Clarification requested on linking PAN with Aadhaar

1 message

Thejesh GN <i@thejeshgn.com>
To: chairmancbdt@nic.in
Bcc: bcc+cbdt@email.speakforme.in

Mon 11 Mar, 2019 at 7:07 PM

To

The Chairman
Central Board of Direct Taxes (CBDT)
Ministry of Finance, Dept. of Revenue,
North Block, ITA II Division
New Delhi - 110001
chairmancbdt@nic.in

Sir,

SUB: Seeking confirmation on the safety of personal information and data protection in the context of the Order dt. 30.06.2018 u/Sec 119 of the Income Tax Act extending time for linking PAN with Aadhaar

1. We are writing to you to request a reconsideration of your order dated 30.06.2018, passed under Section 119 of the Income Tax Act, 1961 (hereinafter referred to as the "Income Tax Act") through which the Central Board of Direct Taxes (hereinafter referred to as the "CBDT") has extended time for linking PAN with Aadhaar till 31.03.2019.

2. It is requested that your office rescind the orders mandating linking PAN with Aadhaar or, in the alternative, extend the time for linking PAN with Aadhaar until sufficient safeguards are put in place to protect the rights and interests of tax payers, including and especially the fundamental right to privacy which the Supreme Court has recognised as an intrinsic part of the fundamental rights contained in Part III of the Constitution, and including the right to dignity.

3. In September 2018, the Supreme Court upheld section 139AA of the Income Tax Act which requires the linking of the Aadhaar number to income tax returns and PAN card. The majority judgment accepted the statement of counsel for the respondents that Aadhaar is an impeccable identity, that no duplicates exist, that it reflects the identity of each person accurately. On matters of security of data, the court only considered the UIDAI and accepted the powerpoint presentation made by the CEO of the UIDAI that it is secure. The majority judgment also acknowledged that there was no data protection law yet in place, and that that must be remedied.

4. Significantly, therefore, the court's partial imprimatur to the Aadhaar programme, and to Section 139AA of the Income Tax Act, through its judgment dated 26.09.2018 (Puttaswamy II), also recognised the inviolability of the right to privacy. The judgment does not validate the methods employed in linking Aadhaar with PAN but merely holds such linking to be constitutionally valid subject to such linking being in conformity, among other things, with the various principles of privacy that the nine-judge bench of the court recognised unanimously in August 2017, in Justice K.S. Puttaswamy (Retd) v. Union of India (Puttaswamy I).

5. Since the date of the judgment, many events have transpired that raise questions about the Aadhaar project, and the validity of Aadhaar as a secure and robust identity. Some illustrative examples are set out below.

a. The State Bank of India has alleged misuse and wrongful generation of Aadhaar numbers. A report on January 29, 2019 explained the manner in which the fraud was being committed, raising concerns about fake numbers being generated by the project. State Bank of India, it may be recalled, has been directed by the UIDAI (as have other banks, see https://economictimes.indiatimes.com/industry/banking/finance/banking/banks-without-stipulated-number-of-Aadhaar-centres-will-face-rs-20000-fine-from-october/articleshow/60376996.cms) to set up enrolment centres in at least 10% of their branches, and to do a certain number of enrolments everyday on pain of penalty (https://www.thehindu.com/business/Industry/Aadhaar-authentication-13-banks-fined-face-penalties/article24835382.ece , August 31, 2018). See https://economictimes.indiatimes.com/industry/banking/finance/banking/sbi-alleges-Aadhaar-data-misuse-uidai-rubbishes-charge/articleshow/67734688.cms

b. A single judge of the Calcutta High Court, in the matter of Debashis Nandy v. Union of India in judgment dated January

3, 2019, was confronted with a case where the father's name had been falsely entered when demographic information was collected at the time of enrolment. His finding in the case is that the Supreme Court judgment does not deal with the authenticity of demographic data, and in fact, demographic information is unverified, and that "there is definitely something amiss with the Aadhaar enrolment process if important demographic information such as the name of the applicant's father, as the case in hand, can be falsified and even go undetected." The judgment records that "the Learned Additional Solicitor General submitted that no verification is sought as regards such information and the application is processed on the basis of the bare information provided by the applicants in their application." The ease with which false identities can be created is the central aspect of this judgment. See https://www.livelaw.in/pdf_upload/pdf_upload-357113.pdf

c. This problem with the Aadhaar system has also been acknowledged by a Division Bench of the Lucknow Bench of the Allahabad High Court in the matter of Smt Parvati Kumari v. State of UP in judgment dated January 9, 2019. In this case, the court held: "We clearly deduce from the above that the other information namely name, date of birth, gender and address as entered in the Aadhaar Card, is furnished by the Aadhaar applicant at the time of authentication/enrolment. Although, the regulations provide for the applicant to rely on a set of documents for giving information in regard to name, address and proof of date of birth, however, because the said information is merely given by the applicant, and is not authenticated by UIDAI at the time of authentication, the Aadhaar Card cannot be conclusive proof in regard to those entries." The only connection that can be established, according to the High Court, is the biometric information collected and the Aadhaar number. See
https://www.livelaw.in/top-stories/aadhar-entries-not-conclusive-proofs-allahabad-hc-142428

d. In the meantime, biometric fraud has surfaced on several occasions. A recent incident is reported at
https://www.indiatimes.com/trending/wtf/hackers-use-Aadhaar-biometrics-to-rob-a-man-s-account-whose-job-is-to-issue-Aadhaar-cards-361274.html and
https://www.huffingtonpost.in/entry/aadhar-biometrics-theft-case-police-arrests-victims-close-friend_in_5c5f2788e4b0eec79b23f356

e. The vulnerability of the UID database, and of the various databases in which the number has been seeded, has been revealed. On January 25, 2019, it was reported that fake voter IDs had been created by Telangana Congress to make a point about the shortcomings in the voter registration system. "All one needs is to create a duplicate Aadhaar card of a person and use a house address which has an electricity bill. The photo and details can be sourced from WhatsApp or from social media accounts, it's that simple. No one will verify if the Voter ID is genuine or fake," explained the Congress worker who created the bogus card. See https://www.thenewsminute.com/article/anyone-can-fake-it-telangana-congress-workers-forge-voter-ids-election-officers-95659

f. More recently, on 26 February, 2019, the Times of India reported that the UIDAI has launched a massive probe into a complaint filed regarding alleged privacy breach and misuse of data of 3.7 crore voters in Andhra Pradesh. The problem has been exacerbated by the seeding of the Aadhaar number in various databases, including in this case the Smart Pulse Survey and the State Resident Data Hub, which contain demographic data in the UID database and in the electoral rolls. "The app has voter ID numbers, names, colour photos, booth-level information, family details, caste information and government schemes and amounts a voter gets as beneficiary. The app comes with all the information inbuilt and is extensively used by TDP activists", the report says. It says that investigation is on to find out how the company, IT Grids (India) obtained family details and beneficiary data. See
https://timesofindia.indiatimes.com/india/tdp-app-breached-data-of-3-7cr-voters-probe-begins/articleshow/68160839.cms

g. The vulnerability of the data in the Aadhaar system was acknowledged by the UIDAI in a press release in February 2018, when the "CEO, UIDAI advised people to be watchful for the protection of their privacy and recommended not to share their Aadhaar number or personal details to unauthorized agencies for getting it laminated, or printed on plastic card." See
http://pib.nic.in/PressReleaseIframePage.aspx?PRID=1519253

This caution extends, as is now evident, more generally, and in situations beyond the control of the individual.

h. Most recently, a data breach is under investigation in Hyderabad, which reveals the vulnerability of systems that incorporate the Aadhaar number in their database. See http://www.newindianexpress.com/states/telangana/2019/mar/03/data-breach-by-tdp-app--cops-search-offices-of-it-grids-detain-four-1945964.html and related news.

It is a matter of record that the SRDH (State Resident Data Hubs) have been set up by collaboration between the UIDAI and state governments.
See https://archive.org/stream/UIDAISRDHStateAdoptionStrategy/UIDAI%20-%20SRDH%20-%20Institutional%20Framework_djvu.txt for the 2012 UIDAI document on the creation and updation of SRDH, which has been the basis of which various SRDHs have been created. See for instance https://apit.ap.gov.in/?page_id=588 and http://degs.org.in/UIDAI.aspx (Delhi) and https://www.karnataka.gov.in/Aadhaar/Pages/Karnataka-Resident-Data-Hub-(KRDH).aspx and https://osrdh.odisha.gov.in/srdhportal/LdapConfig.action and https://makkal.tn.gov.in/makkal/login,

For a summary of the risks of the SRDH system, see https://medium.com/karana/the-360-degree-database-17a0f91e6a33

i. A recent RTI reply from the UIDAI has revealed an astonishing fact: that the UIDAI does not have a Chief Information Security Officer. See https://www.moneylife.in/article/Aadhaar-truth-uidai-never-appointed-a-chief-information-security-officer-reveals-rti/56267.html

j. Breaches of various databases holding Aadhaar numbers have been reported since the judgment, other than the Telangana breach cited above, and including:

- on 19 February, 2019, at https://techcrunch.com/2019/02/18/Aadhaar-indane-leak/ (Indane gas company leaks - it is estimated that over 6.7 million customers could be affected)
- end January 2019, at https://techcrunch.com/2019/01/31/Aadhaar-data-leak/ (Jharkhand government web site)
- at the World Economic Forum, the Global Risk Report 2019 named Aadhaar as having suffered multiple breaches, compromising over 1.1 billion people. See the report dated 19 February 2019 at https://www.moneylife.in/article/Aadhaar-data-breach-largest-in-the-world-says-wefs-global-risk-report-and-avast/56384.html

Another report by Avast Software made a similar assessment. Both had Rachna Khaira's investigative report for the Tribune for reference, but seem to have found reason to endorse it. The assessment also seems to point to 'lax cybersecurity protocols' as the possible reason for the breaches. That the UIDAI routinely denies leaks from its database, even when it has had to blacklist operatives, launch investigations, penalise connected persons, is part of the problem.

k. Since the judgment on September 26, 2018, information gathered from Fact Finding Reports and in the media shockingly reveals at least 12 further deaths where the poor have not been able to access their basic entitlements including ration and pension. This is despite the assurance given to the court by the Attorney General that "no deserving person would be denied the benefit of a scheme on the failure of authentication". (at p.554 of the majority judgment). See for instance https://www.firstpost.com/india/failure-of-a-biometric-machine-leaves-this-up-village-stranded-for-ration-5975641.html

In this case, it was a problem of connectivity, which is why a whole village found itself stranded.

l. There are further reports of the police demanding from housing societies "complete information of their residents" including details of their voter ID, PAN card, Aadhaar, phone number, vehicle number, email address, blood group, driving licence number, 2 passport size photographs and more. (By police notice from the office of the Police Inspector, KP Agarahara Police Station, Bangalore City, dated 28 January, 2019, No. KPAPS/CC/2019.)

The Regional Office in Bangalore of the EPFO continues to demand the Aadhaar number, even as recently as 7 February 2019, despite the Supreme Court judgment which renders this illegal.

This wide range of evidence has raised serious concerns about potential loss of identity, fraud including identity fraud, and privacy. This is apart from the deeply problematic nature of both the manner in which enrolments have happened and continue to happen (see the SBI complaint, supra).

In such a situation, there is ample ground to oppose the linking of the income tax returns and the PAN card to the Aadhaar number. In any event, such a move should be held off till the questions raised are answered and the vulnerabilities of the system and of the individual are satisfactorily dealt with.

6. We would also draw your attention to the judgment of the Supreme Court which accepted the logic of linking Aadhaar and PAN, but not while doing away with the right to privacy. The court accepted the government's averment that it would serve a legitimate state aim, and so there can be inroads made into the right to privacy, if the doctrine of proportionality is met. There was already a law, but that law only mandated the linking of PAN and Aadhaar, and Aadhaar and income tax returns. It did not provide any manner of data protection. The court left it to the government to pass a Data Protection Law that would pass the test of protecting people's rights and interests. That has not yet happened.

In its absence, we draw your attention to the report of the Group of Experts on Privacy constituted by the Planning Commission, under the chairmanship of Justice AP Shah, and whose report was presented to the government in October 2012. The report enunciated nine clear principles ("privacy principles).

These are

* a requirement that the any data collector provide a simple notice of the information collected to all individuals, in clear and concise language, prior to the collection of such information;
* that a data controller ought to give individuals a choice with regard to providing their personal information, and take individual consent only after providing notice of its information practices;
* that only such information as is necessary for an identified purpose be collected;

* that data collected ought to be adequate and relevant to the purposes for which they are processed;
* that individuals ought to be allowed access to personal information about them held by the collecting authority;
* that it be made mandatory that information collected is only disclosed to third parties after notice and informed consent is obtained;
* that the collection and processing of the information is done in a manner that protects against loss, unauthorized access, destruction, use, storage, etc;
* that a data processor ought to take all necessary steps to implement practices, procedures, policies and systems in a manner proportional to the scale, scope, and sensitivity to the data that is collected and processed; and nine, that clear mechanisms be put in place to implement privacy policies, including tools, training, and education; and external and internal audits.

For a more detailed reading of the report, see http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf

You will agree with the conclusion of the report that it is of the utmost importance to acknowledge that data protection is not just about protecting data, but about protecting the person whose data it is.

7. These privacy principles have since been memorialised through the judgment of the Supreme Court in Puttaswamy I (the Privacy judgment), and the holding that the linking of Aadhaar with PAN is constitutionally valid is subject to the measures taken for the said purpose being compliant with these essential principles.

8. Parliament has not enacted such a law. When it is enacted, it will have to be tested to ensure it meets the standards set by the privacy judgment, which was rendered unanimously by a bench of nine judges.

Till then, and given:

* the state of demographic information in the UIDAI database
* the wide range of places where the number has been linked/seeded
* the regularity of data breaches
* the absence of a Chief Information Security Officer in the UIDAI
* the repeated cases of biometric failure and of biometric fraud
* the probability of inorganic seeding, which takes consent away from the individual, and which must be struck down if any further seeding is to be allowed (see p.2 at https://pdsportal.nic.in/Files/Aadhar%20seeding%20guidelines.pdf)
* the failure to delete the Aadhaar number from various databases where it has been wrongly seeded such as in banks and with mobile service providers despite the judgment of the Supreme Court
* the PAN number is required to be handed over to a multiplicity of agencies (15 at a quick count)

We request that you immediately suspend the linking of the Aadhaar number with the PAN card, and remove the requirement of providing the Aadhaar number while filing income tax returns till the problems stated above are addressed.

In addition, since as a data controller you are responsible for data protection, we are requesting you to kindly let us know:

* how the data will be stored
* how the data will be/is being processed,
* what security measures have been taken to prevent the breach of the data base, protect personal information and ensure that there is no unauthorised transfer
* the purposes for which the Aadhaar number will be used, and what measures have been taken to ensure that it is not used for any other purpose
* how you will detect that it has been used for a purpose other than that for which it is collected
* how the breach of our data will be communicated to us
* what action will be taken in the event of a breach
* whose is the liability when there is a leak, transfer or inorganic seeding of the Aadhaar number
* what is the extent, and forms of liability in the event that there is a data breach
* which companies are involved in collecting, storing, processing and dealing with the data in any way, and what measures are in place to protect our data, and our privacy? This is especially important since there is no data protection law.

We also request you to respond to the various other queries raised in this missive.

Kindly make it convenient to send a response within 10 days, since the time for filing income tax returns is drawing close, and I wish to file my returns on time.

Yours sincerely,

Regards,
Thej

Thejesh GN ≒ ತೇಜೇಶ್ ಜಿ.ಎನ್
http://thejeshgn.com