Article Title:"Data privacy needs much better safeguards"

This article was published in 'The Asian Age' on 17th March 2017.

Shortlink https://goo.gl/cINlgZ

Improving our "Ease of Doing Business" rank has been on the cards for some time and as a part of that a conscious effort to haul everyone on a digital platform is being made. Last October, India was reportedly hit by its largest financial data breach which affected nearly 32 lakh debit cards across 19 banks, highlighting the concerns of many who have been questioning data security. In the past few years, the urban citizen has progressively taken to application-based services, online shopping and e-payments. A measure of this growth is the increase in mobile wallet transactions from `10 billion in 2012-13 to more than `490 billion in 2015-16.

The economy had been steadily moving towards online transactions but with demonetisation, there was a significant surge. The reduction in cash circulation resulted in a sudden dependency on digital options for all sections of society. Frequent usage of digital options peaked. BHIM was launched to make cashless transactions more accessible and has crossed 17 million downloads already.

Online transactions are merely an aspect of the larger Digital India campaign. Recently, the government has announced that after April 1, 2017, below poverty line families will not be provided monthly rations if they fail to link their Aadhaar number with the food and civil supplies department. Evidently, a digital approach to governance is on the agenda with initiatives such as Bharat Net, Digi-Locker and the Digital India platform.

This will certainly eliminate duplication of benefits and reduce costs for verification drastically. With ready availability of transactions history as well as credit worthiness, it will integrate individuals and SMEs with a larger variety of creditors and increase bargaining power.

The benefits of such governance are being recognised widely with successful examples of direct bank transfers possibly paving the way for Universal Basic Income soon. But there are certain risks to this approach, which are not as frequently discussed. There are polarised views for and against moving towards digital governance altogether. The use of Aadhaar for authentication, payments, creation of a national repository for documents through digi-locker, among others, are viewed by some with scepticism. The concern of groups opposed to it seems to be that digitisation is being "force-fed" to the masses without proper infrastructure and despite privacy concerns. They fear that availability of personal data with the government will make it unsecure and enhance surveillance.

Though these concerns have some merit, it is unfair to demonise Aadhaar. The growth of a digital citizen is a joint result of increased Internet access, e-commerce and social media. Data brokerage and misuse is a risky byproduct of the same. Absent Without

Aadhaar, there is still ample information available with private parties like Google, Facebook, Amazon, E-bay, Flipkart, etc. Recent reports have boldly claimed that data brokers are selling personal data such as age, marital status, residential address, phone numbers, purchase history and income profiles for dirt cheap prices. Technological advances have made it possible to track a person's location, profile their preferences and transactions. In 2015, the minister for communications and information technology said in a written reply to the Lok Sabha that on an average 5,000 interception orders are passed every month. That year India was ranked the second most intrusive country by Google in terms of requests for data on users. Perhaps, a better outcome would require defining the rights and liabilities of digital citizens, private players and boosting digital governance.

The present system suffers from four thematic flaws. First, the contours of privacy are not clear. Globally, the right to privacy is recognised by the Universal Declaration of Human Rights 1948, of which India is a signatory. In 2016, the UN General Assembly passed a resolution acknowledging human rights on the Internet, including privacy. The Indian Constitution does not explicitly guarantee the right to privacy, and this remains a subject of debate. Though the Supreme Court has in earlier decisions provided a limited right to privacy, the question of whether it is a fundamental right is sub-judice. Turning the clock back a few years, Western citizens conceded their privacy rights to traffic authorities by allowing surveillance through traffic cameras. Today, with the advancement of technology, the information collected by these cameras is filtered through anthropological and criminological research-based algorithms to provide information about possible hotspots for crime. This tool of predictive policing helps in better allocation of resources. Similarly, in India, the digital citizen has to acknowledge that issues of national security and prospects of better governance in some cases form a limitation to the right to privacy. Finding the right balance is crucial.

Second, the Indian scenario is plagued by overlapping legislation governing this area which are outdated and vague. Interception of data can be allowed under three separate laws — the Indian Post Office Act 1898, Indian Telegraph Act 1885 and Information Technology Act 2000. It is odd that WhatsApp messages today can possibly be intercepted through powers granted by the first two laws as well, which were drafted long before such a concept was even conceivable.

Third, the threshold and manner of interception are suspect on account. Absence of a positive right to privacy and data protection coupled with a widely couched power to intercept any data leads to legitimate apprehension. Surveillance in the United States, albeit controversial, has a more scientific approach with bulk collection of metadata, use of algorithms analysing patterns and the requirement to obtain warrants upon probable cause to listen to a phone call or read emails. In India, critics say the power to intercept for "investigation of any offence" could well be stretched to apply to a situation where a possible traffic violation is being investigated. There is no comprehensive list of "intercepting agencies" and their scope available in the public domain. Orders on surveillance requests by intercepting agencies are required to be granted by the Union home secretary or a state home secretary in a time-bound manner. No standard procedure is in place for exchange of relevant information between intercepting authorities. Systems like the Central Monitoring System (CMS) and Network Traffic

Analysis (NETRA) used for surveillance are established by executive process and the review of surveillance orders is also through an executive process. Checks and balances, which form the core of any democratic process, are absent here. Given the quantum of interception orders handed out monthly, a team within the home ministry can specifically look at this aspect and be subject directly to parliamentary review.

Lastly, the vulnerability of data is a core concern. This debate is overshadowed by apprehensions that Aadhaar data, stored through private players, may be susceptible to theft and misappropriation during transmission and private players will shrug off responsibility thereafter. Again, these concerns go beyond Aadhaar, personal data and usage patterns are exchanged commercially to feed into advertisements or articles that we see online. An absolute restriction on these would make unviable the modern economy as we know it. It would be prudent to mandate maintenance of basic security protocols by all private players, restrict exchange of data without proper consent, make it mandatory to inform the end user in case of a breach and a redressal mechanism for this.

Maintenance of Aadhaar data, being sensitive personal information, can be held to a higher standard of accountability. It’s a fool’s errand to resist digital advancements or deny big data’s underbelly. Better governance through digitisation isn’t some evil design. It’s the next stop in our current growth trajectory. However, it must be accompanied by guaranteeing the digital citizen’s right to privacy, ensuring best efforts of data security and narrowly defining the exception of surveillance.