THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

September 30, 2021

Digital ID: A Single Source of Truth

By: Kaushik Jayaram

The push worldwide to give everyone a legal identity was to allow people better access to financial and public services. But this endeavour has quickly morphed into promoting Digital IDs that are increasingly used for surveillance and control.

Sometime in January 2018, a policeman showed up at the door of a businessman in Telangana's Mahbubnagar district to record "his fingerprints, Aadhaar number, phone numbers, social media accounts, voter ID, passport, and the names and numbers of his family members, associates, lawyers, pawn brokers, and "concubines", if any," the *Hindustan Times* reported. The police were verifying this personal information as part of a survey to populate a crime-fighting software called TSCOP (Telangana State Cop).

The *Hindustan Times* report noted that TSCOP was part of "a largely unnoticed big data revolution sweeping across Indian states", where India's biometric Digital ID, Aadhaar is used to collect and consolidate comprehensive data on residents through State Resident Data Hubs (SRDHs). With no law or regulation on data privacy, this data was collected without consent and with no safeguards against misuse.

Without a trace of irony or self-awareness, the SRDHs proclaim themselves to be the "single source of truth" on residents. Unlike data in the Central Identities Data Repository (CIDR), which is reasonably protected and not shared without consent, the SRDHs use Aadhaar — introduced as a measure to efficiently deliver welfare services — to create a 360-degree view of a resident with no restrictions on usage or consent. The Aadhaar-enabled SRDH can be scaled up to include personal data, household information, linking of multiple identifications, voter ID, tax ID, passport, driving licence, locational information, and life events from birth, marriage, birth of children, and death. Every transgression of the individual, a traffic ticket, a credit default, or a court case, could become a permanent part of the profile. The state could conceivably construct an index of social behaviour for a citizen or a resident as in China [1].

A truly panoptic vision of a society is well within reach.

The push for a Digital ID

Project Pegasus might have exposed the seamy side of the digital world, of intrusive technology, spyware, and surveillance. Less noticed is the strong international push to promote digital identity (Digital ID), which has the potential for much wider surveillance and control over vast swathes of the population of the world.

> The push for a legal identity has seamlessly morphed into the need for Digital ID.

Enormous strides have been made in many countries in expanding the use of Digital ID, as part of a narrative of inevitability and technological progress. Around 161 countries have adopted digital ID in some shape or form, some at very nascent stages and several well advanced. Various international and national initiatives have pushed the idea of a universal Digital ID as a technological panacea to improve lives around the world. The focus of this push is the poor and marginalised populations in developing and less developed countries.

Lack of documentation to credibly establish one's identity is a formidable barrier to access financial and public services. Nearly a billion people, or one in seven persons on the planet, have no legal documentation to establish their identity. Another three billion have either inadequate identification or identification that is not sufficiently digital (World Bank 2018, a).

It would be no one's case to argue against the provision of such documentation. A legal identity, issued by a national or regional government, is a basic human right that enables an individual to participate more fully in the economic, political and social life of a country. With this reality, one of the targets of the United Nations' Sustainable Development Goals (SDGs) is to "provide legal identity for all, including birth registration" by 2030.

However, the push for a legal identity has seamlessly morphed into the need for Digital ID. Consortia of international organisations (the UN and the World Bank groups included), development banks, technological associations well as powerful well-funded private foundations[2], have lent considerable clout and influence for the development of a universal Digital ID solution.

> Digital ID, coupled with mobile and internet technologies, offers a highly flexible and cost-effective way of dramatically expanding the spread and reach of financial and payment services.

The apparently limitless benefits of digital technology and seamless integration into an interconnected global economy are powerful incentives.[3] Digital ID, coupled with mobile and internet technologies, offers a highly flexible and cost-effective way of dramatically expanding the spread and reach of financial and payment services[4]. Financial inclusion and access to financial services, education, health care, and other public services as well as welfare benefits including cash transfers, pensions and social security payments, can be directly targeted to the intended recipients without leakages and fraud.

Other claimed economic benefits include better employment and payroll records, improved access to labour markets, efficiencies in other sectors of the economy, agriculture, industry, trade and services, and a clampdown on tax evasion. A McKinsey study estimated that the economic potential of Digital ID would range between a 3% to 13% increase of GDP for a number of countries

Digital ID and mass surveillance

These are indeed substantial benefits from Digital IDs, although they arise primarily from having a legal identification. But Digital ID also enables focused and referential surveillance and monitoring in ways not previously possible with traditional IDs.

> Data privacy is a fundamental right of an individual in a democratic society and weakening it in any form is a slippery slope to the reality of a surveillance state.

The unique ID characteristics of Digital ID perform the function of connecting a record or a whole set of records across multiple databases. Once an individual is identified and tagged with a unique number or a key, it becomes possible to link every conceivable activity of that individual, from banking and financial transactions, payments, education, employment, health, familial and social connections to travel and leisure. In short, an individual's entire life cycle, from birth to death, and everything in between, can be tracked and monitored. It becomes much easier to move from generalised surveillance to monitoring specific individuals.

There are many who do not see this as harmful, "if we have nothing to hide why should we be worried", goes the argument. This gross oversimplification ignores the possibility that anyone can be caught in its web for any real or perceived transgression. As the Supreme Court of India said:

> The right of privacy is a fundamental right. It is a right which protects the inner sphere of the individual from interference from both State, and non-State actors and allows the individuals to make autonomous life choice

Data privacy is a fundamental right of an individual in a democratic society and weakening it in any form is a slippery slope to the reality of a surveillance state. Even nominally democratic regimes tend to abuse the power of surveillance. The Snowden disclosures revealed the scale of the surveillance in America. For an authoritarian regime, the opportunities are endless.

> Federated or decentralised IDs are generally the norm in many countries in Western Europe and North America, while highly centralised IDs are favoured by authoritarian regimes.

Digital ID, conceived as an essential vehicle of inclusion, could as easily be used for exclusion[5]. It can offer access to services and benefits in exchange for loyalty. It could also be used to exclude potential opponents, dissidents, ethnic minorities and other perceived or real enemies of the regime. From political manipulation of an electorate, and social control of particular groups, regimes not constrained by legal or political means, can employ well-targeted and effective ways of control through persuasion, deterrence, or coercion.

Not coincidentally, federated or decentralised IDs are generally the norm in many countries in Western Europe and North America[6], while highly centralised IDs are favoured by authoritarian regimes and among the developing and less developing economies.

Data analytics are also increasingly effective as tools of digital propaganda, whether to sell political messages or cosmetics, as suggested by the apparent success in psychological profiling by data firms such as Cambridge Analytica. However, as anyone who encountered customised digital ads is aware, a lot of its targeting is blunt and indiscriminate. Though the digital assault is relentless, its effectiveness can be overstated. Much of the digital noise, as with real ambient noise, can be ignored. Digital ID changes this dynamic in a fundamental and transformative way.

In metaphorical terms, Digital ID is the essential key to an electronic panopticon. The ability to observe and ultimately control individual behaviour has gone beyond Foucault's imagining[7]. Surveillance is both visible and unverifiable. It is visible because it is assumed to be true. But who is being observed is unverifiable until the consequences are visited directly upon that individual. Social control is better achieved in that state of uncertainty. For an authoritarian regime, it is more effective than overt coercion.

Perils of high modernism

James C Scott, suggested, that the grand projects of the state are often derived from a particular conception of social reordering, dubbed High Modernism. There are four elements to this social reordering, which can combine to transform well-meaning social projects into failures.

First, as proposals, these projects might be perfectly rational means to improve welfare and efficiency in society. Secondly, high modernist ideology sees technology as an infallible means of social progress. When these two elements are joined with a third, an authoritarian state, the combination becomes potentially lethal. And, finally, a prostrate civil society that lacks the will and capacity to resist. (Scott 1998)

> The idea for a verifiable identity got nowhere until private interests, software consortia and government officials made it out as a project to better deliver welfare schemes.

Scott's argument is useful in understanding a project like Aadhaar, India's biometric-based unique Digital ID scheme, which is the largest of its kind in the world with more than 1.2 billion enrolled in it. The original motivation reportedly came from a national security perspective in the wake of the Kargil conflict in 1999. There were calls for a verifiable identity amidst the reports of terrorists infiltrating and acquiring forged identity documents.

The high modernist ideology underlying this aspiration was reinforced by the convergence of interests of private organisations and the state. The idea for a verifiable identity got nowhere until private interests, software consortia and government officials made it out as a project to better deliver welfare schemes to the needy. The project was presented as an all-encompassing solution for various long-standing and complex socio-economic problems.

The imagination boggles at the faith and trust placed in technology and on technologists to design and implement a project of such magnitude. Considerations of data breaches, data privacy, or potential unintended consequences were blithely ignored or underplayed. Aadhaar was launched in 2009, without much public consultation, or a proper legal framework to manage the information, and to safeguard its privacy[8].

> The use or abuse of the data by the state is critically dependent on the nature and the extent of oversight by parliamentary or the judiciary in a country.

As the use of Aadhaar in the SRDHs show, despite assurances of minimal information gathering and data protection, this Digital ID becomes an effective enabler of mass surveillance technology.

Data privacy and protection

Privacy issues are foremost in sharing personal data in a digital format. The World Bank's high-level principles on Digital ID aim to provide a robust framework to protect data privacy. The European Union's general data protection regulation (GDPR) f 2016 is widely recognised as a global standard on data privacy and the use of the personal data of EU residents. The data owners have the right to consent, withdraw consent, to know what information is collected, and crucially to modify their personal data. Many countries have similar regulations or are in the process of developing them.

However, these regulations are largely in response to widespread commercial exploitation of personal data, with large exceptions carved out for the governments in the name of national security, terrorism, money laundering, drugs or other criminal activities. Neither the extant standards, regulations nor laws cover the type of systems that might best protect an individual's data from systemic abuse. The use or abuse of the data by the state is critically dependent on the nature and the extent of oversight by parliamentary or the judiciary in a country. Where such oversight is weak or suborned, there is no effective protection for the individual.

Conclusions

"On August 27th, the Taliban boasted of using US digital identity technology to hunt down Afghans who had worked with the international coalition. This poses a huge threat to all Afghans who are recorded in these identification systems, and should be a wake-up call to all those working on digital identity and digital public infrastructure for development."

As such instances show, transcending any cost-benefit calculations, it is a bedrock principle that an ID should be in the possession of its owner. Documents such as biometric passports, national ID, or a Digital wallet, may be acceptable as functional IDs which are used at the owner's discretion and consent and are not widely linked. A Digital wallet combines the advantage of a Digital ID with more robust safeguards, as the owner can control the nature of personal information to share. Digital ID, especially in a centralised system, violates this basic principle. More fundamentally, the nature of information linked to a Digital ID may never be known.

There is a sense that Digital ID is here to stay. Civil society can try to ring-fence its use as much as possible by questioning its essential premises. As well as judiciary and laws, public awareness and exposure of digital abuses are essential. A people's panopticon or open-source intelligence might be the answer to the state panopticon. Technology could be harnessed to fight technology.

Footnotes:

[1] In China, a citizen scorecard based on a system of social credit is reportedly used to black list law breakers or conversely incentivise good behaviour.

[2] These include Bill and Melinda Gates Foundation, Centre for Global Development, Mastercard, Secure Identity Alliance, Omidyar Network, among others.

[3]

See for example, Natarajan et al 2018; and the World Bank's principles for the development of robust and sustainable Digital ID systems .

[4] The worldwide digital population as of January 2021 is estimated around 4.66 billion, of which 92.6% use mobile devices for internet access.

[5] The role of government-issued ID was a particularly sensitive matter in the case of Rohingya Muslims. The Government of Myanmar used a National Verification Cared (NVC) to identify Rohingya as "foreigners" and would use the NVC based system allegedly for targeted persecution (TER 2020).

[6] The US recognises multiple IDs, including social security numbers, driving licences, and passports. In the United Kingdom, the existing national identity card for citizens and EEA nationals was scrapped in 2011under strong public pressure.

[7] Michel Foucault used Jeremy Bentham's panopticon, an architectural design of a prison/insane asylum, as a metaphor for controlling prisoners through visible surveillance. Discipline is achieved not only by surveillance but also from the awareness of being under observation (Foucault 1991).

[8] The Aadhaar Act was passed in 2016. The Data Protection Bill 2018 is still languishing in a joint parliamentary committee.

References:

Foucault, Michel. 1991. *Discipline and punish: The birth of the Prison.* Translated by Alan Sheridan. New York: Vintage Books.

Natarajan,Harish, Appaya,Mandepanda Sharmista; Balasubramanian,Sriram. 2018. ' G20 Digital Identity Onboarding.' Working Paper. Washington DC: World Bank Group.

Scott, James C. 1998. *Seeing Like a State: How Certain Schemes to Improve the Human condition have Failed.* New Haven: Yale University Press.

TER (The Engine Room). 2020. *Understanding the Lived Effects of Digital ID, A Multi-Country Study*.