Privacy issues exist even without Aadhaar

In part I, I argued that while Aadhaar can be a tool to infringe upon our right to privacy, it is merely one such; there exist other tools that can be similarly exploited. This becomes evident when you analyse each privacy issue related to Aadhaar using the National Privacy Principles framework, and compare Aadhaar's data privacy risks to other national ID systems. We need an independent data privacy regulator, backed by a robust law, to safeguard against the risks.

Here, we explore two such data privacy issues: data disclosure and voluntariness (database linking was analysed in part I).

Data disclosure

According to the National Privacy Principle on data disclosure, "a data controller shall not disclose personal information to third parties, except after providing notice and seeking informed consent from the individual for such disclosure".

On paper, the Aadhaar Act appears compliant with this principle as Section 29 prohibits the disclosure of personal information. Exceptions exist for courts to request demographic data, and for joint secretaries and higher ranks to request biometric data; the latter on the grounds of "national security". However, greater clarity is required on whether individuals will be informed of data disclosures.

In practice, however, data disclosures well beyond these exceptions have taken place. A study by the Centre for Internet and Society found that nearly 130 million Aadhaar numbers had been published online by four government departments. In many cases, these were published along with information on "caste, religion, address, photographs and financial information". If someone manages to steal these individuals' fingerprints as well (which is becoming less difficult), one possibility is that Aadhaar-linked bank accounts can be cleaned out using micro-ATMs.

Demographic data disclosure, however, is not limited to Aadhaar. For transparency reasons, state election commission websites disclose the personal information of every person registered to vote online. Agencies scrape these databases and sell them.

Like database linking, the onus of abiding by the principle of data disclosure is on the "data controller". The four government agencies that disclosed Aadhaar data—not the Unique Identification Authority of India (UIDAI)—are the relevant data controllers in this case. However, UIDAI has not pressed charges against them; under the Aadhaar Act, it is solely authorized to do so. Given UIDAI's role of working with the government to enable and encourage the use of Aadhaar, it should not also be responsible for regulating them. Additionally, the Election Commission's data disclosure norms demonstrate that the issue is bigger than Aadhaar.

This, therefore, points to the critical need for a data privacy regulator to investigate and penalize unauthorized disclosure of sensitive personal information. A strong regulator, with a clear law, will also serve as an effective deterrent for negligent disclosure practices.

Voluntariness

The ability to voluntarily opt in and out of data systems, based on informed consent, is central to the National Privacy Principle of "Choice and Consent". Once an individual opts in, the principle clarifies that they "also have an option to withdraw (their) consent given earlier to the data controller".

With regard to opting in, UIDAI has maintained that Aadhaar enrolment is voluntary. However, Section 7 of the Aadhaar Act and various orders by government agencies require Aadhaar to access basic services. Though exceptions are allowed, in practice they are implemented inconsistently, making Aadhaar near-mandatory.

To be sure, the choice principle states that data controllers can choose not to provide services if an individual doesn't consent to provide data, "if such information is necessary for providing the goods or services". However, we need more explicit guidelines on what features satisfy this condition, something that can be defined in a data privacy law.

With regard to opting out, no such UIDAI provision exists. One argument is that more data increases UIDAI's capability to establish the uniqueness of new enrollees. However, it is unclear why this is the case because even if millions opt out of Aadhaar, UIDAI's ability to guarantee the uniqueness of new enrollees compared to existing enrollees doesn't diminish.

While voluntariness is actively discussed with Aadhaar, the same is not true for other IDs and data initiatives. For example, fingerprints are collected to issue Indian passports, but the use of this is not clear—raising concerns around voluntariness as well as purpose limitation.

Through this analysis, it becomes clear that data privacy issues exist even without Aadhaar. To tackle the risks to privacy, India requires a strong, competent and independent data privacy regulator, backed by a robust law.

With the recent Supreme Court judgement and upcoming hearings, we have a unique opportunity to strengthen our institutional ability to manage future risks. We must seize this opportunity to try and secure a privacy-protected future.

Ronald Abraham is a partner at IDinsight and co-author of 'State of Aadhaar' report 2016-17.

Research contributions from Shreya Dubey and Akash Pattanayak.

This is part 2 of a two-part series on Aadhaar and privacy.

END