A Question of Identity: What Should Aadhaar Be Like?

Soumen Chakrabarti* **Om Damani*** **Manoj Prabhakaran***
Krithi Ramamritham* **Bhaskaran Raman*** **S Sudarshan***

Dept. of Computer Science and Engineering
IIT Bombay

April 16, 2018
(With minor revisions on April 19, 2018)

Abstract: *A national identity scheme has long-term and large-scale implications to the welfare of the people, efficiency of governance and law enforcement, individuals' fundamental right to privacy and national security. Motivated by several issues surfaced by the implementation of Aadhaar, and several privacy and security concerns that have been pointed out, we develop a (non-exhaustive) list of* technical guidelines *for national identity schemes. We observe that the current Aadhaar design significantly deviates from these guidelines, strongly suggesting that to address the root causes of the issues that have manifested so far, many parts of the system require major redesign. We also put forth several* policy guidelines, *which we believe are crucial to the success of a national identity scheme in India.*

Digital technology is a powerful tool, and India, like any other modern nation, can ill afford to keep away from exploiting the promises it offers. Yet, one needs to wield this technology with caution, like a scalpel rather than a sledge hammer, especially when it is applied at a national scale and affects millions of the poorest and most vulnerable. One should also bear in mind that any cyber infrastructure that is being developed today will become targets for cyber warfare in the future.

Developing a secure and privacy preserving national ID scheme presents an unprecedented challenge for which no amount of expertise will be excessive. In this whitepaper we offer an analysis of some fundamental principles that such a system should aim for, based in no insignificant way on lessons drawn from the current Aadhaar experiment and the lively debate that it has resulted in.

Document Outline: We start by articulating a few fundamental expectations we have, on an identification system that is being put in place by the government. We go on to consider how the current Aadhaar system fares with respect to these expectations. Rather than attempt to fix individual issues, we identify a list of high-level *technical design guidelines* that address broad classes of issues. The current design is seen to significantly violate these guidelines. (We do not provide an alternate solution here, but in a forthcoming companion whitepaper we shall describe a

* Sorted alphabetically. Email: {soumen,damani,mp,krithi,br,sudarsha}@cse.iitb.ac.in

candidate scheme that adheres to these guidelines.) We also provide several policy guidelines geared towards creating a robust Aadhaar ecosystem.

Basic Premises

National identity schemes have been seen as tools for inclusion of marginalized groups, improving transparency and increasing the efficiency of administration.[1] Social inclusion is indeed one of the most prominently stated motivations for implementing Aadhaar.[2] On a related note, "right to identity" in the form of birth registrations has been considered a fundamental right of a child,[3] and a key ingredient in their well-being.[4] As such, we expect enabling social inclusion to be the primary focus of a national identity scheme.

An identity scheme is also seen as a tool to prevent identity fraud. Identity fraud is a growing concern, especially in today's age of digital transactions. It could take the form of identity theft (impersonation) or creating false identities, for gaining access to an individual's resources or for evading law enforcement while carrying out various other illegal activities. The perpetrators as well as victims of identity fraud can be individuals, criminal organizations, corporations or even nation states. An effective identity scheme could help in the fight against this growing malaise by making impersonation harder and traceability better.

On the other hand, incorporating an identity scheme into day-to-day transactions of people incurs costs that should be carefully controlled. Specifically, it should not lead to denying or disrupting access to essential services and critical infrastructure; this applies equally to the disruption caused in the normal course of the scheme's operation, and that caused by active attacks that exploit any vulnerabilities that the identity scheme created. Further, such a scheme should not violate individuals' fundamental right to privacy, and legitimate needs for anonymity. Again, this applies equally to possible privacy violations in the normal course of operation, and potential violations due to security breaches.

To reiterate, we shall expect a good identity scheme to *simultaneously* meet the following requirements:

- It should be a tool for improving inclusiveness, empowering the disenfranchised, and improving the efficiency of administration.
- It should not disrupt access to essential services, nor create vulnerabilities that can be exploited to cause such disruption.

---

[1] World Bank's "Identity for Development" initiative estimates that over a billion people worldwide are unable to prove their identities and argues that "achieving inclusive development ... requires a sustained effort to address the world's identification gap."

[2] The UIDAI website summarizes the Aadhaar identity platform as enabling "the Government of India to directly reach residents of the country in delivery of various subsidies, benefits and services…."

[3] E.g., Article 7(1) of the UN Convention on the Rights of the Child.

[4] According to UNICEF "Registering children at birth is the first step in securing their recognition before the law, safeguarding their rights, and ensuring that any violation of these rights does not go unnoticed."

- It should help in curbing identity fraud, even if some of the administrators and systems employed by the scheme are compromised.
- It should not violate individuals' fundamental right to privacy, nor create vulnerabilities that can be exploited to cause such violation.

In the sequel, we consider all these requirements to be equally important when designing an identity scheme. While we believe that the current design of the Aadhaar ecosystem is mindful of these demands, its implementation often trades off all the other expectations listed above in favour of preventing identity fraud.[5] As we shall argue, such stark trade-offs are not always necessary (or justified). Indeed, we argue that today's technology would allow us to greatly *improve* on all the above aspects simultaneously (compared to the situation of not using an identity scheme), rather than trade them off against each other.

Lessons so far

The scale and speed at which Aadhaar enrolments have been implemented, reaching out to over a billion Indians, is quite impressive. Yet, the current Aadhaar design has attracted much criticism on various fronts. We briefly examine how it fares with respect to the expectations above.

With respect to ensuring social inclusion, Aadhaar's *potential* is arguably on par with that of the other identity schemes existing in India. While Aadhaar has enrolled a large fraction of the population, almost all of these individuals already possessed other identity documents.[6] On this front, the exact nature of the identity scheme is perhaps not as critical as just reaching out to the people with basic services and establishing a steady communication channel between the populace and the responsible authorities. But unfortunately, the way Aadhaar has been deployed on ground, perhaps with a singular focus on fraud prevention, appears to have led to much social *exclusion*. This relates to the next expectation in our list above: While in principle, providing everyone with a uniform identity document could streamline administrative processes, the move to use Aadhaar-based authentication in the Targeted Public Distribution System (TPDS) and pension schemes has led to several alarming reports of denied services.[7]

With respect to preventing identity fraud too, the current system has revealed several cracks. It has been seen to place too much trust on third-party service providers (e.g., mobile phone operators and payment banks) and numerous enrolment agencies, providing them, as well as others, with new opportunities to commit identity fraud.[8] Several mobile applications and online services built

[5] It has also been observed that many commercial interests are intertwined with the design of the Aadhaar ecosystem. We expect that the businesses built around Aadhaar will evolve around the design of the ecosystem, rather than the other way around, and hence commercial considerations are not part of our basic premises.

[6] As of October 2016, with over 105 crore residents already enrolled, less than 0.1% did not have alternate identity and residence proofs.

[7] A few such instances were reported here, here, here, here and here.

[8] A few such instances were reported here, here, here, here and here.

on top of the Aadhaar ecosystem have been revealed to have serious security vulnerabilities.[9] One particularly concerning set of applications involve the use of Aadhaar authentication as part of authorization. This was illustrated by a case of diversion of Direct Benefit Transfers to payment bank accounts opened without the knowledge of the users.[10] As another example, a protocol for "e-registration" of property rental agreements in Maharashtra leaves open the possibility of agreeing on one document with a party while actually registering a different one, without the party realizing the switch.[11] In fact, given the the ubiquitous use of biometrics in the Aadhaar ecosystem, it is also possible to obtain the requisite fingerprints in the pretext of carrying out an entirely different transaction. Another set of vulnerabilities arise from the manner in which Aadhaar has been linked to various services, leading to a major risk of phishing attacks.[12]

We note that some of the above vulnerabilities can be traced to the confusion among the multiple roles Aadhaar plays. The current Aadhaar ecosystem is being used for unique identification (by UIDAI as well as by third party service providers), for authentication (i.e., matching an individual with their ID), for "KYC" (i.e., obtaining and verifying information associated with an ID), for authorization (i.e., creating a proof that a transaction was approved by an individual), as a convenient repository for multiple certificates/documents (called DigiLocker), etc. Further, Aadhaar is used to uniformly authenticate individuals with a variety of big and small service providers, who may not all need the same level of authentication of their customers.

Finally, Aadhaar has received a lot of criticism on the privacy front. Aadhaar ID, by design is a perfect instance of personally identifiable information and, when part of leaked data, it compromises the privacy of the affected individuals in an unprecedented manner. Unfortunately, it is virtually impossible to guarantee that data leaks will not occur from any of the various governmental and private services that use Aadhaar IDs, irrespective of how secure the central database itself is.[13] Another major privacy concern arises from the hundreds of Authentication User Agencies (AUAs) that funnel authentication requests from several service providers to UIDAI: these loosely regulated entities can track individual users across multiple service providers who use their services.[14]

---

[9] "Insecure App Making." Karana, September 2017.
[10] E.g., see "The Airtel-Aadhaar fix." Frontline. January 2018.
[11] The registration process assumes that the individual providing the fingerprints are aware of the exact sequence of steps, and is personally reading the messages shown to them on a screen. There is no safeguard against showing the individual messages from a simulated transaction involving a different document.
[12] As of this writing, searching for "Aadhaar link" on Google Play Store returns several questionable apps offering to "link" Aadhaar with various services (as repeatedly required by various government agencies).
[13] One such leak in April 2017 exposed over a million pensioners' details (including Aadhaar ID and details of their pensions). Over 200 such instances involving governmental agencies had been recorded by July 2017.
[14] While a proposed Aadhaar API version 2.5 (March 2018) requires certain information to be encrypted, tracking of users needs only the metadata in this API. Specifically, the "UID token" shared with an AUA is designed to remain constant for a given user *even if the user changes their Virtual ID across transactions*. Indeed, this "feature" serves no other purpose other than allowing AUAs to (continue to) track users when virtual IDs are used in lieu of Aadhaar IDs. Collusion or a side-channel with a single service provider lets the AUA fully identify and track the user across all service providers that use that AUA.

It must be appreciated that efforts are underway to address *some* of these issues, leading to a few changes in the design of the Aadhaar system (though we note with concern that such revisions are not accompanied by any admission of fault). However, it needs to be seen if such changes are sufficient, and if they will address the *root causes*. Many of these issues arise from a complex web of socioeconomic and technological factors. It is also possible that many problems that cause hardships to the poor and under-represented may not even have been recognized as issues that need solutions. So rather than find *ad hoc* solutions that address currently known issues individually (an instance of "overfitting"), we seek to formulate a short list of simply stated design and policy guidelines which would have prevented many such issues from arising.

Use of Biometrics: Lessons from Around the World

General purpose, centralized national identity databases, with personal information like photographs or other biometrics, have been considered in several countries over the years. One of the earliest proposals for such a database was the *Australia Card* initiative (proposed in 1986), but it was never enacted.[15] In the United Kingdom, such a scheme was implemented, but then withdrawn.[16] A similar debate arose recently in Israel, over a national identity scheme which originally mandated collecting biometrics of citizens. Among other protests, several Israeli cybersecurity and cryptography experts raised security and privacy concerns.[17] The eventual law enacted last year made providing fingerprints optional, while mandating photographs.[18] Countries like Estonia and Belgium have advanced national identity schemes that do not collect biometrics.[19] In Portugal's Citizen Card system biometrics are stored only on each individual's card, and biometric matching is carried out "on-card."[20] Many countries, including most European Union countries, use electronic-passports that contain fingerprint information of the passport holder, but do not store this information in a central database (nor use this information outside of border-control purposes).[21] In these cases, proposals for storing biometrics in centralized databases have always been avoided or have led to strong resistance.

On the other hand, several other countries in the developing world have nation-level biometric identity systems being built, many of them with support from The World Bank's "ID4D" initiative.[22] Pakistan[23] and South Africa[24] have built national biometric databases with scores of millions of fingerprints. Reports indicate that China is building an extensive multi-modal biometric database of

[15] "Just Another Piece of Plastic for your Wallet: The 'Australia Card' Scheme." Roger Clarke. June 1987.
[16] "Success Story: Dismantling UK's Biometric ID Database." The Electronic Frontier Federation.
[17] Three letters (in Hebrew) were written to the Members of the Knesset over a 6 year period, with the last one gathering signatures from 74 prominent scientists. This report summarizes the contents of the letter in English.
[18] "Israel Adopts Biometric Database Despite Security Concerns." Bloomberg BNA. March 2017.
[19] Identification for Development (ID4D) Integration Approach - Study. World Bank (2015)
[20] "Biometrics with strict confidentiality: The Portuguese experience." Gemalto.
[21] "Biometric passport." Wikipedia.
[22] ID4D Annual Report (2017) (pg. 21) lists its engagement with 32 countries.
[23] "Pakistan's experience with identity management." BBC News, June 2012.
[24] "South African ID card : identity and citizenship." Gemalto.

its residents.[25] Also, many governments, including in the European Union and the United States, maintain biometric databases of *non*-citizens who enter their territories.

We note that when biometrics are used, sometimes it is used for deduplication (ensuring that one individual is not given multiple identities) and sometimes for authentication (as a means to check that the individual presenting an ID is the same as the individual to whom it was issued). The former use often involves capturing significantly more biometrics than the latter (e.g., all 10 fingerprints instead of just two). In much of the developed world, citizens' biometrics, if at all used, are used for narrowly defined purposes of authentication in highly controlled settings (e.g., border crossings). It has been observed that the use of biometrics for social transfers is correlated with a poor democratic record.[26]

The best estimates of biometric matching failures in Indian conditions is provided by the current Aadhaar system itself. Estimates for the rate of biometric authentication failures in the field(when users who had already successfully enrolled in the Aadhaar system try to authenticate themselves using biometrics to third-party service providers) are significantly higher than that during the registration process.[27] We note that if there are crores of authentication requests per day,[28] even an accuracy rate of 99.95% leaves lakhs of people affected every month.

Co-existence of Multiple Identity Schemes

Before proceeding further, we clarify that we assume that there could be several other valid identity schemes in the country (e.g., passports), and a newly designed scheme like Aadhaar will co-exist with them. We take the view that enrolling in any of these schemes will be voluntary, in accordance with the current laws of the land.

We also leave open the possibility that the Aadhaar system itself could be implemented as a *federation* of multiple identity systems. The technical guidelines below would then apply to each of these systems, as well as to their collection as a whole. But there will be several additional guidelines that will need to be developed to ensure seamless and secure interaction among the multiple systems. We shall leave these details outside the scope of the current document.

---

[25] "China: Voice Biometric Collection Threatens Privacy." Human Rights Watch. October 2017.

[26] "Are countries with a poor democratic record more likely to mandate an Aadhaar-like ID?" *Scroll.in*, Sep 2017.

[27] A report by UIDAI estimated 0.057% false matches *during* the registration process, but UIDAI CEO's recent response to queries in the Supreme Court shows a 6.00% error rate for fingerprint authentication in general, affecting almost 37 million transactions (it is not clear, which period is considered for these statistics). Also there are numerous reports of biometric errors when users attempt to authenticate for access to services (e.g., here, here, here, here and here).

[28] As of 2017 January, UIDAI was reportedly receiving over 2 crore authentication requests per day. (It is not clear what fraction of these involve biometrics.)

Technical Design Guidelines

We list a few "principles" that we believe a robust Aadhaar system should adhere to. We do not yet offer a solution ourselves, but rather collect guidelines against which the current and future designs can be evaluated. These desiderata are motivated by the lessons above (as well as basic security and privacy considerations). But we caution the readers that this should only be taken as a preliminary list. Indeed, we are guided by the point of view that a complex system such as Aadhaar, with multiple human and socioeconomic factors affecting and affected by it, should be designed with inputs from many experts, over several iterations of design, (shadow) deployment and analysis, and we do not intend to contradict that view here.

Below, for the sake of familiarity, we shall write UIDAI to denote the authority in charge of implementing the identity scheme. (But as mentioned above, there could be several such authorities who interact with each other.)

- *Separation of well-specified functions*: If the Aadhaar ecosystem is used for different functions (like identification, authentication and authorization), each function should be formally well-specified, including its goals and operating assumptions. Users should have fine-grained control over (and knowledge of) the functions invoked at any point.

- *Minimal dependence on biometrics:* If biometrics are used, it should only be used by UIDAI for "deduplication." Third-party service providers should not require users to provide biometrics to devices at their premises (and instead rely on other more *reliable* and *resettable* mechanisms like OTP, Chip and PIN, etc. for authentication).

- *Minimal need for interaction with remote servers*: Centralized servers present several problems: they are prime targets for cyber attacks, network connectivity failure is bound to occur at a non-negligible rate, and the intermediaries between service providers and such servers create privacy, security and regulatory concerns. Hence, most of the functionality should be reliably available to users and service providers without the need to contact a remote server in real-time.

- *Minimal collection/storage of information:* To reduce the value of UIDAI servers as a target for cybercrime, the amount of personal data collected or stored should be minimized. As much as possible, each user's data will be stored by that user (e.g., on a smart card) and should not be present in a server. When data is stored remotely (e.g., for the purposes of deduplication), cryptographic methods should be used to protect it.

- *A strong adversary model and graceful degradation*: It must be assumed that several users and several service providers who use the Aadhaar services (including government agencies) are "adversarial" (due to malicious intent, human errors or software glitches).

Their devices or smart cards could be compromised and they could arbitrarily collude with each other, and this should not affect anyone else's security. UIDAI's own service centres should be considered vulnerable, and their compromise should have only limited and revocable impact on the overall system. Equipment manufacturers and software providers should also be considered as untrusted, and protected against (e.g. using designs which combine multiple components from multiple providers, in a fault tolerant manner).

- *Responsible tracking*: It should be infeasible to track any individual's Aadhaar transactions just based on the information collected by UIDAI, or that collected by a set of service providers. Yet, technically, there can be provisions (protected by a strong legal framework to prevent abuse) for tracking individuals when there is due cause, with the active participation of multiple stakeholders and watchdogs.

- *Be the mechanism of choice for the privacy conscious*: We seek to turn Aadhaar into a platform that will provide strong privacy guarantees, better than what is on offer without Aadhaar. In particular, by using Aadhaar, individuals can avoid providing personal information (authenticated or otherwise) to service providers beyond what is absolutely needed for providing the service.[29]

Current Aadhaar vis a vis the Guidelines

In its current avatar, Aadhaar contradicts several of the above guidelines, each of which we examine below.

Firstly, as noted earlier, multiple functions have been conflated together in the current Aadhaar ecosystem. For instance, unique identification by the government has been conflated with unique identification by each service provider (proposed use of "Virtual IDs" only partially remedies this issue). Also, identification is conflated with authentication, as a service provider intending to capture a unique identification for a customer is expected to authenticate the individual in person (ruling out, for instance, the possibility of allowing a proxy to approach the service provider). The distinction between authentication and authorization is also blurred, as providing biometrics for authentication is taken to imply authorization transactions that the users may not be aware of. The ability in the current system to collect biometrics under one pretext and use it for another purpose violates our guideline that the users must have fine-grained control over the functionalities being invoked (as well as the guideline that biometrics be used only by UIDAI for deduplication). Yet another issue is that a facsimile of an "Aadhaar card" is often accepted as a proof of identity and address, while the card itself provides little security against forgery. (Incidentally, the information collected at the time of Aadhaar registration itself is largely unverified.)

[29] For instance, a mobile phone subscription does not require the service provider to learn anything about the subscriber (given a security deposit to protect against payment defaults). A cooking gas cylinder subscription (without subsidies) would require the user to provide the address at which the cylinders are to be delivered.

The way biometrics are used in the current design of Aadhaar violates many sound security principles and practices. The design crucially depends on fingerprints being secret (as they are used by various service providers to authenticate users), but they are easy to steal and forge, and cannot be revoked. The situation is aggravated by the fact that the users are expected to expose their fingerprints to a wide variety of devices operated by entities, some of which may be compromised,[30] making fingerprints all the more vulnerable in the Aadhaar ecosystem. Incidentally, even the design choices in specifying secure biometric capture devices are problematic.[31]

The authentication protocol violates several of our principles, apart from the way biometrics are used. The service provider needs to contact the server with the biometric for verification. This exposes all service providers to the threat of large scale disruptions if the Aadhaar services were to become temporarily unavailable. In addition, the authentication requests reveal tracking information to UIDAI. Further, such information is stored for long periods, violating the principle of minimal storage. Also, the third-party service providers are trusted not to trick users into authorizing transactions with other colluding service providers.

Towards Alternatives

Given the serious shortcomings the current design of Aadhaar has with respect to the above guidelines, one needs to explore alternatives. There have been some proposals in the literature which are likely to fare better.[32] We believe that a robust (and affordable[33]) solution can be based on secure smart cards issued to each user. These smart cards can interact with devices owned by the third-party service providers to reveal minimal amount of information to them, while making it possible to invoke tracking later on. Cheaper, but less functional temporary alternatives are also possible. In an upcoming companion whitepaper we shall elaborate on a candidate design that stays much more faithful to *all* of the above guidelines.

Policy Guidelines

Aadhaar is a complex system, and it is not easy to formulate foolproof policies that cover all eventualities adequately. As such, it is important to involve a diverse collection of institutions, experts in various fields, various stakeholders and individuals while drafting policies. Agencies like

[30] Mandating secure biometric capture devices is not sufficient protection, as a user will not typically be able to distinguish between a fake device and a genuine one.

[31] Aadhaar Authentication API 2.0 (2017) uses a long term public-key encryption key for UIDAI, violating the principle of forward secrecy. Further, the choice of using a 2048-bit RSA key is problematic given that prevalent estimates are that such keys provide only "112 bits" of security and would be unsafe past the year 2030.

[32] Specifically, Rajput and Gopinath (2017) and Agrawal et al. (2017) discuss alternate design choices.

[33] E.g., Pakistan's biometric-based national identity scheme currently uses a "Smart National Identity Card" which is issued for a modest fee of PKR 400 (roughly INR 225, currently).

TRAI routinely put out "consultation papers" to solicit inputs from the public and industry.[34] We strongly believe that UIDAI should follow a similar approach to policy framing.

Having said that we offer a few policy suggestions ourselves.

Protect Users from Illegal Data Collection. It should be illegal for service providers to ask for data not required for the service. But without strict enforcement and awareness, service providers can coerce users into revealing personally identifiable information and other personal data (for instance, to track users across multiple services). There should be strict penalties for service providers who acquire data illegally (or via loopholes), and there should be campaigns in place to educate the population about personal data privacy.

Protect users against the "kill switch." A key concern about "linking" everything to a national identity system is that governments can cause "civic death" of a user by suspending the functionality of their identity. It should be ensured that provisions designed for fighting fraud and crime can only be narrowly targeted (e.g., freezing all bank accounts) and not devolve into a "kill switch." A strong legal framework and safeguards like judicial permission, auditing and transparency should be in place to ensure this.

Plan for Exceptions. UIDAI should consider many possible exceptional conditions and carefully specify how to deal with them. A list of exceptions should be crowd-sourced and curated. The protocols for handling exceptions for an individual user should not unduly inconvenience the user, and if necessary temporary workarounds should be facilitated. Serious security exceptions should be anticipated (e.g., vulnerabilities are routinely discovered in implementations of cryptographic protocols).

Easy and Efficient Grievance Reporting/Redressal: It should be easy for the users to report usability issues, bugs and security vulnerabilities via a variety of channels (phone, social media, UIDAI website etc.), and track the status of these reports openly. (For major security vulnerabilities, a responsible disclosure policy should be encouraged, by providing a private reporting facility with a guaranteed resolution deadline.)

Plan for an Evolving Technical Design: Many design choices currently used are debatable. Further, technological advances will introduce new implementation options, or change the cost-benefit analysis. Hence, the design of the system should stay open to major revisions.

Also, there should be a transparent mechanism to collect statistics relevant to Aadhaar and make them available to researchers. The goal of this exercise should be to improve the design and not to simply support current design choices.

[34] TRAI public consultation website.

There should be a detailed plan for phased roll-out of updates (with minimal inconvenience to the users), rollbacks when security vulnerabilities or serious usability concerns are uncovered, fallback plans with graceful degradation of service if various components in the system fail or come under sudden cyber attacks. There should be sustained research and development efforts aimed at improving the design and carrying out thorough analyses of all aspects of the Aadhaar ecosystem, and there should be a plan to incorporate outcomes of these efforts into the deployment.

Accept liability and insure users. Aadhaar is an evolving technology with a large footprint. There have been several instances where technical issues with the use of Aadhaar have greatly inconvenienced many people, often from the most vulnerable sections of the society. The resulting damages are entirely borne by the users, even though they are not at fault. In contrast, laws regarding technologies like credit cards largely indemnify its users from losses (say, due to fraud). UIDAI must protect the users of the Aadhaar ecosystem - individuals and businesses - possibly in the form of an insurance scheme, to compensate them for damages due to issues in the ecosystem. An independent agency should be in charge of taking speedy decisions on loss claims (and for suo moto initiating claims when appropriate).

Informed Choice: Enrolling in Aadhaar should be purely voluntary and this should be well-advertised. Any services built on Aadhaar should be required to provide reasonable alternatives for those who have not opted in. Also, there should be wide-spread awareness about the restrictions on third party service providers (e.g., they shall not collect biometrics in the name of Aadhaar). There should be well-advertised means for individuals to report denial of service or coercion, and such reports should be swiftly acted upon. UIDAI can promote Aadhaar by advertising the conveniences and enhanced privacy it offers to the individuals. But potential risks should also be openly discussed (by UIDAI and others) so that individuals can make an informed choice.

Right to Erasure: Given that enrolling in the Aadhaar system is voluntary, staying in the system should also be voluntary. Individuals should have the option of unenrolling themselves, resulting in time-bounded erasure of their biometrics and contact information, and cancellation of their Aadhaar ID and all associated data. An erasure protocol needs to be carefully specified to (a) retain the ability of tracking for a bounded period of time (e.g., one year), and to (b) protect the individual, as much as possible, from retroactively losing the anti-tracking protection that Aadhaar had accorded them. It should also specify how to handle re-enrollment (before the biometrics are erased). Erasure also entails monitoring the account for some set period against identity abuse.

Security Measures Against Insiders and the Government: As a security measure against insiders, not even system administrators should have illegitimate access to any of the data in the system. This should be ensured using a defense-in-depth approach, combining cryptographic techniques (e.g., secure multiparty computation) and secure hardware (e.g., processors that support encrypted memory). The system should also be resistant to changes in protocol, even if ordered by the government, without alerting several officials. Also, the system should combine multiple components developed by different teams or corporations in a manner that can tolerate the corruption of a few of them.

Tracking Policy: There should be strong legal safeguards against invoking provisions for tracking individuals, and technological safeguards to ensure that it is possible only with the consent and active participation of several stakeholders. If an individual was tracked for investigation, and the investigation shows that there was no due cause, then the individual's privacy needs to be restored. The technical design should provide mechanisms for this. Also, the individual should be notified about the investigation, so that they can take proactive steps for recovering their privacy.

Conclusion

Digitized national identity schemes offer many benefits, if designed safely and securely. The current Aadhaar implementation effort, despite several problematic design choices, has set us on a path towards such a scheme.

But it is important to bear in mind that Aadhaar is not a panacea to all the ills of the society. While it may help in fighting large scale identity fraud and related crimes, it may not by itself offer a solution against exploitation of the poor and vulnerable. Indeed, though preventing pilferage in the Targeted Public Distribution System (TPDS) and government subsidies has been seen as a driving application for Aadhaar, there is much evidence that such a technological solution does not prevent corruption, but only changes the form in which corruption manifests.[35] Instead, Aadhaar should be seen as providing an auditing mechanism that can empower individuals and communities against exploitation. This point of view has an important implication to the design choices we make: An auditing mechanism should not disrupt the primary functionality of the services it protects. Hence it becomes incumbent upon the designers of the system to make it as non-intrusive as possible.

One may ask if it is too late to reengineer a system that has over a billion people already enrolled. Thankfully, the answer is no. A new system, as we envisage, can leverage much of the investment that has already gone into the current system. But much thought, consultation, additional expenses (e.g., for issuing smart cards) and a few more years will be needed to design and deploy a robust system that can withstand the myriad challenges faced in creating a modern identity scheme for the largest democracy in the world. Meanwhile, we recommend that the current system be considered experimental and used accordingly.

Acknowledgments

We gratefully acknowledge our colleagues at the Computer Science and Engineering department at IIT Bombay, as well as visitors to the department and commenters on early drafts, for inputs that contributed to this whitepaper.

[35] E.g., "Can biometrics stop the theft of food rations? No, shows Gujarat." *Scroll.in*. December 2016.