



The line between providing government services like Google predicts your next possible search comes at a huge trade-off. Clearly, the line between a techno-utopia and a surveillance dystopia can be really thin. India needs a proper data protection law drafted carefully drafted with due consultations with stakeholders.

**By Osama Manzar**

Let's start by running down some numbers. It is a fact that India is both, one of the most connected countries and one of the most unconnected countries. For example, internet users do not number more than 700 million of India's population of 1.35 billion. Of these, only 300 million people use the internet regularly; the rest are either token users or, as is called, not 'habitual users'. Another perspective on internet uses in India is that about 800 million people live in rural areas, and smartphone penetration in rural India is not more than 300 million. It is not contested that a smartphone is one of the more apt device to use the internet for any purpose. Therefore, in terms of sheer numbers and scale of availability of digital Infrastructure, at least 700 million Indians do not have any digital infrastructure or digital means to conduct any work online.

Discover more

[science](#)

[Scientific](#)

[Science](#)

Yet, every Indian citizen, connected or unconnected, private or public, poor or rich, employed or unemployed, man, woman or any gender, has a digital identity, a digital footprint, or a digital stamp of sorts. In other words, the government in India has a right/willingness/aspiration/authority to 'digitalise' you, the citizen. But it also does not want to give the citizen a right over their data or privacy or a simple digital right.

Let's break this down in the light of two developments – the country's Unique Identification (UID) system called the Aadhaar, and the personal data protection laws. Claiming to be a welfare-guaranteeing project that planned to identify citizens to weed out loopholes and welfare 'leaks,' the Aadhaar and the authority issuing it, the UIDAI, claimed to fight corruption and increase inclusion. On that pretext, huge amounts of data on a billion-plus citizens were collected and stored – including detailed biometric data. Unlike the US' welfare programme like the Social Security Number, the Aadhaar works to uniquely identify anyone with this collected data.

- Advertisement -

Discover more

[Scientific](#)

[Science](#)

[science](#)

### **EU exemplifies regulation**

The first issue has to do with what we started with – that India is grossly under-connected (at least half the country does not have internet access). This means that there are still thousands of people who either have no way to make an Aadhaar, or are not aware of the welfare schemes that they ought to be entitled to, or can apply for these schemes.

Another issue is that this collected data is stored centrally by the agency, and until very recently, other than activists' flagging issues, there was little awareness on what exactly could go wrong. In the last couple of years, there have been several reports of data breaches and leaks exposing information pertaining to crores of people to malicious attackers. This is reportedly also one of the largest such breaches in the history of the internet.

Discover more

[science](#)

[Science](#)

[Scientific](#)

This is where the importance of a data protection law comes in. The European Union, for example, has a fairly tight regulation on how data is being collected, stored and used. It is called the GDPR, and by invoking the privacy law and of human rights law from Article 8 of the Charter of Fundamental Rights of the European Union, it is a model on how to frame such legislation.

How? Both, India's government and the private sector seemingly have the right to digitalise the citizen and his/her data. However, the citizen does not have the right or privilege to ask a question pertaining to this data. Like, "how is the data that is being collected/taken/recorded from me being used? Is the data collected about me private? Is it in 'safe' hands? Will my privacy be secure? Does the data stay sovereign?"

### **Techno-utopia or surveillance dystopia?**

To briefly explain the people's lost digital rights or right to privacy and data in the light of "Right to Information", "Right to Food", "Right to Education", "Right to Health", and "Right to Shelter". All these are fundamental rights and pretty much human rights. Now, Aadhaar has been at the forefront of a lot of exclusions from these very rights. There have, of course, been reports of such exclusions. Digital and human rights activists have documented many of them.

Discover more

[Science](#)

[Scientific](#)

[science](#)

Linking Aadhaar to all this data intends to create a system of 'real-time governance,' which along with the 360-degree profiling would track people in real-time across databases of birth, death, healthcare, vehicle registration, ownership of land or properties, and even policing. The line between providing government services like Google predicts your next possible search comes at a huge trade-off. Clearly, the line between a techno-utopia and a surveillance dystopia can be really thin.

At DEF, our work has been primarily to empower marginalised communities by enabling them with digital access and literacy. This opens up several avenues for their upliftment.

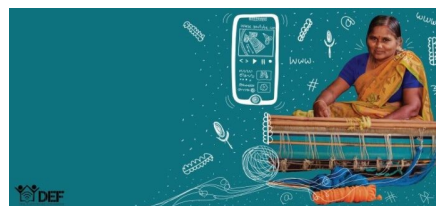
Simultaneously, they are also able to avail several of the welfare schemes the government has been promising them. DEF has helped set up several Community Information Resource Centres (CIRCs), which are digital data houses, or ICT hubs, where members of the rural community gather to meet their digital needs in education, health, livelihood, public service delivery. Our CIRCs also double up as points of internet delivery through community networks.

Discover more

[Science](#)

[Scientific](#)

[science](#)



### **Aadhaar. Data. Hunger**

However, the point is this: On one side, there is the fact that Aadhaar has been leading to exclusions, and centrally stored data is vulnerable to breaches. However, at the same time, there is a need to work to empower communities by enabling them to get access to both digital tools and the documentations required for them to get the minimum entitlements the government provides. Aadhaar is presently demanded for almost everything. For housing welfare-related schemes, the government requires both Aadhaar, and also geo-tagged locations to track building progress and follow up for fund disbursement.

Likewise, Aadhaar has been linked to most other welfare schemes, to connect bank accounts to get basic pensions or cooking gas subsidies. There have been most infamously, reports of starvation deaths following Aadhaar authentication failures leading to inability in obtaining rations. The same applied to admissions, and even mid-day meals that were given in schools. When schools were closed due to the COVID-19 pandemic, there were long queues of students in front of kiosks to withdraw the mid-day meal equivalent of cash subsidy given to students of rural schools.

Discover more

[Science](#)

[Scientific](#)

[science](#)

Let us look at this from another lens. The 2021 Global Hunger Index ranks India at 101 among 116 countries. As a reminder, in conservative estimates, a staggering 900 million of the country's population depends on the Public Distribution System for foodgrains, and 120 million children in over 1.27 million schools depend on the mid-day meal schemes. If it were not for these entitlements, India's position on the Global Hunger Index would be further alarming.

### **Commoditising personal data**

Added with the problems of exclusion are the mentioned issues of data privacy and protection. By forcing people to link their identities with Aadhaars, and openly calling to monetize data, the government is opening up personal data as a commodity without doing the primary safeguards needed. People are coerced into giving data, and have no idea why their data is being collected or how they will be used. While the idea of an OpenData platform to let the public access of shareable data is a boon to research, the notion of commercially opening up private data before proper mechanisms are in place cannot be viewed similarly.

Discover more

[science](#)

[Science](#)

[Scientific](#)

What we need is a proper data protection law, one drafted not on the government's whims to bring in ways to monetize public data and exclude people, but one carefully drafted with due consultations with stakeholders. Data laws need to be rethought – more on the line of how we drew up the RTI laws (before amendments diluted it!). Just like we have a movement that is demanding the continuity to the RTI (like the Jawabdehi Campaign for Social Accountability), we need a ground-up call to design data rights such that it benefits communities and not commodities.

The internet, and ensuring digital access to more marginal communities is an important part of the puzzle to effectively address issues of education, sanitation, gender, health, and rights and more. But in doing this, we must ensure that there are neither any exclusions due to lack of infrastructure and access, nor are there shortcomings in safeguarding people's data.

**Citizen coerced to part with data**

The biggest challenge of Indian society is that digital tools, digital media, and diverse digital platforms are being adopted rapidly, and assuming rapid pervasiveness of digital adaptability, both government and major digital platforms are pushing a no-alternative type system of offering all solutions via digital means. Insisting access to natural services and daily needs of lives via digital media and also making all policies assuming digital is the only means is leading to large scale digital exclusion, increasing the cost of seeking services, and constantly giving data that is asked or made mandatory without collateral accountability.

The situation of Indian citizens being pushed to the wall, and made to part with their data as a mandatory practice is nothing but treating, even coercing the population as if they are consumers without rights. Therefore, it is only natural that the masses need their digital rights, data rights, and digital human rights before they are asked for their data. Time is passing by – we needed the data and privacy law yesterday, we should keep fighting for it today.

*Osama Manzar is the founder and director of Digital Empowerment Foundation, a Senior Ashoka Fellow and also a member of the advisory committee for Digital Services at the National eGovernance Division (NeGD). He can be reached @osamamanzar*

*Image: Digital Empowerment Foundation.*

- Advertisement -

Discover more

[Science](#)

[science](#)

[Scientific](#)