THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

February 8, 2024

Digi Yatra: Service or Surveillance?

By: Disha Verma

Worries about privacy, surveillance, & unfair exclusions have been raised about Digi Yatra, India's airport facial recognition system. They are amplified by disturbing reports of airport staff coercing & deceiving passengers to sign on. This raises serious questions about Digi Yatra's true purpose.

Alarm bells are ringing over Digi Yatra, India's airport facial recognition system. Privacy fears abound, fuelled by concerns about data misuse, excessive surveillance, and potential exclusion errors. Reports of passengers being coerced or misled into using it also heighten worries about opaque processes and accountability. With such a troubled rollout, questions are being raised about whether Digi Yatra truly serves or surveils.

Digi Yatra is an opt-in service at Indian airports launched by the Ministry of Civil Aviation on 8 June 2017 with the aim of making air travel "seamless, contact-less, hassle-free and paperless" for all passengers. The service enables digital processing of passengers at airports by using facial recognition technology (FRT) and Aadhaar-linked credentials to authenticate them instead of traditional boarding passes.

Digi Yatra Not Mandatory

The information furnished by the Ministry of Civil Aviation in response to Right to Information applications filed by the Internet Freedom Foundation in August 2023 states, "Digi Yatra gates exists in airports for passengers who voluntarily choose to use this facility (sic) … Digi Yatra is not mandatory. The other manual process e-gates continue to be available for passengers."

The Ministry's Digi Yatra Biometric Boarding System (DYBBS) Policy is also clear that "creation and use of the Digi Yatra ID Travel Credential by a passenger will be completely voluntary". Consent of passengers becomes paramount because Digi Yatra carries with it a number of privacy and surveillance concerns, and relies on technology that is not necessarily very accurate.

> [M]ere cognisance and reassurances being provided by Digi Yatra officials may not be enough, as the manner of its deployment in recent memory has likely created a trust deficit between the service and passengers.

More recently, concerns have been expressed about the unlawful and undignified manner in which Digi Yatra is being deployed at airports. Airline passengers across India are reportedly being ambushed and coerced by private airport personnel and security staff into signing on to the "voluntary" Digi Yatra service and scanning their faces at multiple airport check-points.

A recent Hindu report on a LocalCircles survey revealed that of 21,000 domestic passengers flying out of the Delhi Airport, 29% signed up for Digi Yatra without realising it, and only 15% used the service knowing "*the benefits it offered*."

This problematic manner of deployment has solicited responses from both Minister for Civil Aviation, Jyotiraditya Scindia (here) and Digi Yatra Foundation CEO, Suresh Khadakbhavi (here), who have noted the absence of passenger consent and claimed to undertake staff training to address the issue. Although, mere cognisance and reassurances being provided by Digi Yatra officials may not be enough, as the manner of its deployment in recent memory has likely created a trust deficit between the service and passengers. After these preliminary remedial measures are rolled out, there is a possibility that airports will soon revert to old tools of coercion, misdirection, and causing inconvenience to passengers not opting for Digi Yatra. Moreover, official claims about Digi Yatra's design being privacy-preserving are not enough, as it continues to have weak privacy policies and safeguards, and remains vague about its data sharing practices while collecting an excessive amount of information from passengers.

FRT Not Above Board

The use of institutionalised FRT has historically been a topic of controversy globally. In the aftermath of the Black Lives Matter movement in 2020, multiple companies, including Microsoft, IBM, and Amazon, announced that they would not sell FRT to American police departments in the short term and make a final decision after either re-evaluating their stance or if a law regulating FRT came into force. However, the use of FRT by the executive in India goes on without any checks in place.

The Indian Constitution recognises a person's right to life, which is read also as the right to live with dignity. The Supreme Court in K.S. Puttaswamy v. Union of India [(2017) 10 SCC 1] recognised that dignity is connected with privacy. FRT systems used in public spaces (such as airports) are per se violative of privacy and dignity. Studies have shown that making FRT ubiquitous as an ecosystem reduces the identity of citizens to merely a rapidly shared and transacted datapoint, imposes a sort of continuous and involuntary visibility, and constricts the behaviour of people.

> Several studies show that facial recognition technology is inaccurate, especially for people of colour (which includes Indians) and women. FRT systems are particularly error prone when encountering new faces.

FRT creates unique risks because our faces are our most prominent identifiers. Unlike fingerprints, our faces are on our passports, Aadhaar cards, PAN cards, and driver's licences. The facial data stored in FRT-based authentication systems, for instance, is far more vulnerable than any other biometric identifier because it can be used to create 360-degree profiles of citizens and can result in "dragnet surveillance".

Dragnet surveillance refers to the collection and analysis of information on entire populations or communities, instead of just those who are under suspicion for committing a crime. A 360-degree profile is institutionally created when a single ID number across datasets links together different data sources. The use of digital identifiers, especially facial biometric data, may lead to unauthorised profiling of individuals through correlation of identities across multiple application domains.

> The Privacy Policy fails to mention the specific purposes for which this data is collected. But it says that it may also be used for "improvement of products, contacting for surveys, and to process user/customer requests".

Further, several studies show that FRT is inaccurate, especially for people of colour (which includes Indians) and women. FRT systems are particularly error prone when encountering new faces. In addition, components of FRT, such as computer vision systems, are inherently non-transparent and their decisions are not easy to understand even by the people who built them. When they make an error, the user cannot tell what reasoning the machine has used, let alone correct it. It would be unwise to allow such opaque and inexplicable processes to infringe on our privacy.

Vague and Contradictory

An examination of the DYBBS Policy and Digi Yatra's Privacy Guidelines show the service stands on weak legal foundations. However, the kind of data it collects (and the magnitude of it) is alarming. In Digi Yatra's Privacy Policy, the categories of data listed for collection include, and are not limited to, identity and contact data, biometric data, business information, technical data such as passwords and video or image data, images or video. These are captured with the consent of passengers on mobile apps, kiosk systems or e-gates at airport checkpoints.

The Privacy Policy fails to mention the specific purposes for which this data is collected. But it says that the collected data may also be used for purposes other than those, such as "improvement of products, contacting for surveys, and to process user/customer requests". In reality, data such as contact or business information or audio-visual data do not have a reasonable link to the objective of the service, which is simply to authenticate passengers against their facial biometric data. Digi Yatra deviates from the privacy principle of data minimisation and collects more information than that which is "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Further, some clauses are a mystery. The Privacy Policy allows for collecting, storing, processing, transferring, and sharing a passenger's personal information with third parties or service providers for the purposes set out in the policy (which include marketing, events, programmes and promotions). But it also states that the data collected under Digi Yatra "cannot be used by any other entity since it is encrypted". The contradiction here has not been addressed by the Ministry or the Digi Yatra Foundation, the entity responsible for operating the service, which leaves one uncertain if any of this data is encrypted.

There is also ambiguity about what kind of personal information is shared from a passenger's smartphone and how it is used by the Digi Yatra mobile application. In an April 2023 press statement, the Ministry claimed, "Under Digi Yatra, passengers' data is stored in their own device and not in centralised (sic) storage … In the Digi Yatra process, there is no central storage of passenger's Personally Identifiable Information (PII) data. All the passengers' data is encrypted and stored in the wallet of their smartphone. It is shared only between the passenger and the airport of travel origin, where passenger's (sic) Digi Yatra ID needs to be validated. The data is purged from the airport's system within 24 hours of departure of flight."

This appears to contradict the DYBBS Policy, which states, "The Airport operator [DYBBS] will retain the Travel Data including the Digi Yatra ID Travel Credential for a duration of 30 days from the date of travel after the Passenger's Flight departs". This implies that the data is stored, and that union government functionaries have access to it when required.

> Digi Yatra lacks an anchoring legislation or operative data protection rules. It also fails to meet the requirements of necessity and proportionality because mere convenience cannot be used as a justification to restrict privacy.

The press statement is also at odds with an interview given by Avinash Komireddy, the founder and CEO of Dataevolve, the start-up that designed the Digi Yatra ecosystem, where he states that "data authentication takes place on the Amazon Web Services cloud platform". This has not been mentioned by the Ministry in any of its statements or in the DYBBS Policy. Overall, how data is stored and authenticated in the Digi Yatra ecosystem has not been made transparent, which raises concerns for whether privacy standards are being complied with.

Flunks the Puttaswamy Test

The Supreme Court laid down certain thresholds to justify state intrusion into the right to privacy guaranteed to citizens in its decision in Puttaswamy v. Union of India. These thresholds are—legality, necessity, proportionality and procedural safeguards.

Digi Yatra fails to fulfil the legality threshold because it lacks an anchoring legislation or operative data protection rules. It also fails to meet the requirements of necessity and proportionality because mere convenience cannot be used as a justification to restrict privacy. It goes one step further by failing to prescribe any grievance redress mechanisms, penalties for contraventions, or any rights of data principles in case of privacy violations. In all, Digi Yatra fails to fulfil any of the conditions that justify infringing on passengers' fundamental right to privacy.

Exempt from New Law

Finally, when the Digital Personal Data Protection Act, 2023 (DPDPA) comes into play with its procedural Rules notified, it still may not be able to adequately protect the sensitive personal data of Digi Yatra users, specifically facial biometric data. First, Section 17 of the Act holds the power to exempt Digi Yatra and its data processing authorities from its very application at any given time. If such an exemption is notified, the provisions of seeking informed consent before data sharing, among others, will not apply to the service, and the existing privacy policies may not be able to provide adequate safeguards to Digi Yatra's data processing and sharing practices.

Second, the DPDPA does not classify "sensitive personal data" as a distinct category needing additional safeguards and caution. Global instruments such as the European Council's "Guidelines on facial recognition" recognise the sensitive nature of biometric information such as facial data and the vulnerable position the processing of such data may leave the data principles in. Therefore, until specific Rules under the DPDPA prescribe higher standards for processing sensitive information such as facial biometric data, Digi Yatra will be operating without appropriate privacy safeguards.

Not At All Transparent

The Right to Information (RTI) Act, 2015 was enacted to promote transparency and accountability to the operations of Indian public authorities. Digi Yatra, being a union government-backed initiative affecting thousands of airline passengers and their privacy, should be transparent in its operation and the authorities should be accountable for its ripple effects. But this is not the case.

> Even though 26% shareholding lies with public institutions such as the Ministry and the Airports Authority of India, the Digi Yatra Foundation itself is absolved from any accountability to Indian citizens.

Digi Yatra is helmed by a special purpose vehicle, the Digi Yatra Foundation, which is tasked with implementing the Digi Yatra Central Ecosystem following the DYBBS Policy issued by the Ministry. This is the nodal body responsible for running the service and therefore the entity that determines how and why personal data is processed. The Foundation, a private company incorporated under Section 8 of the Companies Act, 2013 on 20 February 2019, does not fall within the purview of the RTI Act. Even though 26% shareholding lies with public institutions such as the Ministry and the Airports Authority of India, the Foundation itself is absolved from any accountability to Indian citizens. This is a worrying circumvention of the RTI Act.

Further, there is a lack of public audits to ascertain the data security of the sensitive biometric information collected by Digi Yatra, except for periodic vulnerability audits and certifications conducted by the Standardisation Testing and Quality Certification Directorate and the Computer Emergency Response Team (CERT-In). Regrettably, these reports and audits are also not publicly accessible because CERT-In has recently been exempted from the ambit of the RTI Act.

Not Very Effective

It is highly unlikely that Digi Yatra will satisfactorily deliver on enhancing "passenger experience and provide a simple and easy experience to all air travellers". A simple example could be a busy airport, where someone's image is not captured properly and does not match their government-issued ID. Even assuming that the FRT being adopted under Digi Yatra has a low inaccuracy rate of 2%, this would mean thousands of passengers will not be correctly verified. This would lead to wasting time, including delay in flights taking off, and could also pose a security threat.

A service similar to Digi Yatra was implemented by the US Department of Homeland Security (DHS) and it was shown to have multiple legal, technical, and privacy problems. Legal concerns were raised by the Electronic Frontier Foundation, which stated that "we cannot overstate how big a change this will be in how the federal government regulates and tracks our movements or the huge impact this will have on privacy and on our constitutional 'right to travel' and right to anonymous association with others." It also highlighted how such systems will end up discriminating against minorities due to technical problems.

The American Civil Liberties Union sued the DHS and other agencies for records related to the US government's use of FRT that the group said could pose "grave risks to privacy". On the Indian front, a Kanpur-based professor had moved the Allahabad High Court on the ground that the use of FRT and biometric scans for attendance-recording purposes is antithetical to the right to privacy under Article 21. Use of FRT in surveillance across Tamil Nadu and specifically within the city of Chennai has also been challenged in the Madras High Court in August 2023, on which a notice has been served by the court and hearings are pending.

Conclusions

The Internet Freedom Foundation has written to the Ministry of Civil Aviation, NITI Aayog, Airports Authority of India, Digi Yatra Foundation, and the Delhi, Bengaluru, Mumbai, Cochin and Hyderabad airports, bringing their attention to the worrisome implementation of the Digi Yatra service across airports in India. The Internet Freedom Foundation has urged them to completely withdraw Digi Yatra from Indian airports owing to its large gamut of concerns relating to privacy, surveillance, exclusion errors and lack of institutional accountability and transparency, coupled with the highly disturbing manner in which it is currently being deployed at airports – with reports of coercion and deception, at the cost of passengers' dignity, privacy, and autonomy.

Acknowledgement: *This article is an edited version of the Internet Freedom Foundation's newsletter "Resist Surveillance Tech, Reject Digi Yatra", which covers many more issues that published here. The original article can be accessed in full here.*

Disha Verma is an Associate Policy Counsel at Internet Freedom Foundation. She engages with state deployment of technologies in governance, welfare service delivery and surveillance.