Digi Yatra and the Defect in the Idea of ‘Consent’

techpolicy.press/digi-yatra-and-the-defect-in-the-idea-of-consent/

Sukriti April 30, 2024

Sukriti / Apr 30, 2024

Shutterstock

Most air travelers find passing through security at the airport to be unpleasant. Around the world, facial recognition is increasingly being deployed on the premise that it can speed up the process of identifying travelers, improving security and efficiency. But in India, a widely deployed system is based on a defective model of consent that compromises individual autonomy.

Digi Yatra is a facial recognition technology based system that aims to offer a quick and hassle free experience for travelers at airports in India. It promises a paperless and contactless entry for travelers through all airport checkpoints by verifying identity through a facial scan. Passengers can register on the Digi Yatra application with their Aadhaar number and travel details to facilitate document-free travel through the use of facial recognition. First launched in 2022, the system is currently in operation at thirteen airports in the country – Delhi, Bengaluru, Varanasi, Hyderabad, Kolkata, Vijayawada, Pune, Mumbai, Cochin, Ahmedabad, Lucknow, Jaipur and Guwahati.

The Ministry of Civil Aviation (MoCA) released the first Digi Yatra policy in 2018 and an updated policy in 2021. Currently, Digi Yatra is being implemented by a Joint Venture called Digi Yatra Foundation ("DYF"), which consists of the Airport Authority of India, with a 26% stake and Bengaluru Airport, Delhi Airport, Hyderabad Airport, Mumbai Airport and Cochin International Airport with the remaining 74% stake.

Although the use of Digi Yatra is supposed to be voluntary, recent reports indicate passengers are being coerced to sign up for Digi Yatra by airport personnel, despite their protests. After receiving several complaints, the MoCA clarified that the service remains voluntary and airport personnel have been instructed to obtain the consent of passengers for using Digi Yatra. More recently, an investigative report by the news site The Ken analyzed the data protection threats that arise from the development and implementation of the Digi Yatra app.

Given the controversy surrounding it, it is worth interrogating the idea of 'consent' to government backed services, of which Digi Yatra is only one. Ultimately, Digi Yatra is based on a defective model of consent that compromises individual autonomy. In employing facial recognition, Digi Yatra tests the limits of 'consent' for data protection, privacy, and autonomy.

Citizens' perceptions of the State and diminished choice

Indians may be said to place a higher trust in government services, as Indian citizens have traditionally relied heavily on the government for public welfare services. Given that Digi Yatra is an initiative of the MoCA, the public perception towards the initiative can distort individual consent. The context in which people make a choice may subject it to distortion. A

perception of a state-sponsored initiative taps into citizen's trust in the State in offering welfare services of public utility. This can impact individual discretion in disclosing personal data, given that there is little awareness or understanding of potential implications of disclosing personal data for facial recognition technologies.

Additionally, airports in India present logistical barriers to those without the Digi Yatra application to drive more people to opt for it. For instance, almost all terminal gates at the Indira Gandhi International Airport at New Delhi and the Kempegowda Airport at Bengaluru employ Digi Yatra, which makes the non-Digi Yatra- facial recognition option cumbersome and inconvenient, thus narrowing and manipulating available choices. To illustrate this point, while traveling from the Bengaluru Airport, upon asking for the non-Digi Yatra option, only one entry gate was made accessible, which was the very last entry gate. Even then, non-Digi Yatra entry at that gate was allowed by opening a separate spot.

Considering the above subjective behavior of citizens, one cannot consider a requirement of consent for Digi Yatra as meaningful or free.

Limits of consent and implications for data protection

Use of FRT has been found to have various implications for data protection and privacy. Even as MoCA reassured the public that the data collected for Digi Yatra is purged within 24 hours, the Digi Yatra Policy of 2021 creates certain exemptions, while allowing access to *"any Security Agency, GOI [Government of India] or other Govt. Agency… to the passenger data based on the current/ existing protocols prevalent at that time."* Apart from the dearth of public awareness on the issue that appears to influence the willingness of citizens to give consent, facial recognition also arguably has a "fatal consent problem." As scholars Evan Selinger and Woodrow Hartzog have argued, that consent is a "broken regulatory mechanism" for face-based identification, within which they include systems such as Digi Yatra. Selinger and Hartzog argue that the logic of consent for facial recognition is ill-founded because an individual is never fully aware of the threats that facial recognition carries for their autonomy.

They further argue that facial recognition compromises "obscurity." Obscurity refers to the "ease or difficulty of finding information and correctly interpreting it." Obscurity is an important idea because it furthers individual autonomy, since privacy is presupposed in society to mean that information is disclosed to some audiences but not everyone. This differs from the concept of anonymity, which means "nobody knows who you are." Obscurity often requires "structural constraints," which are technological limitations that make access and identification of individual movements and behaviors difficult and expensive.

Selinger and Hartzog argue that to enable people to give valid consent for facial recognition technologies, they need to be made aware of the importance of obscurity for privacy and its compromise by the use of facial recognition. However, Selinger and Hartzog suggest that

since obscurity is inevitably lost with facial recognition technologies, the privacy regulatory regime should provide for “meaningful obscurity protections.”

In the case of Digi Yatra, the concerns with obscurity remain true, rendering it “inconsentable.” However, the concerns are aggravated because of the absence of any statute in India regulating the use of facial recognition, and the legal vacuum within which Digi Yatra operates, which is a mere standalone policy document. Moreover, the government’s exemption of Digi Yatra from the Right to Information Act (RTI) leads to a severe lack of transparency. Even if it was not considered exempt under RTI, the government is empowered to exempt it under the Digital Data Protection Act, 2023 from disclosing any information under RTI by qualifying Digi Yatra as a State instrument.

The investigation conducted by The Ken revealed that the Digi Yatra Foundation’s claim that the data is only stored on the user’s device is unlikely to be the case. Further, the personal data of individuals may also remain at risk as the Digi Yatra Policy of 2021 plans on allowing users to use ‘Digi Yatra value-added services,’ which will allow users to avail third party services from “Digi Yatra ecosystem stakeholders/partners”. These could include cab, hotel, or lounge services. The sample consent notice for this requires consent to the use of the passenger’s phone number, email ID, ticket and boarding pass data, and face biometric data to avail these services. This could lead to loss of autonomy over data leading to risks of data aggregation, data monetization, and profiling.

The impact of a citizen’s perception of the State in deciding consent as well as the limitation in the idea of consent itself with regard to facial recognition together operate to compound the problem of consent for Digi Yatra. It is important that Digi Yatra remains a strictly voluntary service. For Digi Yatra to be truly voluntary as a service, the current model of implementation needs an overhaul.

Authors

Sukriti
Sukriti works as an Analyst at the Centre for Communication Governance at National Law University Delhi (CCG). She is interested in data protection and privacy, platform governance, and issues of digital rights and free speech.

Topics

Join our newsletter on issues and ideas at the intersection of tech & democracy