The Aadhaar ecosystem leaks too much data

People don’t respond well to dystopian scenarios”, a professor of marketing warned me late last year. The true extent of Aadhaar-linked data leakage is hard to process, so we tend to ignore it. Smaller inconveniences are easier to understand.

Some awareness, however, has now seeped into public consciousness due to an exposé by Rachna Khaira in *The Tribune*, who showed that access to the entire database could be purchased for as little as Rs500. The response was predictable. First, multiple denials that a breach had even occurred. Second, an FIR against Khaira and The Tribune, combined with allusions of “an orchestrated campaign to malign Aadhaar”. Third, when the repeated assertions of Aadhaar’s safety wore thin, a public dare demanding to know how anyone could be harmed if their private information got leaked.

Section 59 of the Aadhaar Act covers activities that are illegal under the rest of the Act. Many states have sought to collect deeply personal information such as religion and caste in their state resident data hubs (SRDHs), coupled with biometrics, and without the cover of a state law. UIDAI (Unique Identification Authority of India) has enabled this in their enrolment and other software with such innocuous names as “DBT Seeding Data Viewer (DSDV)” and “Rapid Aadhaar Seeding Framework (RASF)”. Andhra Pradesh links everything to Aadhaar, all the way down to minor traffic offences. The police are allowed access to biometrics for identifying criminals and lost children. The sensitivity of such detailed personal information coupled with voter ID during an election should be obvious.

The Aadhaar ecosystem is widespread, extending to former UIDAI members like Nandan Nilekani and think tanks like iSPIRT, private firms like Khosla Labs, venture capital firms and their research vehicles like Omidyar and IDinsight, service providers like Airtel, Jio and Paytm, and the National Payments Corporation of India. UIDAI is a hopelessly ill-equipped steward of the ecosystem, and its ongoing meltdown is apparent to anyone tracking the details. While the ecosystem members may not always agree with each other, what unites them is their desire to keep Aadhaar afloat regardless of the risks, because it lowers their government-imposed “know your customer” (KYC) costs. This is an inversion of democracy, where societal concerns are primary. This Aadhaar ecosystem treats a breach as a simple accident, without regard for consequences to the victims.

In 2014, Nilekani, former chairman of UIDAI, accidentally leaked his own Aadhaar details when he posted a photograph of his Aadhaar card with the number masked out while keeping the accompanying QR code which contained his number, date of birth and residential address. Copies of his information remain available on multiple websites, accessible via a simple Google search. If someone as powerful as Nilekani is unable to make the internet forget his details, what hope does anyone else have?

The Tribune breach required one to know an Aadhaar number to retrieve personal information. It takes a computer mere seconds to produce all 80 billion possible Aadhaar numbers. The one billion currently-valid numbers can be filtered out by using the 130 million already-leaked numbers, and the rest using a number of verification services, including UIDAI’s own—which is technically protected by a “captcha” to prevent such automated attempts, but which is so trivial that amateurs break it to win programming contests, and then share on code repository GitHub.com. One has to be incredibly naïve to believe hostile actors, including foreign powers, haven’t already harvested all data.

A valid Aadhaar number is a key that opens multiple locks. Dialing *99*99# connects you to NPCI’s query service on Aadhaar mapper (QSAM), which cheerfully tells you which bank the

Aadhaar holder is receiving subsidy deposits in. Indane's website will tell you the name of the Aadhaar holder and their LPG connection ID, and the history of banks they have received subsidies in. Keep probing services like this, and soon enough one builds a comprehensive profile of an individual containing information that is most certainly not known to Google and Facebook, the Aadhaar ecosystem's preferred bogeymen. Forget state-level actors, this is now available to common scamsters. **Everyone from housemaids to members of Parliament have fallen prey** to targeted phishing scams that use private information to convince the victim that they genuinely represent the service provider, only to find that money has been stolen from their bank accounts soon after.

The leaks get worse. UIDAI has no capability to audit the security practices of even its licensed ecosystem of over 300 agencies, all with the power to query the main database, sublicence access, and combine with other data. Every few weeks a new leak is discovered. The SRDHs operate without public oversight and contain contact information of children. The Krana blog documents how the known leaks happen, but who knows how many undocumented leaks are actively abused?

One must remember that the Aadhaar ecosystem also holds data on all military personnel. The military has independent standards for everything, from data storage to transmission, because of how sensitive their data is, and now UIDAI and its out-of-control ecosystem are leaking data left, right and centre. Aadhaar endangers national security and the government needs to act fast.

Kiran Jonnalagadda is a co-founder of the Internet Freedom Foundation.

Comments are welcome at theirview@livemint.com

END