All that data that Aadhaar captures

Predictably enough, the recent Supreme Court order affirming that **privacy is a fundamental right** sent Aadhaar's public-relations machine into damage control mode. **After denying the right to privacy for years**, the government promptly changed gear and welcomed the judgment. Ajay Bhushan Pandey, CEO of the Unique Identification Authority of India (UIDAI), **suddenly asserted**, "The Aadhaar Act is based on the premise that privacy is a fundamental right." He also clarified that the judgment would not affect Aadhaar as the required safeguards were already in place.

The fact of the matter is that Aadhaar, in its current form, is a major threat to the fundamental right to privacy. The nature of this threat, however, is poorly understood.

There is a common perception that the main privacy concern with Aadhaar is the confidentiality of the Central Identities Data Repository (CIDR). This is misleading for two reasons. One is that the CIDR is not supposed to be inaccessible. On the contrary, the Aadhaar Act 2016 puts in place a framework for sharing most of the CIDR information. The second reason is that the biggest danger, in any case, lies elsewhere.

To understand this, it helps to distinguish between three different types of private information: biometric information, identity information and personal information. The first two are formally defined in the Aadhaar Act, and protected to some extent. Aadhaar's biggest threat to privacy, however, relates to the third type of information.

In the Aadhaar Act, biometric information essentially refers to photograph, fingerprints and iris scan, though it may also extend to "other biological attributes of an individual" specified by the UIDAI. The term "core biometric information" basically means biometric information minus photograph, but it can be modified once again at the discretion of the UIDAI.

Identity information has a wider scope. It includes biometric information but also a person's Aadhaar number as well as the demographic characteristics that are collected at the time of Aadhaar enrolment, such as name, address, date of birth, phone number, and so on.

The term "personal information" (not used in the Act) can be understood in a broader sense, which includes not only identity information but also other information about a person, for instance where she travels, whom she talks to on the phone, how much she earns, what she buys, her Internet browsing history, and so on.

Coming back to privacy, one obvious concern is the confidentiality of whatever personal information an individual may not wish to be public or accessible to others. The Aadhaar Act puts in place some safeguards in this respect, but they are restricted to biometric and identity information.

The strongest safeguards in the Act relate to core biometric information. That part of the CIDR, where identity information is stored, is supposed to be inaccessible except for the purpose of biometric authentication. There is a view that, in practice, the biometric database is likely to be hacked sooner or later. Be that as it may, the UIDAI can at least be credited with trying to keep it safe, as it is bound to do under the Act.

That does not apply, however, to identity information as a whole. Far from protecting your identity information, the Aadhaar Act puts in place a framework to share it with "requesting entities". The core of this framework lies in Section 8 of the Act, which deals with authentication. Section 8 underwent a radical change when the draft of the Act was revised. In the initial scheme of things,

authentication involved nothing more than a Yes/No response to a query as to whether a person's Aadhaar number matches her fingerprints (or possibly, other biometric or demographic attributes). In the final version of the Act, however, authentication also involves a possible sharing of identity information with the requesting entity. For instance, when you go through Aadhaar-based biometric authentication to buy a SIM card from a telecom company, the company typically gains access to your demographic characteristics from the CIDR. Even biometric information other than core biometric information (which means, as of now, photographs) can be shared with a requesting entity.

Quite likely, this little-noticed change in Section 8 has something to do with a growing realisation of the business opportunities associated with Aadhaar-enabled data harvesting. "Data is the new oil", the latest motto among the champions of Aadhaar, was not part of the early discourse on unique identity — at least not the public discourse.

Section 8, of course, includes some safeguards against possible misuse of identity information. A requesting entity is supposed to use identity information only with your consent, and only for the purpose mentioned in the consent statement. But who reads the fine print of the terms and conditions before ticking or clicking a consent box?

There is another important loophole: the Aadhaar Act includes a blanket exemption from the safeguards applicable to biometric and identity information on "national security" grounds. Considering the elastic nature of the term, this effectively makes identity information accessible to the government without major restrictions.

Having said this, the proliferation and possible misuse of identity information is only one of the privacy concerns associated with Aadhaar, and possibly not the main concern. A bigger danger is that Aadhaar is a tool of unprecedented power for mining and collating personal information. Further, there are few safeguards in the Aadhaar Act against this potential invasion of privacy.

An example may help. Suppose that producing your Aadhaar number (with or without biometric authentication) becomes mandatory for buying a railway ticket — not a far-fetched assumption. With computerised railway counters, this means that the government will have all the details of your railway journeys, from birth onwards. The government can do exactly what it likes with this personal information — the Aadhaar Act gives you no protection, since this is not "identity information".

Further, this is just the tail of the beast. By the same reasoning, if Aadhaar is made mandatory for SIM cards, the government will have access to your lifetime call records, and it will also be able to link your call records with your travel records. The chain, of course, can be extended to other "Aadhaar-enabled" databases accessible to the government — school records, income-tax records, pension records, and so on. Aadhaar enables the government to collect and collate all this personal information with virtually no restrictions.

Thus, Aadhaar is a tool of unprecedented power for the purpose of mining personal information. Nothing in the Aadhaar Act prevents the government from using Aadhaar to link different databases, or from extracting personal information from these databases. Indeed, many State governments (aside from the Central government) are already on the job, under the State Resident Data Hub (SRDH) project, which "integrates all the departmental databases and links them with Aadhaar number", according to the SRDH websites. The Madhya Pradesh website goes further, and projects SRDH as "the single source of truth for the entire state" — nothing less. The door to state surveillance is wide open.

What about private agencies? Their access to multiple databases is more restricted, but some of

them do have access to a fair amount of personal information from their own databases. To illustrate, Reliance Jio is in possession of identity information for more than 100 million Indians, harvested from the CIDR when they authenticate themselves to buy a Jio SIM card. This database, combined with the records of Jio applications (phone calls, messaging, entertainment, online purchases, and more) is a potential gold mine — a dream for "big data" analysts. It is not entirely clear what restrictions the Aadhaar Act imposes, in practice, on the use of this database.

In short, far from being "based on the premise that privacy is a fundamental right", Aadhaar is the anti-thesis of the right to privacy. Perhaps further safeguards can be put in place, but Aadhaar's fundamental power as a tool for mining personal information is bound to be hard to restrain. The very foundation of Aadhaar needs to be reconsidered in the light of the Supreme Court judgment.

Jean Drèze is Visiting Professor at the Department of Economics, Ranchi University

END