and live voice calls from popular mobile messaging apps.

Interestingly, "end-to-end" encryption has become a buzzword which is now widely used to emphasise the security of any such product, mostly to make it more attractive to users — so much so that common people tend to believe that the encryption between the two "ends" is simply unbreakable. Is end-to-end encryption a magic bullet for security?

Certainly, some messaging apps encrypt messages between the user and them. However, aren't most encryptions end-to-end? Still, they are always vulnerable at the two ends, as is clear from the Pegasus episode. In addition, who says that they're 100 per cent secured in-between? We know the encrypted message is scrambled. But, is it impossible for an interceptor to decode it? Do we think that cryptography systems are based on mathematical problems so complex that they cannot be solved without a key? Certainly not. A classic example was British mathematician Alan Turing's cracking, during the Second World War, of Enigma, an enciphering machine used by the German armed forces to send messages securely, by changing the cipher system daily.

The security of the encrypted message no doubt depends on the strength of the encryption, and the computing power and efficiency of the interceptor. With more and more powerful computers, and quantum computers around the corner, encrypted messages using standard encryption methods are bound to become increasingly vulnerable. Also, one must keep in mind that the proof of security of the encryption algorithms is often based on several "assumptions", whose validity is never tested. Overall, an end-to-end encryption maybe sufficiently secured, but its not a panacea. All digital messages in social media can be hacked, even if they are deleted. Almost everything connected to the internet is at risk of cyberattacks.

There are other vulnerabilities; for example, WhatsApp offers the option to back up chats to Google Drive or iCloud, but those back-up copies are not protected by end-to-end encryption.

WhatsApp, with over 1.5 billion users worldwide, including 400 million in India, might be most vulnerable due to its large user base. What about other messaging apps such as Signal, iMessage, GroupMe, Viber, LINE and Telegram? Most of them are also encrypted end-to-end, but complete security is possibly a hypothetical and non-existent state in cryptology. LINE is incredibly popular in East Asia. This writer has seen a 2018 article by two Japanese researchers on breaking the message integrity of an end-to-end encryption scheme of LINE.

Telegram has been widely used by the Hong Kong protestors to organise protests while hiding their identities. A few months ago, a group of Hong Kong engineers observed that a feature in Telegram's design might have allowed mainland Chinese or Hong Kong authorities to learn the real identities of users. Telegram tried to fix this bug to allow users to disable identity matching by phone number.

Cyber-security is often a game of cat and mouse. In fact, two major directions of research in cryptology are breaking the available security, and devising more efficient security. If "non-breakable" security can at all be devised, that will be the end of cryptology, indeed!

However, security is just a belief. It is better to understand this, and act accordingly. One of my cryptologist friends believes that an app or an encryption is safe as long as it is not hacked or snooped. I disagree. I think that safety is ensured until we know that it has been hacked or snooped.

The quest for devising more secure encryption and stronger security, however, continues.

The writer is professor of statistics, Indian Statistical Institute, Kolkata

OTHER VIEWS

RBI must address slowdown, even as inflation rises

It should frontload rate cuts in its December monetary policy review

The Monetary Policy Committee of the Reserve Bank of India is scheduled to meet in the first week of December. With various economic indicators indicating that growth has slowed down considerably over the past few months, the consensus so far has been that the MPC will cut the benchmark repo rate for the sixth straight time in December, bringing it below 5 per cent. But the sharper than expected spike in headline retail inflation in October has complicated the policy choices before the MPC. Data from the National Statistics Office shows that headline retail inflation edged up to 4.62 per cent in October, up from 3.99 per cent in September, largely on the back of higher food inflation. Core inflation, which is essentially inflation excluding food and fuel, has moderated further, however, signaling continued weakness in demand.

In its last policy review, the RBI had lowered its estimate for growth this year to 6.1 per cent, down from its earlier assessment of 6.9 per cent. But there is little possibility of the RBI's projections materialising, as various high frequency indicators suggest that growth is likely to fall below 5 per cent in the second quarter. So, while the MPC should carefully assess the trajectory of food inflation, its primary concern should be to

arrest the slowdown. It should frontload the rate cuts in its December policy, though the magnitude of the cut will depend on the extent to which growth deviates from the RBI's own projection.

The Indian Express, November 15

SC ruling on RTI is welcome

Paves way for greater transparency

The welcome ruling by a five-member Constitution Bench of the Supreme Court that the office of the Chief Justice of India is a "public authority" under the RTI Act, as much as the apex court itself, now enables the disclosure of information such as the judges' personal assets. The judgment's majority opinion, written by Justice Sanjiv Khanna, emphasised the need for transparency and accountability and that "disclosure is a facet of public interest". The Bench unanimously argued that the right to know under the RTI Act was not absolute and this had to be balanced with the right of privacy of judges.

The RTI Act is a strong weapon that enhances accountability, citizen activism and, consequently, participative democracy, even if its implementation has come under strain in recent years due mainly to the Central government's apathy and disregard for the nuts and bolts of the Act. Yet, despite this, the Supreme Court judgment paves the way for greater transparency and could now impinge upon issues such as disclosure, under the RTI Act, by other institutions such as registered political parties. This is vital as political party financing is a murky area today, marked by opacity and exacerbated by the issue of electoral bonds, precluding citizens from being fully informed on sources of party incomes.

The Hindu, November 15

Media has right to criticise

Criticism and defamation are different

Freedom of the press — the Tebbit test of a democracy — had not been specifically mentioned in Section 19(1) of the Constitution but that may only be because BR Ambedkar, one of the architects of the Constitution, believed that the media's right to air their opinion is concomitant with the right of the citizens to express themselves freely and fearlessly. The minders of New India have let Ambedkar down in this respect as well. Andhra Pradesh, which has elected YS Jaganmohan Reddy's YSR Congress to power, has given its nod to an earlier provision that empowers secretaries of government departments to file complaints against the media for publishing defamatory news. Ambiguities exist in the interpretation of defamation: Thin-skinned governments are ever willing to blur the line between legitimate criticism and defamation in a bid to stifle dissent. The media's right to be critical of a government or a specific department should be absolute in a democratic system of governance. Moreover, statutes exist to restrain the press from indulging in vendetta.

The media as an institution has also been complicit in its own undoing. One of the reasons being attributed to Mr Reddy's excess is that the media in Andhra Pradesh has, for long, been divided on the basis of political allegiances. Fairness must be integral to the media's conduct.

The Telegraph, November 15