A GROWING UNEASE: DATA DILEMMAS OF THE CONNECTED INDIAN

by Geeta Lobo, Anthony Dsouza and Piyush Dixit I October 2020

IPSOS BRIEFING
INDIA

GAME CHANGERS

Ipsos

OVERVIEW

In this paper, we examine the attitudes of the digital Indian to sharing data. We start by looking at the affinity Indians have for digital technology, their salient data anxieties and the conflicting mindset this creates.

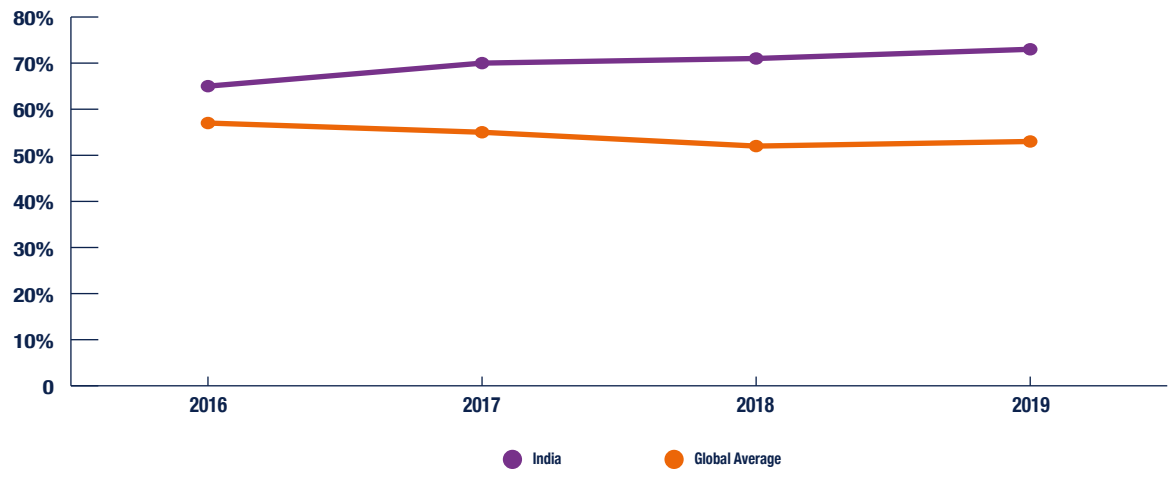
We have also highlighted the implications of this mindset for brands, especially those which offer digital services.

GROWING ANXIETY

Research has shown that there are between sixty to ninety apps installed on the average Indian smartphone[1] and this number is constantly on the rise. When we download an app, usually we allow access to our contact list, messages, picture galleries and messenger images. Our shared data, however, does not just stop there. There is a lot of passive information accessible to the app providers. We could also be sharing our exact location at any given point - our residence location or our frequent haunts - and maybe even some sensitive financial details.

Permissions by themselves may be harmless and even useful in providing users with a good experience. However, not all of this data is in our control, much of it is not even in our possession. There is an increasing recognition of the power of this data and growing anxiety about its misuse. In a connected world, this data becomes a ready resource to be harnessed for furthering the objectives of those who control it. This often comes at the cost of the individual who not just risks material loss but can face a loss of privacy, autonomy and even identity. Data anxiety is the worry of losing control and possession of data which is critical and confidential as we work our way through the connected world.

Figure 1 How concerned are you about your online privacy compared to one year ago? (% saying they are concerned)



Source: 2019 CIGI-Ipsos Global Survey, Internet Security and Trust

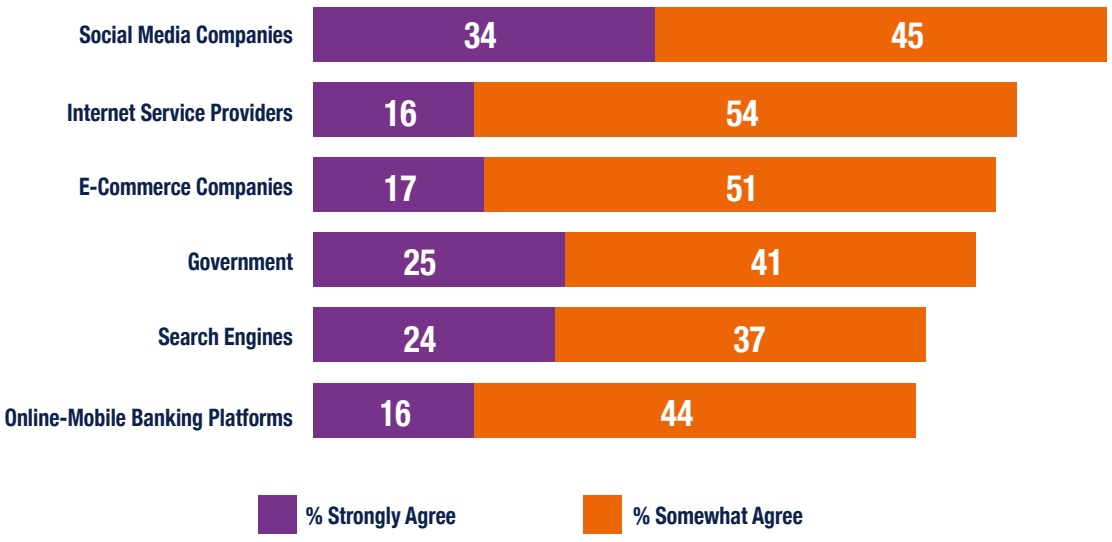
In mature markets the biggest concerns are about loss of privacy and autonomy. The digital trace left behind online can be leveraged to influence opinion, choices and behaviour. These concerns have led to regulations and safeguards such as GDPR[2] coming into force in the EU. In India, though the awareness and knowledge of the hazards are limited, anxiety about becoming data theft victims is rising. A recent Ipsos survey[3] of attitudes to internet security and trust reveals that the concerns of online privacy among Indians is very high and growing. The proportion of those who are concerned over online privacy has risen from 65% in 2016 to 73% in 2019.

THE SOCIAL MEDIA DILEMMA

People are particularly distrustful of social media platforms compared to other players. Banks and financial services are trusted more because they are believed to have stringent security systems and policies towards ensuring data protection. Privacy, though a concern, is still not a barrier to entering the digital world as is evident from the rapidly growing base for social media platforms. Social media users in India have more than doubled in the last five years, growing from 168 million in 2016 to 376 million in 2020.[4]

People are willing to continue using them, hoping that necessary action will be taken by the platforms in future to ensure data privacy. Incidents like the Facebook-Cambridge Analytica data scandal have not made it easy either, raising a disturbing concern for many that their personal data is not safe and cannot be trusted with big companies.

Figure 2 To what extent do the following contribute to your distrust in the internet?



Source: 2019 CIGI-Ipsos Global Survey, Internet Security and Trust (perception among Indians)

FEARS OF FINANCIAL FRAUD

Though banks and financial institutions are well regarded when it comes to data protection, there is still considerable anxiety about the potential of a material loss. This includes worries about theft of critical financial information while conducting cashless transactions, especially online. Indians have always been wary of financial technology, be it credit card transactions or online banking. Part of this is due to the history of financial data[5] theft, be it phishing, data skimming from ATMs or credit card fraud. Indians' innate discomfort with online financial transactions is evident from the fact that, in India, E-Commerce grew sharply only after Cash-on-Delivery (CoD) was extended as a payment option. In India, for nearly 80% of online shoppers, CoD is still the preferred mode of transaction, compared to 23% globally.[6] In fact, close to 95% of transactions in India are cash transactions.

BIG BROTHER COMPLEX

"No one likes to see a government folder with their name on it"- Stephen King's quote seems apt to explain the growing anxiety in India with sharing information. The extensive data collection and data integration that the state is undertaking is a great source of unease. Though reliable data is the critical foundation for e-governance and efficient implementation of many welfare schemes, the growing appetite that the Indian state has shown for its citizens' data is now causing serious concerns. Any attempts to gather sensitive information from the population at large is always a contentious issue. Caste information collected in the population census or the National Population Register (NPR) are all data gathering exercises which have been controversial. The worries in this context go beyond concerns about privacy. The most salient concerns are about constant vigilance, loss of liberty and even extend to identity loss with exercises like NPR. This was also evident in the recent 'Aarogya Setu' fiasco.[7] This contact tracing app sponsored by the Indian government had few takers, until it was made mandatory for anyone resuming work from an office and those living within a COVID-19 containment zone. The government later had to step down from this stringent stance and roll back to merely recommending the use of the app – once the concerns over privacy and possible misuse of banked data reached a crescendo.

The current data protection laws in India are very narrow. The IT Act 2000 does not address the need for a stringent data protection law being in place. It only contains a provision regarding cyber and related IT laws in India and delineates the scope of access that a party may have. The IT Act and the Personal Data Protection Bill, which were introduced in Parliament in 2006, are yet to see the light of day. In fact, recently proposed legislation meant to protect data rights, the Data Privacy Act 2019, while regulating use of data by private players gives the government wide ranging powers to exempt its agencies for reasons of national security or law & order. The integration of the citizen's biometric identity data with other data such as transactions, communications or location data potentially creates a powerful database which could get misused to infringe on citizens' liberty. Though there are no salient cases of misuse, other than alleged tapping of conversations of political opponents, the possibilities itself create a lot of anxiety. To add to the worries, the recent reports of a data breach at the Unique Identification Authority of India (UIDAI)[8], which holds sensitive biometric data of the population at large, have raised concerns about the security of such data and misuse by unauthorised elements.

UNEASY TIMES AHEAD

Ironically though, Indians can be expected to become increasingly data conscious in the years ahead, partly due to various legislation aimed at protecting the data rights of citizens.[9] Even the wider base of Indians who may have otherwise been willing to blithely give up their data to private players, in return for attractive digital services, cheaper data access and a wide array of convenient solutions, will likely become more aware and vigilant.

The proposed legislations for securing citizens' data rights will curtail the powers of private players. There are guidelines in the Data Protection bill about the procuring, processing and retention or storage of such data. Already, localisation of what is deemed to be sensitive data has posed challenges for large telecom and technology players. For example, the central bank in India, the Reserve Bank of India (RBI), requires payment data of Indians to be stored exclusively on local servers. This has led some global players including Mastercard, Visa, PayPal, Google and Amazon to push for some relaxation.

These regulations will also limit the extent to which data analytics can be used to inform marketing and communication for brands.

Stronger regulations and legislations that protect citizens' rights to their own data can quell some of this anxiety. But many of these conflicts could also put citizens and the state on opposing sides of the table. On the whole, growing awareness and data consciousness in the coming years can be expected to strengthen anxiety about sharing data both in India and across the world. Deployment of advanced technology based on artificial intelligence is likely to fuel this insecurity further.

DATA RESPONSIBILITY – THE NEW MANTRA FOR BRANDS

The impact of this trend on the BFSI (banking, financial services and insurance) sector is self-evident. In India, concerns of data security especially the need for secure transactions could dampen adoption of digital financial services. For brands across sectors, personalisation and targeted promotions will likely be impacted. It could also significantly influence the nature of participation in social media platforms.

Brands will now be expected to demonstrate that they are 'data responsible' to remain trustworthy, and this is particularly critical for technology brands.

Digital technologies have profoundly changed the way in which we do business, shop, work and live. In today's digitally transformed and connected world, data is produced in vast streams daily, at a mind-boggling volume and pace. Not surprisingly, a heightened focus on providing privacy to the consumer and protecting their data has become of paramount importance.

REFERENCES

1. https://economictimes.indiatimes.com/magazines/panache/indians-spend-roughly-3-hours-a-day-on-smartphones-but-are-they-paying-big-bucks-for-apps/articleshow/62866875.cms
2. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/
3. https://www.ipsos.com/en/2019-cigi-ipsos-global-survey-internet-security-and-trust
4. https://www.statista.com/statistics/278407/number-of-social-network-users-in-india/
5. https://economictimes.indiatimes.com/tech/internet/data-breach-incidents-in-india-higher-than-global-average/articleshow/65107118.cms
6. https://www.statista.com/statistics/508988/preferred-payment-methods-of-online-shoppers-worldwide/
7. https://www.livemint.com/industry/infotech/why-privacy-advocates-have-concerns-over-aarogya-setu-app-11588509094177.html
8. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/
9. https://economictimes.indiatimes.com/news/economy/policy/personal-data-protection-bill-exemptions-for-government-agencies-worry-experts/articleshow/72465610.cms?from=mdr and https://dataprivacymanager.net/7-data-privacy-trends-for-2020/

BRIEFING
INDIA

Geeta Lobo Executive Director, Social Intelligence Analytics, Ipsos in India

Anthony Dsouza Executive Director, Innovation, Ipsos in India

Piyush Dixit Research Director, Brand Health Tracking, Ipsos in India

The **Ipsos Briefing** papers
are produced by the
Ipsos Knowledge Centre.

www.ipsos.com
@Ipsos

GAME CHANGERS