UIDAI's Public Policy Innovations

30 August 2016

Ram Sewak Sharma
Telecom Regulatory
Authority of India,
New Delhi
rssharma3@gmail.com

Abstract

The Unique Identification Authority of India (UIDAI) was mandated to issue unique identification numbers to every resident of India. The Authority has largely accomplished this mandate in a short time and within budget because it took many innovative and bold decisions.

The first innovative decision we consider in this paper is the UIDAI's decision to add iris images to the set of biometrics collected by it. Another innovation of the UIDAI was its practice of conducting on-field trials. The last innovation we consider relates to how the UIDAI promoted competition and standardisation.

The success of the UIDAI offers lessons for other government projects. Government processes need not prevent it from taking innovative decisions. High-quality procurement and project management skills can help the government outsource many functions that are currently housed within it. Testing major hypotheses through field trials before launching projects at scale can help ensure best use of public resources.

NIPFP Working Paper No. 176, September 2016. The views expressed in the paper are those of the author. No responsibility for them should be attributed to NIPFP.

The author is thankful to Professor Ajay Shah and Mr Prasanth Regy of the National Institute for Public Finance and Policy (NIPFP) for giving detailed comments and suggestions on an earlier draft. He also thanks Ajay Shah, Prasanth Regy, and Sanjay Jain for helpful discussions and suggestions on improving the paper.

Contents

1 Introduction

The Unique Identification Authority of India (UIDAI) was mandated to issue unique identification numbers to every resident of India. In a country as large as ours, this was a very difficult task to achieve. But the UIDAI has largely accomplished this mandate within a short period of about six years. It was able to do this only because it took many innovative and bold decisions. This article seeks to examine some of these innovations. It also tries to derive lessons from UIDAI that could be applied in other government projects.

As an example of an innovative decision, consider UIDAI's decision to add iris images to the set of biometrics collected by it. The UIDAI felt that unless iris images were used in addition to fingerprints, it would not be able to fulfil its mandate of unique identification. However, there were many concerns related to the use of iris images. Was this technology mature enough? Was it too expensive? Were there enough vendors in the market to prevent lock-in?

The UIDAI set up a committee to deliberate on the issue of which biometrics to collect and what standards to use for unique identification. This committee recognised the value of using iris images in improving accuracy. However, it fell short of recommending the inclusion of the iris in the biometric set and left the decision to UIDAI. After a detailed examination, the UIDAI came to the conclusion that the inclusion of iris to the biometric set was necessary for a number of reasons, such as ensuring uniqueness of identities, and achieving greater inclusion. In retrospect, this turned out to be one of the most important decisions of the UIDAI.

Another innovation of the UIDAI was its practice of conducting on-field trials. When the UIDAI began its mission, there were many questions inside and outside the organisation on whether the very idea of unique identification for every resident was feasible at all. The idea of using biometrics to ensure the unique identification and authentication of all the residents of India was an untested one. There were many assumptions behind it, and the data required to test the validity of these assumptions was not available. For instance, most of the research done on using biometrics for identification or authentication was done in western countries, and that too, on relatively small numbers of people. Would these findings apply to India? Could the fingerprints of rural residents and manual labourers be captured successfully, or would they be excluded from Aadhaar? What about the iris images of old or blind people? Do the devices available in the market serve the purpose? What would be the most efficient and effective way to organise the process of enrolment? These questions needed to be answered rigorously if the project was to be successful.

The UIDAI conducted a set of trials (called Proofs of Concept, PoCs) in several states across the country. The areas were selected to be representative of real-life enrolment and authentication. A number of biometric capture devices of different makes were used, and several different enrolment processes were tried out. The PoCs were carefully designed to answer sharply articulated questions, either to verify UIDAI's assumptions, or to capture the data required to fill in gaps in the UIDAI's knowledge.

The results of the PoCs indicated that the major hypothesis of the UIDAI was correct: that it was possible to capture biometric data that was fit for the purpose of deduplication and verification. The results also showed that iris capture did not present any major challenges. An efficient enrolment process was devised using the data captured during these trials.

The last innovation we consider in this article relates to how the UIDAI promoted competition and standardisation. Given the scale and importance of the project, the UIDAI felt it was important to increase efficiency and reduce costs by leveraging the competencies available in the private sector. At the same time, it was also essential to avoid a situation where any one private player could exercise significant power over the effective functioning of the Aadhaar system: the Authority wanted to ensure that there was a competitive market for providing services to it. To promote such a competitive market, the Authority used a two-pronged strategy of using open standards (creating standards where there were none), and using open APIs (Application Programming Interfaces).

The Authority used this strategy in procuring vendors for deduplication. Algorithms for deduplication had never been tested at the scale required in this project. To reduce the risk of poor quality deduplication, the UIDAI came up with a very novel solution. It decided to engage three biometric service providers (BSPs), instead of just one. These BSPs would interface with the UIDAI systems using open APIs specified by the Authority. This decision helped avoid vendor lock-in, and increased scalability.

The UIDAI selected the three top bidders on the basis of the total cost per deduplication. Even after these three vendors were selected, the Authority was able to set up a competitive market among them, using an innovative system to distribute deduplication requests among them. Vendors were paid on the basis of the number of deduplication operations they were able to carry out, and the Authority allocated operations to them on the basis of how fast and how accurate they were. This led to a situation where the BSPs were constantly competing with each other to improve their speed and accuracy.

Where standards were not present, the UIDAI was willing to create new standards in order to increase competition. Every biometric device had its own interface, distinct from the interfaces of other biometric devices. If a capture application wanted to support 10 commonly used devices, then the application developer would have to implement 10 different interfaces. This would have made it very costly to bring new devices into the project, even if these new devices were cheaper and better. In order to avoid this situation, the UIDAI created an intermediate specification. Vendors could implement support for this specification, and their devices could be certified. This allowed all capture applications to work with all certified devices.

The success of the UIDAI offers many lessons for other government projects. Perhaps the first lesson we can draw from it is that innovation is indeed possible within the government. Government processes need not prevent it from taking innovative decisions. In fact, processes commonly used within the government, such as expert committees and consensus-based decision-making, can provide methods to examine difficult issues in a credible manner. High-quality procurement and project management skills can help the government outsource many functions that are currently housed within it. Large scale and complexity need not be deterrents to private sector participation: the scale can make the project more attractive to private parties. Another lesson government agencies could learn from the UIDAI is the need to test major hypotheses through field trials before launching projects at scale. Conducting such field trials provides an opportunity to change the design or the implementation roadmap well in time, thus saving precious public money from being wasted.

2 The Background

2.1 Aadhaar

The UIDAI is mandated to assign unique identification numbers to every resident of India. These 'Aadhaar' numbers are 12 digits long. The Authority attempts to guarantee that:

1. Every resident of India has one Aadhaar number (inclusion)
2. Every resident of India has only one Aadhaar number (uniqueness).
3. Every person who has an Aadhaar number can use it to validate the identity he claims (authentication).

To achieve this, the UIDAI has collected biometric and demographic data of residents and issued Aadhaar numbers to them. As of July 2016, it has issued over a billion Aadhaar numbers, and authenticates about seven million people every day (UIDAI 2016). To enrol such a huge number of people while ensuring uniqueness, and then to ensure that they can be accurately authenticated, is a significant feat in the area of public policy. This paper attempts to highlight some of the key innovations implemented by the UIDAI that were critical to achieving this feat.

2.2 Mechanics of Aadhaar

When a person enrols for Aadhaar, all ten fingerprints and images of both the iris are captured, along with a photograph and his or her basic demographic data. Before the person is given a new Aadhaar number, the biometric features of this person are compared with the biometrics of all the persons who have been allocated Aadhaar numbers earlier.

If the biometrics of the person match with biometrics already present in the gallery (the database of all the people already enrolled), it means that that person has already been enrolled, and that he or she is trying to enrol again. The system rejects this attempt. This prevents issue of two Aadhaar numbers to the same person. If the biometrics do not match any other person's biometrics, then the person is issued an Aadhaar number. He can now use this number to authenticate his identity.

However, testing for uniqueness or for authentication both involve checking for matches between biometrics, and these checks are not infallible. Algorithms to determine whether two biometrics are the same do not look for an exact match, because multiple captures of the very same biometric might vary. Instead, they use a threshold: if the match between the two biometrics exceeds the threshold, they are considered identical, and else, they are considered different. Setting the threshold to any particular value forces a trade-off: if the value is too high, two captures of the same biometric may be considered different, and if the value is too low, then different biometrics may be considered identical.

Correspondingly, there are two possible errors that can arise at the time of initial deduplication (UIDAI 2010b). A person who is new to the database might be mistaken for another person who already exists in the database, and he might thus be denied an Aadhaar number. The likelihood of this is called the False Positive Identification Rate (FPIR). This will prevent the person from getting an Aadhaar number, even if he has not got one earlier.

The second error is that a person who already has an Aadhaar number enrols again, and he is not detected to be already present in the gallery. The likelihood of this happening is called False Negative Identification Rate (FNIR). This would enable the same person to have two (or even more) Aadhaar numbers. The principle of ensuring the uniqueness of identities would be violated, and such a person would be able to receive more benefits or services than he is entitled to, using his multiple avatars.

Once enrolled, UIDAI enables a person to authenticate himself. Here, a person claims to have a certain Aadhaar number, and provides his biometrics. UIDAI compares the biometrics associated with that Aadhaar number with the submitted biometrics, and provides a Yes or a No, confirming or denying that the person is who he claims to be.

Again, two kinds of errors are possible here. The biometrics of a person who falsely claims a different identity might be erroneously found to match that identity, and UIDAI would thus confirm him in his false claim; this likelihood is called the False Acceptance Rate (FAR). The person would be able to impersonate others and avail services and benefits meant for them.

Another possibility is that a person might make a true claim about his identity, but his biometrics may not match his previously captured biometrics, and his claim might be rejected. This likelihood is called the False Rejection Rate (FRR), and such an event would prevent the person from availing services that he is entitled to.

Ideally, there should be no false rejects and no false accepts. Generally, both cannot be made zero: there is an inverse relationship between these two parameters. Tightening the system so as to reduce the false accepts may result in more false rejects, and vice-versa. However, it is possible to ensure that both have very low values — thus effectively eliminating false acceptance and false rejection.

2.3 Scale

These issues are compounded by the fact that the scale of the UIDAI project was unprecedented. Concerns were raised (Ramakumar 2010; Standing Committee on Finance 2009; Mathews 2016) that biometric deduplication and authentication may not work in India. While these concerns were addressed by the UIDAI, it was not clear in the beginning that this problem would be solvable.

Internationally there are many other biometric programs, but none that approach the magnitude of Aadhaar: 1.2 billion people, many of whom have biometrics that are not easy to capture and verify. Enrolling all these people and capturing their biometrics is in itself a challenging task. Deduplicating them at a rate that kept pace with enrolments, and providing quick responses to authentication requests, would both be tasks with no parallels anywhere.

The scale of the problem imposed limitations on the accuracy requirements of deduplication and authentication. Deduplication algorithms had never been tested and scaled up to such numbers. Apart from the accuracy, speed was another concern. The speed of algorithms normally depends on the input size (in this case the number of persons who have already enrolled), and the execution time can become very large as the gallery size increases. As there were no deduplication algorithms in the public domain, it was not known how the algorithms will behave at large input sizes. The computational complexity is a multiple of the gallery size and the number of enrolments on any given day. As an example, if we have issued Aadhaar numbers for 750 million people and we have to enrol 1 million people per day, the worst-case number of comparisons required will be $750 \times 10^6 \times 10^6 \times 12$, which is 9 quadrillion.[1] If deduplication could not happen fast enough, then Aadhaar applications would pile up while the system was busy disposing of previous applications.

2.4 UIDAI's approach

In this article, we would like to point out some of the major innovations in the approach that the UIDAI took. A major innovation was the addition of iris images to the set of biometric data captured by the UIDAI. This had never been done at this scale, and the technology's ability to handle UIDAI's requirements was unproven. Another innovation was the proactive approach taken by the UIDAI to establish standards and promote competition. A third was the frequent field trials performed by the UIDAI, in order to test its hypotheses relating to the feasibility of enrolments and biometric capture. Each of these played an important role in the successful execution of the project.

3 The Use of Iris Images

3.1 The Problem

The Unique Identification Authority of India, as its name suggests, had a mandate to devise a method to *uniquely* identify every resident of the country. Thus unique-

[1] We multiply by 12 because there are 10 fingerprints and 2 iris images.

ness and inclusiveness are both central objectives of the UIDAI. The question of which biometric, or which combination of biometrics, can serve these objectives, was a major concern. Besides, most academic studies of biometrics had been done in the west. It was not clear that these results would be applicable to Indian conditions.

3.2 How Iris Images could help

The Authority set up a Biometric Standards Committee in order to understand which biometrics needed to be used, and to determine the standards applicable to these biometrics. The Committee assessed that fingerprint images alone could suffice for a deduplication accuracy of about 95% (UIDAI 2009). However, given the large population, this may lead to a very large number of duplicates in the system. For illustration, if we assume that 0.05% of the population tries to register twice, the number of people that have duplicate Aadhaar identities would be as high as 1.2 billion $\times 0.05\% \times 5\% = 30,000$. Recognising this, the Committee also suggested that in order to improve the accuracy of the enrolment process, iris images could be collected as a third biometric, in addition to face photographs and fingerprints.[2] Since the iris is an independent modality, it could improve deduplication accuracy significantly. It may be noted that the Committee did not go so far as to recommend the use of the iris; it left the decision to the UIDAI.

Another motivation for the use of the iris was achieving greater inclusion (UIDAI 2010a). The quality of fingerprints varies significantly with the occupation of the person. Those who perform more physical labour may have worn-out fingerprints, and inability to capture their fingerprints could lead to their exclusion. This is especially true of the poor, who are in any case the most likely to be excluded from the services of the State. The UIDAI was especially conscious of the need to ensure the inclusion of such people. The iris is protected against damage and wear, and remains more stable than fingerprints over long periods of time. Thus, the iris biometric is very useful as an additional mechanism for ensuring uniqueness, as well as enabling authentication.

Iris images are also more useful than fingerprints and photographs from the point of view of security. It is relatively easy to disguise facial features. It may even be possible in some cases to defeat fingerprint-based authentication. But disguising the iris is very difficult. So iris-based authentication could be used for applications where security is especially important, such as access control or financial transactions.

[2] While a photograph of the face was also captured, it was not used for deduplication.

The addition of the iris biometric also helped avoid vendor lock-in. The fact that the iris is an independent modality with very high accuracy, gave the UIDAI the freedom to avoid proprietary end-to-end solutions for deduplication. Instead, the Authority was able to go in for best-of-breed solutions, spurring competition and reducing cost, while achieving high accuracy.

The use of iris had other advantages as well. Capturing the iris image is similar to taking a photo, an experience most people are familiar with. No physical contact is required. Iris images enables the inclusion of children, since the iris stabilises by 4 years of age, while the fingerprint stabilises only by about 15 years of age. Iris deduplication is faster than finger-print based deduplication, so the process of enrolment does not get held up. As an uncorrelated mode of deduplication and authentication, iris provides some insurance as well: if, in the future, it turns out that there are fundamental issues with any one modality of deduplication or authentication, the presence of another modality will be very important.

3.3 Constraints on the use of the Iris biometric

The decision of the UIDAI to add the iris to the biometric set and use it for deduplication was a bold one. A major concern at the time was the maturity of the technology. While fingerprints had been in use for 150 years, the patent for using iris images for identification was granted as recently as 1994 (Daugman 1994). There were doubts about how well the technology would suit the purpose. For instance, there were reports that iris-based authentication system deployed at U. K. airports in 2004 had a high FRR, and the system was later scrapped (BBC 2007; BBC 2012).

However, there was also evidence that the technology had achieved high accuracy and speed. The U. S. National Institute of Standards and Technology (NIST) had evaluated several commercially available iris identification algorithms, and determined that the technology had achieved standards of accuracy comparable to fingerprints (Grother et al. 2009).

Another concern was whether, having decided to use the iris biometric, the UIDAI would be beholden to one or a few vendors. If vendors used proprietary technology, then the UIDAI would be tied to one company and would not be able to migrate away due to high costs of switching. In such a scenario, the vendor would be able to charge exorbitant prices. The Authority determined that the risk could be mitigated by a policy of promoting more vendors, following standards, and creating standards where required.

The Authority also evaluated the cost of collecting iris images. The major cost during enrolment is travel and logistics. The marginal cost of collecting and using iris images was estimated to be around Rs 4.40 per person. It was felt that the benefits that would follow from the increased confidence in unique identification, inclusion, and authentication would be well worth the additional Rs 500 crore that would be required for collecting iris images for the entire population.

Of course, there still remained a major risk: the fact that there was no prior example of iris images being used for deduplication or for authentication on such a large scale. To mitigate this risk, the UIDAI tested it out on the field, in several Proofs of Concept (PoCs). These PoCs are described in section 4 of this article. The results of the PoCs gave the UIDAI the confidence to go ahead with the use of iris technology.

4 On-field Validation

4.1 The Problem

The idea of using biometrics to ensure the unique identification and authentication of all the residents of India was an untested one. There were many assumptions behind it, and the data required to test the validity of these assumptions was not available. For instance, could the fingerprints of rural residents and manual labourers be captured successfully, or would they be excluded? What about the iris images of old or blind people? Could these biometrics be captured with sufficient detail that they could be used for deduplication and authentication? What would be realistic estimates of FPIR, FNIR, FRR, and FAR? What would be the most efficient and effective way to organise the process of enrolment? These questions needed to be answered rigorously if the project was to be successful.

4.2 Proof-of-Concept studies

The UIDAI conducted several on-the-ground experiments, called Proofs of Concept (PoCs). These experiments served two purposes: it enabled the Authority to explore the solution space and learn what might work and what might not; and it allowed the Authority to test its assumptions. This approach enabled the UIDAI to mitigate its risk by constantly seeking knowledge and validation from the field.

The UIDAI adopted a systematic approach to these PoCs. It designed them to answer well-defined questions, conducted them under realistic conditions, and analysed them rigorously.

4.3 Enrolment

The first set of PoCs was conducted in early 2010 in a few blocks in Andhra Pradesh, Karnataka, and Bihar. The areas selected were mostly though not entirely rural, so that the enrolees would be broadly representative of the overall population. In order to test the efficiency of deduplication, the same set of people were enrolled again after three weeks. A number of biometric capture devices of different makes were used. A number of different enrolment processes were also tried out.

The result of the PoC indicated that the major hypotheses of the UIDAI were correct. It was possible to capture sufficiently good biometric data that was fit for the purpose of deduplication and verification. Iris capture did not present any major challenges. An efficient enrolment process was developed.

4.4 Fingerprint Accuracy

The UIDAI conducted a set of PoC studies to determine the accuracy of fingerprints in authentication in India (UIDAI 2012). The objective of the study was to determine the accuracy of using fingerprints for authentication, the quality of the devices available to capture fingerprints and their interoperability, and whether accuracy could be improved by using multiple fingers, trying with the same finger again, or by identifying and using a 'best finger'. The study also attempted to determine how long authentication would take under different loads on the system.

This set of PoCs were conducted in phases across the states of Karnataka, Delhi, Himachal Pradesh, Maharashtra, and Jharkhand. Over 50,000 Aadhaar holders were covered in these PoCs.

It was found that fingerprints alone could provide an authentication accuracy ranging from 93.5% (using a single 'best' finger) to about 99% (using two fingerprints and 3 attempts), at an FAR of just 0.01%. Also, it was shown that the UID authentication system was capable of handling large volumes of authentication requests.

4.5 Feasibility of Using the Iris biometric

Similar to the PoC examining the accuracy of fingerprints for authentication, this PoC was designed to answer questions such as: can Aadhaar holders conveniently and efficiently use iris images for authentication; how accurate such authentication would be; what was the state of readiness of devices for iris capture; and whether the authentication system was ready for the large-scale use of iris images.

This PoC was performed in Karnataka. About 18000 online authentication transactions were performed by 5700 residents. An offline technology study was also conducted, in which 5833 residents went through capture sessions on eight different models of authentication cameras.

The study revealed that the vast majority of the residents were able to conveniently attempt iris authentication — the failure to capture (FTC) was just 0.33%. Further, the FRR was less than 0.5% at a FAR as low as 0.0001%. This indicated that very high authentication accuracy was possible with the use of iris images. In addition, it was found that several high-quality iris capture devices were available. This indicated that a competitive ecosystem of iris capture devices was present, easing concerns of vendor lock-in.

5 Promoting Competition

5.1 The Problem

Given the scale and importance of the project, it was important to increase efficiency and reduce cost using the private sector. At the same time, it was also essential to avoid a situation where any one private player could exercise significant power over the effective functioning of the Aadhaar system. The Authority wanted to ensure that there was a competitive market for providing services to it.

5.2 UIDAI's Competition Strategy

To promote such a competitive market, the Authority used a two-pronged strategy:

1. Open Standards: The Authority decided to rely on existing standards wherever possible. For instance, ISO standards were used for fingerprints. This reduced the risk of vendor capture: all vendors who conformed to the standard could participate.

   There were some areas where standards did not exist. For instance, there was no pre-existing standard for interfacing with biometric capture devices. In such cases, the Authority created standards and asked vendors to comply with them.

2. Open APIs (Application Programming Interfaces): The UIDAI created APIs and mandated that all its vendors had to communicate through those APIs. This allowed multiple vendors to plug into the UIDAI's systems. This also allowed the Authority the freedom to replace vendors if necessary.

As illustrations of this strategy, we consider three instances below.

5.3 Procuring vendors for deduplication

Deduplication algorithms had never been tested and scaled up to the numbers required in this project. The speed of algorithms normally depends on the size of the input (in this case the size of the gallery), and the execution time can become very large as the gallery size increases. It was not known how the algorithms for deduplication will behave at large input sizes.

To reduce the risk in the area of biometric deduplication, UIDAI came up with a very novel solution. It decided to engage three biometric service providers (BSPs), instead of just one. This turned out to be a very important decision.

There were three reasons to go with multiple vendors:

1. Avoid vendor lock-in: Most large scale international projects that used biometrics suffered from vendor capture. Globally, there were a few major companies who dominated the market for biometrics. They used proprietary algorithms that work with their own scanners, and the data may also be stored in a proprietary format. This has an advantage: the combination of proprietary capture devices, algorithms, and formats, often gives a higher accuracy rate than a system based on open standards. But this also has a major disadvantage: it is practically impossible to replace the vendor. The imperative of maintaining compatibility with previously captured biometrics would ensure that the vendor always stays in a position of power. The vendor would be able to dictate the price and the quality of the service. The Authority would lose its freedom of action.

2. Scalability: There was no way to establish the scalability of a particular vendor solution *a priori*. If the project had selected a single vendor, there was the risk that the vendor's deduplication solution could not scale up to the large number of deduplications required. The entire program would come to a halt, or the Authority would be hostage to demands for more and more hardware. But with three vendors, if a particular vendor failed to scale, it could be removed from the system, or replaced with someone else. In fact,

the Authority could even remove two vendors if required, as long as the third was able to scale.

3. Competition: With multiple vendors, the Authority was able to get them to compete constantly for each deduplication, even after the RFP was awarded. This resulted in better accuracy, greater speed, and lower hardware requirements. This is discussed in more detail in section 5.4.

The RFP stated that the UIDAI would provide the hardware to perform the deduplication. The winner would be the one whose total cost of operation — the sum of the costs of the hardware and the software — would be the least. The second and the third-best bidders would be offered a chance to be selected if they accepted the deduplication price quoted by the winner. If they refused, the offer would pass to the next best bidders, till three bidders were selected. This arrangement helped ensure that the Authority got the best price at the RFP.

5.4 Allocating deduplication requests among vendors

Even after three vendors were selected for deduplication, the Authority was able to set up a competitive market among them, using an innovative system to distribute deduplication requests among them. The broad features of this system were:

1. All the BSPs would start with the same gallery.

2. The enrolment packets for the new enrolees were distributed among the BSPs in a certain ratio (explained below) and each was asked to deduplicate the packets sent to them. The BSPs were to report the results of the deduplication to the UIDAI.

3. The ratio of distribution of new enrolment packets among the three vendors was determined through a formula having accuracy, speed, and hardware requirements as its parameters. BSPs could secure more enrolment packets by achieving higher accuracy, greater speed, and lower hardware requirements, relative to the other BSPs.

4. The BSPs were paid on the basis of the number of deduplication operations they were able to carry out, so they had a strong incentive to achieve high throughput at high accuracy and low hardware usage.

5. There was a threshold value of accuracy which, if breached, resulted in the suspension of the BSP. The concerned BSP would then have to improve the accuracy of its algorithm and demonstrate it to the UIDAI before it could receive any more enrolment packets.

6. If a BSP was not able to perform with the required speed, it could be suspended and asked to modify the algorithm to improve the speed.
7. A small fraction of the packets distributed to the BSPs were probe packets. The BSPs were not told which packets these were. They were distributed to all the BSPs, and after the BSPs performed deduplication, their results were checked. This helped to determine the accuracy of the BSP's algorithm.
8. If any of the BSPs reported a duplicate, the case was given to the other two BSPs as well without telling them. This also helped UIDAI to test the accuracy of the algorithms of the BSPs.

This led to a situation where the BSPs were constantly competing with each other to improve their speed and accuracy.

5.5 Creating Standards for Devices

Every biometric device had its own interface, distinct from the interfaces of other biometric devices. There was no standard 'device driver' for biometric devices. So each capture application had to integrate with all the devices it wanted to support. If a capture application wanted to support 10 commonly used devices, then the application developer would have to write 10 different interfaces, one for each device. This would make it very costly to bring new devices into the project, even if these new devices were cheaper and better.

In order to avoid this situation, the UIDAI created an intermediate specification (UIDAI 2010c). It also set up a certification process in collaboration with Standardisation, Testing and Quality Certification (STQC), a standards body backed by the central government. Vendors could implement support for this specification, and their devices could be certified. This would allow all capture applications to work with all certified devices.

This helped to ensure that many devices were available for the program, driving down the prices for all the components of the enrolment kit. The price of a standard 4 fingerprint capture device came down from about USD 2,000 to under USD 500.

6 Lessons

The success of the UIDAI in performing the difficult task assigned to it offers us much food for thought. Perhaps the first lesson we can draw from it is that innovation is indeed possible within the government. It is possible to achieve both scale and speed, even for a body acting within the constraints of government systems.

Government processes need not prevent it from taking bold decisions. In fact, practices commonly used within the government, such as the use of expert committees, and the emphasis on consensus-based decision making, can provide methods to examine difficult issues in a credible manner. For instance, consider the question of whether to use iris images. There was some disagreement within the government about this issue: there were reasonable concerns about the necessity of collecting iris images, the maturity of the technology, and vendor lock-in. The Committee mechanism was helpful in examining these issues in a transparent manner.

The example of UIDAI also helps us rethink the functions that should be housed within the government and the functions that could be performed outside it. The UIDAI could have created a bureaucratic behemoth with permanent employees all across the country, registering people and capturing their biometrics; instead, it created a very lean organisation and outsourced many functions to private agencies.

It was able to do this outsourcing only because of the high quality of its procurement processes. The UIDAI contracted out many large functions, and the bidding, selection and project execution for these happened largely without controversy. If such high-quality procurement skills were available to other departments, it is possible that many other functions that are currently performed by the government could be done better outside it. This procurement skill itself need not reside within the government — in the case of UIDAI, it took the help of consulting agencies to manage its procurements.

However, procurement is only part of the task. In order to outsource complex tasks to private companies, the government also needs to be good at contract management. To achieve this, the foremost requirement is that the government should be clear on the objective. Next, it should write RFPs with a level of detail commensurate with the complexity of the project. It should also establish well-designed processes for the governance and management of the projects, and oversee the execution continuously.

UIDAI also shows us that scale and complexity need not be a disadvantage, and that sometimes they can be used to the benefit of the project. Many projects run by the central or state governments in India are very large. This scale makes them attractive to private firms. They may be willing to provide their services to these projects at a low cost either because they can amortise their fixed costs over a very large base, or because they feel that they can leverage their participation in that project to get projects in other parts of India or other parts of the world. For instance, when the UIDAI established device standards and asked manufacturers to write conforming implementations, or when the UIDAI imposed difficult bid conditions, there was still no shortage of private participants.

Another lesson government agencies could learn from the UIDAI is its willingness to conduct empirical trials to gather more knowledge. Once a large-scale program is in place, bureaucratic inertia can make changes difficult, and the effects of incorrect assumptions and poor program design can become impossible to rectify. Instead, such schemes could be preceded by a few small pilots, designed to answer questions such as: Does this program work? Under what circumstances? How can we change processes or programs to maximise the chances of success? If the learnings from the evaluation of these pilots could be used to modify the design of the program before it is scaled up, the chances of success are likely to increase.

7 Conclusion

We have pointed out in this article that the UIDAI could achieve its objective successfully because it adopted a very different approach from most government organisations. It took tough decisions, such as the one to use iris images; it constantly experimented on the ground and learned from these trials; and it exploited private-sector competitiveness to achieve its task at low cost. It should be noted that this is not an exhaustive list of its innovations, but without these three decisions, it is unlikely the UIDAI would have been able to fulfil its mission.

This offers us many valuable lessons, the foremost being that even large government projects can be done fast and efficiently. Government processes need not be obstructive. In fact, the mechanisms of bureaucracy, such as committees, adherence to financial regulations, and desire for consensus, can help to resolve difficult issues and take tough decisions. Well-designed pilots and field-tests can help the government evaluate the effectiveness of large programs, so that it can deploy public resources more usefully. High quality procurement and contract-management processes can enable the government to leverage the dynamism of the private sector to provide public goods effectively.

* * * * * * *

References

BBC (2007). "Eye scans 'mean airport delays'". In: *BBC News* (Jan. 10, 2007). URL: http://news.bbc.co.uk/2/hi/uk_news/politics/6249205.stm.

– (2012). "Eye scanners at England airports turned off". In: *BBC News* (Feb. 16, 2012). URL: http://www.bbc.com/news/uk-england-17058448.

Daugman, J.G. (1994). *Biometric personal identification system based on iris analysis.* US Patent 5,291,560. URL: https://www.google.com/patents/US5291560.

Grother, Patrick et al. (2009). *Performance of iris recognition algorithms on standard images.* National Institute of Standards and Technology. URL: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=903606 (visited on May 19, 2016).

Mathews, Hans Verghese (2016). "Flaws in the UIDAI Process". In: *Economic and Political Weekly* 51.9 (Feb. 27, 2016).

Ramakumar, R. (2010). "The Unique ID Project in India: A Skeptical Note". In: *Proceedings of the Third International Conference on Ethics and Policy of Biometrics and International Data Sharing.* Hong Kong: Springer-Verlag, pp. 154–168. URL: http://dx.doi.org/10.1007/978-3-642-12595-9_20.

Standing Committee on Finance (2009). *The National Identification Authority of India Bill, 2010.* Fifteenth Lok Sabha. URL: http://164.100.47.134/lsscommittee/Finance/42%20Report.pdf (visited on May 3, 2016).

UIDAI (2009). *Biometrics Design Standards For UID Applications.* Unique Identification Authority of India. URL: https://uidai.gov.in/UID_PDF/Committees/Biometrics_Standards_Committee_report.pdf (visited on May 3, 2016).

– (2010a). *Ensuring Uniqueness: Collecting iris biometrics for the Unique ID Mission.* Unique Identification Authority of India. URL: https://uidai.gov.in/UID_PDF/Working_Papers/UID_and_iris_paper_final.pdf (visited on May 3, 2016).

– (2010b). *UID Enrolment Proof-of-Concept Report.* Unique Identification Authority of India. URL: https://uidai.gov.in/images/FrontPageUpdates/uid_enrolment_poc_report.pdf (visited on May 3, 2016).

– (2010c). *UIDAI Biometric Capture API Draft.* Unique Identification Authority of India. URL: https://uidai.gov.in/UID_PDF/Working_Papers/UID_Biometrics_Capture_API_draft.pdf (visited on May 11, 2016).

– (2012). *Role of Biometric Technology in Aadhaar Authentication: Authentication Accuracy Report.* Unique Identification Authority of India. URL: http://uidai.gov.in/images/role_of_biometric_technology_in_aadhaar_authentication_020412.pdf (visited on May 3, 2016).

– (2016). *Current Highlights: Total Authentication Transactions.* July 2016. URL: https://authportal.uidai.gov.in/ (visited on Aug. 24, 2016).