

Performance Lessons from India's Universal Identification Program

Alan Gelb and Julia Clark

Abstract

Biometric identification is spreading rapidly across the developing world, where it is helping to close the “identification gap” that separates poor countries from rich ones.

India's Unique Identification (UID) project offers important lessons for other countries. UID's performance data show that large countries can implement biometric ID programs with low levels of exclusion and high accuracy, but this requires the combined use of multiple biometrics.

Data on authentication provides strong indications that iris technology is both more inclusive and more precise than fingerprints. However, even well-designed systems will

need to allow for failures to enroll and for errors by providing other options to identify and authenticate individuals.

UID's modest cost levels owe much to its standards-based approach, which encourages competition among suppliers and avoids lock-in to proprietary technology. UID also sets standards for the disclosure of performance data which other programs should emulate, and which can be used to help calibrate technology to needs.

These lessons are also useful for the foreign donors that support many identification systems in poor countries and are concerned that they be both inclusive and effective.

Alan Gelb and Julia Clark. 2013. “Performance Lessons from India's Universal Identification Program.” CGD Policy Paper 020. Washington DC: Center for Global Development. <http://www.cgdev.org/publication/performance-lessons>

CGD is grateful for contributions from the UK Department for International Development in support of this work.

Center for Global Development
1800 Massachusetts Ave NW
Third Floor
Washington DC 20036
202-416-4000
www.cgdev.org

This work is made available under
the terms of the Creative Commons
Attribution-NonCommercial 3.0
license.



CGD Policy Paper 020
May 2013

Contents

Introduction	1
Features	2
Performance Measures	3
Enrollment	4
Authentication	5
Lessons for Other Countries	8
Accurate, Inclusive, Biometric ID Systems are Feasible for Large Countries	8
The Eyes Have It	8
Two is Better than One (or Twelve is Better than Ten)	9
Anticipate Problems and Biometric Failure	9
Competition Contains Cost	9
Disclose Performance Data	9
Annex Tables	11
References.....	12

We thank Salil Prabhakar for helpful comments. All errors are the responsibility of the authors.

JEL Codes: H80, J10, O33, O38, Z18

Introduction

Developing countries are adopting biometric identification technology at an impressive rate. Gelb and Clark (2013) note 160 programs in 70 countries that together cover over 1 billion people and include a wide range of applications—financial access, public payroll management, social transfers, health insurance and tracking and voter rolls—as well as national identification systems. Rich countries have robust systems of identification for their citizens, based on strong basic official documentation such as birth certificates. In contrast, many citizens of poor countries lack reliable official identification, and are therefore excluded from many of the points of engagement between a modern state and its citizens.¹ They cannot open bank accounts or register property, and there is no easy way to confirm that they have received the public transfers or services to which they are entitled. New technology is seen by some as an opportunity to rapidly close the “identification gap,” as well as to improve the performance of individual development programs.

The spread of biometric technology is not without controversy. Some concerns relate to the potential for increased surveillance and erosion of privacy, others to the possibility that technology will support policies that further exclude the poor and vulnerable rather than widening inclusion. A further concern has been on the performance of the technology itself, in real-world large-scale applications in developing countries. Will it exclude many individuals who are not able to provide suitable biometrics? Will there be many errors and cases of mistaken identity? How successful is the technology in preventing one individual from having multiple identities? ²

These questions are not unreasonable. In particular, distressingly little data is available on performance, either for identification or for authentication, or in terms of the proportion of poor populations unable to furnish sufficiently high-quality biometrics. Although there has been extensive laboratory testing of different hardware and software for a variety of biometrics, including fingerprints, iris, face and voice,³ testing under carefully controlled conditions does not provide adequate information on real-world performance, which can be affected by many factors (Wayman et al 2010). Lighting cannot always be adequately controlled, sensors may not always be in perfect condition and operators may not be adequately trained. Populations with a high incidence of heavy manual labor may include many individuals who are unable to provide fingerprints. In addition, most applications have involved proprietary systems, and the vendors have not been forthcoming with public operational performance data. Part of the reason is that a large proportion of biometrics

1 Breckenridge and Szreter (2012) provide a panoramic overview of the development of identification systems in a wide range of states as well as the interests that motivated their creation. According to UNICEF

2 For a useful summary of concerns about the deployment of biometric systems see <https://www.eff.org/wp/biometrics-whos-watching-you>. Ramakumar (2010) offers a skeptical view of India’s UID project that reflects similar concerns.

3 See for example Jain (2011), Watson et al (2005), Phillips et al (2007).

applications—probably the large majority in global terms—are in law and order and security-related areas.

India has recently launched the ambitious Unique Identification (UID) program—which aims to provide every resident of India with a unique, secure identification or *Aadhaar*⁴ number. This massive effort, which has already enrolled some 240 million people, is being closely watched by many countries. UID is still at a relatively early stage, and links to the delivery of public programs are only now getting under way. Nevertheless, simply in terms of numbers enrolled and identified to date and low unit cost, the UID program is impressive. It is also a marker in terms of the fundamental basing of the system on biometrics. The Unique Identification Authority of India (UIDAI) which manages the program has recently published a series of papers documenting performance of their biometric identification system (UIDAI a, b, c). These appear to be the first public release of large-scale operational performance in a developing country. They should be of great interest to all countries in the process of planning to strengthen their identity systems by introducing or upgrading biometric technology, and also to donors contemplating support to such programs in developing countries. They do not of course address all performance issues -- it remains to be seen how robust the system is against active efforts to spoof it by providing faked fingerprints or iris images, to capture biometric data in transmission or to penetrate the database. But the data do suggest potential standards for other programs.

Features

UID has some distinctive features. Both fingerprint and iris data are collected to increase the quantity of biometric information and also to help include people who might not be able to provide either good prints or good iris scans. Software is open-source (Linux); hardware is off-the-shelf and competitively procured. The system is built to be scaled in response to need. Standard interfaces tie the components together. Where no standards previously existed, as for iris scanners, UIDAI created them to encourage competition among suppliers. Rolling out the project in a decentralized way involved the empanelment of a wide variety of entities to enroll individuals; some 50,000 centers are now operating.

Learning from previous experiences, including failed programs in India itself (Zelazny 2012), UIDAI places a heavy emphasis on data quality throughout the process. It collects as much operational data as possible, including on the details of each individual enrolment as it is carried out, process by process. This is included, together with biometric and demographic data, in the packet of information sent from the enrollment point to the data center. Inadequate hardware that requires multiple attempts to capture fingerprints—or poorly performing operators—can therefore be spotted quickly as enrollment proceeds. So can operator short-cuts, such as reporting unusually high percentages of enrollees unable to provide biometric data. UID has used real-time feedback from its monitoring system to

⁴ See Zelazny (2012) for a detailed description of the evolution of the UID program.

identify and correct such efforts to subvert the registration process. The project uses proprietary technology in only one instance: three vendors compete in the complex area of de-duplication, and each also serves as a check on the accuracy of the others. As expected, UID is also impelling further development, standardization and competition within the biometrics industry.

This open structure was shaped by the size of the task at hand. The UID project needs to be able to cover a huge population of 1.2 billion people, with sufficient quality to provide reliable and unique identification at an affordable price. At under US\$3 per head, the unit cost of each unique Aadhaar number is the lowest recorded for any identity system worldwide. UIDAI keeps costs low by relying on remote cell-phone authentication against the central data base—rather than issuing a costly card to enable off-line authentication—and by requiring minimal information from enrollees. Further certification, proof of nationality for example, must be done in a separate exercise. Having a unique Aadhaar number issued by UIDAI itself entitles the holder to no specific privileges or programs.

Performance Measures

How inclusive and accurate is UID technology? How many people are unable to enroll biometrically into the system and need to be identified by other (demographic) means? How effectively can the technology screen against mistakes when determining unique identity? How many people, once enrolled, are not able to authenticate themselves against their stored record? How does iris data stack up against fingerprints? Based on initial experiences and testing, UIDAI has provided some answers to these questions for a large sample of India's population.

Performance can be summarized in three statistics. Failure to Capture (FTC) is the percentage of the population that is unable to provide sufficiently high quality biometrics to be enrolled in the system without alternative mechanisms.⁵ Two other probabilities are important. The first is the probability that the system erroneously accepts a mistaken or false identity claim submitted by an individual, the False Acceptance Rate (FAR). The second is the probability that the system erroneously rejects a correct identity claim, the False Rejection Rate (FRR). The concept of FTE is common to both the enrollment and authentication phase, but FAR and FRR have different interpretations when applied to the enrollment phase to ensure uniqueness (de-duplication) and the later verification or authentication phase, leading to sometimes confusing terminology.

In enrollment, applications are de-duplicated to make sure that a physical person cannot obtain more than one identity. A false acceptance of a second, or third, claim of identity means that the system has responded negatively to the question of whether the individual's biometrics are already enrolled in the system. For this reason, the false acceptance rate or

⁵ Failure to Capture (FTC) should be distinguished from Failure to Enroll (FTE) because those unable to provide biometric data can still be registered using demographic information.

FAR is often referred to, more precisely, as the False Negative Identification Rate (FNIR). The other possibility, that an individual not in the system is positively identified as already in the system and thus falsely rejected from registering (FRR), is more precisely termed the False Positive Identification Rate (FPIR).

In authentication mode (or verification of a claimed identity in order to access a service), the FAR measures the probability that the system will mistakenly accept an individual's erroneous assertion that she is who she claims to be, while the FRR measures the probability that her legitimate identity claim is rejected.

For simplicity, we will use the terms FAR and FRR to represent the respective errors both in enrollment and authentication, but recognizing that they have different meanings in each. There is of course a basic underlying parallelism. A high FAR will signal vulnerability to fraud, both in enrollment (individuals can acquire multiple identities) and in authentication (fraudulent identity claims). A high FRR signifies erroneous exclusion, both from deserved enrollment or from legitimate authentication.

In each of the enrollment and authentication stages there is a tradeoff between the FAR and the FRR, since the balance between them is determined by the parameters of a matching function. This is expressed as the Detection Error Tradeoff (DET) curve. A more precise system will have a DET curve closer to the origin than one that is less precise. The more accurate a system, the lower the FAR for any given FRR and vice versa. Choosing the optimal point on a given DET curve depends on the application. For entry into a secure nuclear facility, one would want a very small FAR to detect all unauthorized entrants. For access to a health insurance program for poor households, it may be more important to ensure that people are not mistakenly excluded by having a small FRR, even if a higher FAR means accepting a few more ineligible people into the program.

Enrollment

UIDAI issued performance data after the enrollment of the first 84 million people. Because both fingerprints and iris are taken, FTC errors were small, at 0.14 percent, or 14 in 10,000; most people have at least one of these biometrics. Even with this small percentage, countries aiming for Indian standards will still need to allow for some “demographic” enrollees, those whose identities must be established and authenticated by non-biometric means. For a country with a population of 30 million—the average of Ghana and Uganda, or “Ughana”—an FTC rate of 0.14 percent would yield some 42,000 demographic enrollees. To be inclusive, the enrollment process would need to accommodate these individuals.

How many people might acquire multiple identities by enrolling twice (a false negative)? UIDAI deliberately introduced faked enrollments to see how well they were caught by the system. The small resulting FAR of 0.035 percent suggests that few people will find it worthwhile to attempt to enroll twice—and even fewer will succeed. As an illustration, suppose that as many as 1 percent of people in a country the size of Ughana tried to enroll

twice, even with these low odds of success. At the Indian FAR rate, there would then be only about 100 cases of double identity in a population of 30 million. This is many fewer than with traditional identity systems (e.g., the US Social Security Number)⁶, and certainly tolerable when using the identification system to distribute entitlements or help manage public programs.

How many people would be denied enrolment because of a wrong determination that they had already enrolled? The False Rejection Rate (FRR) of the identity system is critical, especially with a large population. Since every new enrollment has to be checked against every existing enrollment, the number of comparisons increases with the square of the population. With up to 1 million new enrolments every day needing to be checked against those already enrolled, the UIDAI data center must currently run some 100 trillion person-person comparisons every 24 hours to keep up. Even a very tiny probability of a false rejection (a false positive) will lead to millions and millions of spurious alerts that will quickly overwhelm any manual system set up to address them.

Against an existing enrolment gallery of 84 million at the time, UIDAI reported a FRR of 0.057 percent. For any individual 1:1 comparison, this implies a very small probability of a false rejection of about 6.8×10^{-12} , or 7 in one trillion. Extrapolating this to our hypothetical Ughana population yields approximately 3,000 false rejections—individuals that would appear to be duplicates but are not. This represents a small and manageable number of cases that would need to be followed up by manual review.⁷

Authentication

How well can biometrics be used by the public to establish individuals' claims to their identity, open bank accounts, collect benefits, register property or other transactions as needed? Starting in early 2012, UIDAI conducted a series of large-scale studies on the use of fingerprints, and later iris, for authentication. These studies were testing different hardware devices at the same time and also alternative authentication criteria because the use of multiple biometrics offers a range of choices. Should the test be on one fingerprint or two? Can the “best” two fingers be captured and labeled to reduce the level of error without introducing further memory failures or operator error? Should a single or dual-capture iris camera be used? How many attempts to capture data are allowed for any one individual? Which matching algorithm should be used? The tests therefore produced a range of results which vary considerably. From these, it is possible to derive a “bottom line” guide to

⁶ According to a study by I.D. Analytics, some 6.1 percent of Americans (nearly 20 million people!) have at least two social security numbers. The majority reflect data entry problems rather than fraud. <http://www.idanalytics.com/news-and-events/news-releases/2010/8-11-2010.php>

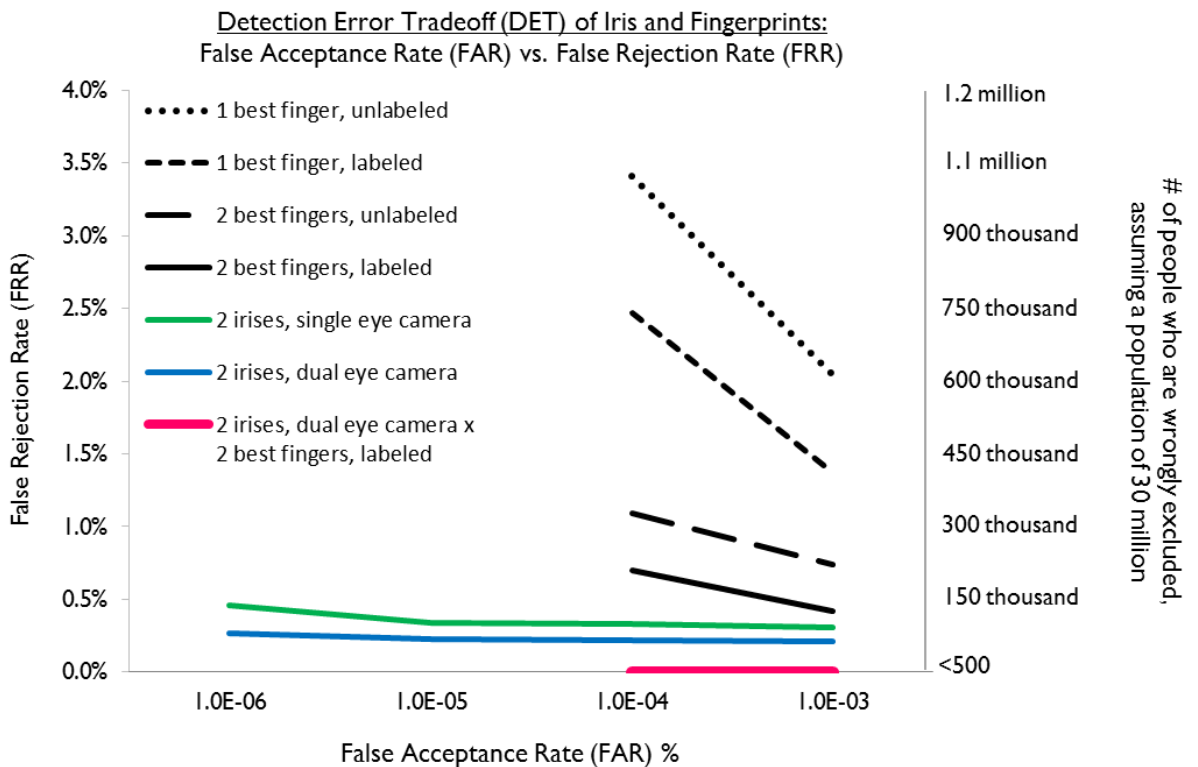
⁷ For a huge population like India's, even this small level of error would result in some 3.1 million false rejections if continued through the program. UIDAI plans to contain the numbers by eliminating some sources of error unearthed by the initial study, and also by relaxing the FAR if needed to further reduce the FRR. Handling false rejections has reportedly been a manageable problem to date.

performance. These use two labeled “best” fingers or two irises on a dual-capture camera, and allow a reasonably small number of repeated attempts in an effort to authenticate. The UID results are summarized in Annex Tables 1 and 2.

The first conclusion is that iris authentication is more inclusive than authentication via fingerprints. Its FTC rates were much lower; only 0.33 percent of the sample was not able to provide sufficiently good quality iris readings, compared with about 1.7 percent for fingerprints, even taking the most favorable 2-finger option. Age and heavy manual labor were the main reasons behind fingerprint exclusion. For irises, many cases of FTC resulted from an old type of cataract surgery no longer practiced. These cases were more frequent for older individuals.

The other category of those excluded is people able to provide good biometrics but falsely rejected in their attempt to authenticate themselves. As noted above, there is a tradeoff between the FRR and the FAR, and the latter needs to be kept sufficiently small to deter fraud. Figure 1 depicts the performance of the fingerprint and iris authentication systems along the DET curves as the FAR is varied from 0.1 to 0.001 percent, and also shows the number of affected people that would result in Ughana. Again, the iris authentication was superior. At a common FAR of 0.01 percent, the FRR for fingerprints was 0.71 percent and for iris only 0.22 percent.

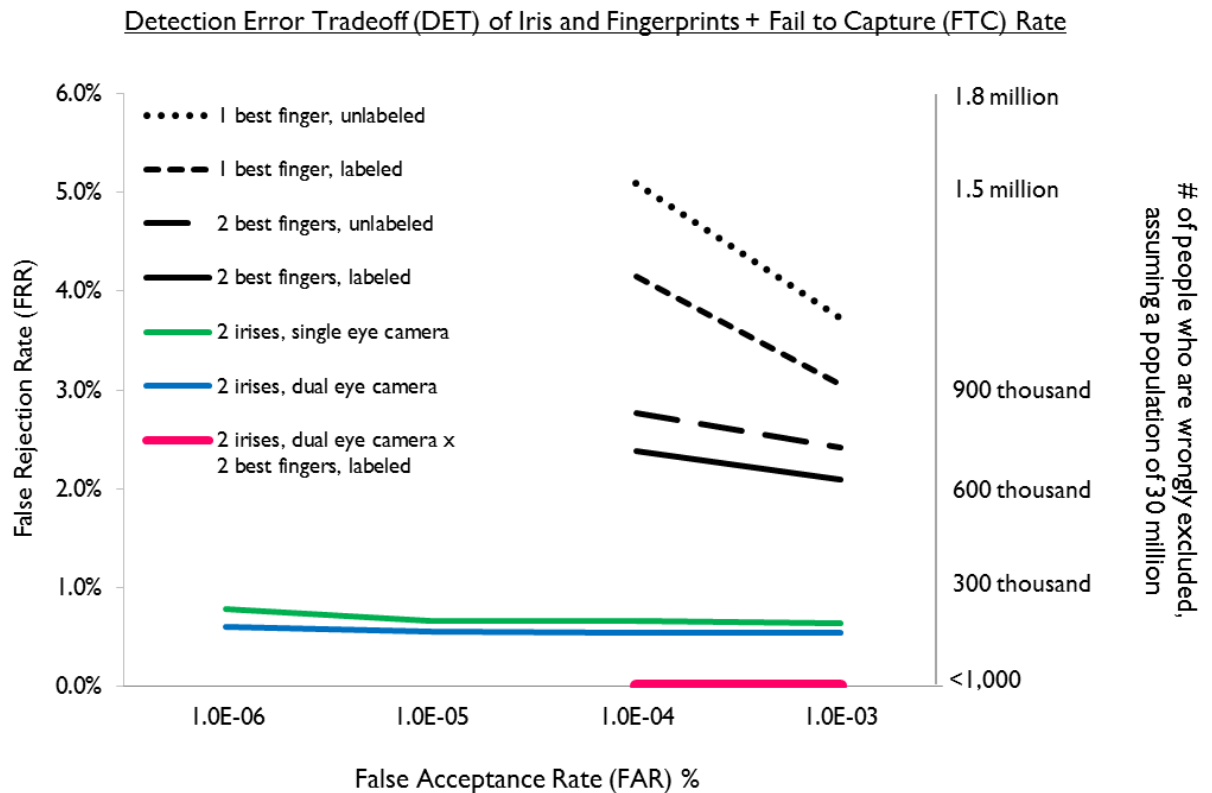
Figure 1



Iris also showed the advantage that its DET curve is relatively flat, meaning that very small FARs can be accommodated without unduly raising the FRR. This makes it especially useful for high-security operations.⁸

Figure 2 puts the FTC and FRR effects together, to show those unable to authenticate themselves for either reason. At a FAR of 0.01 percent, about 2 percent of the population is unable to authenticate themselves by fingerprints, compared with to less than 0.6 percent for iris. Some of these could of course possibly succeed in later, repeated attempts.

Figure 2



Combining the two biometrics to allow a wider range of options would greatly reduce the number of exclusions. If failures were independently distributed, only about 133 people in 1 million would be affected by exclusion—some 4,000 people in our hypothetical Ughana. In practice, the number would be somewhat higher, since older people have a higher

⁸ UID accuracy appears to be at least comparable with levels cited in Jain 2011, Wilson et al. 2005 and Phillips et al 2007, suggesting that the program has managed to maintain quality under operational conditions. Iris shows the additional advantage of a low FTC rate, reducing the percentage of those excluded.

probability of failing both the fingerprint and iris authentication tests. These individuals would need to use other methods, such as visual photo identification, PINs or passwords.⁹

Lessons for Other Countries

UID is still at an early stage. Only one fifth of the population has been enrolled and the linkage to public programs is just beginning. There are still tensions with other branches of the government, some of which have, or believe that they have, a mandate to issue identification.¹⁰ As noted above, the data do not cover all risks, some of which may only emerge after the system becomes more widely used.

Another caveat is that the data reported by UID reflect the state of biometric identifiers among India's population. Exclusion and error rates for fingerprints tend to be higher for low-income populations involved in heavy farming and other manual work. The incidence of old-style cataract operations (which affect iris identification) is also probably higher in India than in many countries. Even though the average population in richer countries is older than that of India, UID's performance can perhaps be considered as a lower bound for such countries.

Recognizing these factors, UID offers some important lessons:

Accurate, Inclusive, Biometric ID Systems are Feasible for Large Countries

Only China, India and the US have larger populations than the number of people already enrolled in UID. With over 240 million enrolled (and climbing), UID would be the fourth largest country in the world, and it will soon overtake the US in terms of numbers. UID's performance suggests that accurate, biometric-based, identification is quite feasible for large countries, including the US.

The Eyes Have It

Iris trumps fingerprints. UID's data suggest that iris scans are far more inclusive than fingerprints, especially when applied to poor populations engaged in heavy manual labor. They are also more precise for authentication, in terms of having a lower tradeoff curve between errors of acceptance and rejection, even in the best case when the best two fingerprints are known and individually labeled. The rapidly falling price of iris technology

⁹ If iris and fingerprint FTCs were independently distributed and people could use one or the other, the FTC for authentication would be $0.0033 \times 0.017 = 0.0056$ percent or 56 in one million. This is less than the reported FTC for the enrollment phase (0.0014) suggesting that failures are somewhat correlated. For exclusion, combining FTC and FRR for each method and assuming independence yields $(.0033+0.0022)*(0.017+0.0071) = 0.0135$ percent.

¹⁰ Parallel to the UID project, the Ministry of the Interior's National Population Registry—which has the constitutional mandate to identify citizens—is also conducting a biometric census.

makes it a viable option, especially if it reduces the incidence of errors needing costly follow-up.

Two is Better than One (or Twelve is Better than Ten)

Except perhaps for very small countries or programs, UID's experience argues strongly for the combined use of multiple biometrics, including iris scans as well as fingerprints. UID shows that countries with large populations can implement inclusive, precise, high-quality identity systems by using existing technology, but not without multiple biometrics. Few people have neither a usable iris nor fingerprints, though the incidence of problems is somewhat higher among the aged.

Anticipate Problems and Biometric Failure

Even a program designed as carefully as UID will see cases of exclusion and accept/reject errors. They may be small in number, but if the identification system is to be inclusive it will have to provide alternatives. Public information is not available on the errors in many ongoing biometric identification programs and in many cases one suspects that those operating or financing the program have only a hazy idea of what the errors might be. UID suggests, however, that exclusion and error rates are not negligible in programs using simple technology and, in particular, that they will be rather high for programs enrolling and authenticating individuals with one, or a few, fingerprints.

Competition Contains Cost

The UID program has been rolled out in a particular way: it is heavily standards-based and emphasizes careful, real-time, quality monitoring and competition between suppliers, rather than being locked-in to particular hardware and technology. This "plug and play" approach increases choice and reduces costs. It also facilitates open, competitive, standards-based procurement—a rarity in the high-tech area where procurement is often problematic or corrupt. Not all countries have the strong technological capacity of India, which is central to its ability to manage a program in this way. However, they can build on India's experience, including through cooperative arrangements to increase scale economies. Could one imagine, for example, an Africa-wide facility housed by the African Union or NEPAD (its development program) that offered a high-quality, integrated identification program to any country? Key donors, such as the European Union, United Nations and the World Bank, which already fund many identity management systems, could support such a facility. There is now no excuse for old-fashioned cozy deals with favored suppliers.

Disclose Performance Data

Should identity programs disclose performance data? One reason for not doing so could be to maintain a fiction of infallibility. If people believe that it is impossible to cheat the system few will try to do so. But if they believe that the system can be fooled, many more might try. This raises the possibility of multiple equilibria. Suppose, for the hypothetical case of

Ughana, that the enrollment FAR was 1 percent rather than 0.035 percent, and that knowledge of this induced as many as 5 million people to attempt multiple enrolments. Instead of 100 duplicate identities there would be 50,000. A similar percentage increase in the FRR would result in almost 10 million false (positive) rejections, far more than could be resolved with any manual follow-up process. This would effectively destroy any pretense of uniqueness in the ID system.

Discretion might seem the more attractive policy in these conditions. If people think that the technology is infallible, fewer will probably try to cheat it – at least for a while. However, the breakdown of the identity management system would have serious consequences. In the first instance, those hurt by failures of a supposedly “infallible” system bear a strong burden of proof. They cannot expect to access a well-working grievance process for none will be provided. And in the longer run, as its mystique evaporates, the identity system will no longer be trusted by anyone, eliminating any value.

The UID project has shown the value of disclosing performance data. It provides information essential for assessing the project’s progress so far, and benchmarking the accuracy of cutting-edge biometric identification technology. But this transparency also enhances UIDAI’s credibility and sets a standard for other counties as well as for programs supported by donors. UID is remarkable not only for what it has already done and what it seeks to accomplish, but also for the way in which it operates. There is now no excuse for other countries not to share data—or for donors not to insist on it when financing identification programs.

Annex Tables

Table 1. Authentication: Detection Error Tradeoff (DET) of Iris and Fingerprints

False Rejection Rate (FRR)	False Acceptance Rate (FAR)			
	1.0E-06	1.0E-05	1.0E-04	1.0E-03
2 irises, dual camera	0.27%	0.23%	0.22%	0.21%
2 irises, single camera	0.46%	0.34%	0.33%	0.31%
2 fingers, labeled			0.70%	0.42%
2 fingers, unlabeled			1.09%	0.74%
1 finger, labeled			2.47%	1.37%
1 finger, unlabeled			3.41%	2.04%
2 irises, dual camera x 2 fingers, labeled			0.0015%	0.0009%

Table 2. Authentication: Detection Error Tradeoff (DET) of Iris and Fingerprints

False Rejection Rate (FRR)	False Acceptance Rate (FAR)				Iris	Finger	FTC
	1.0E-06	1.0E-05	1.0E-04	1.0E-03			
2 irises, dual camera	0.60%	0.56%	0.55%	0.54%			0.33%
2 irises, single camera	0.79%	0.67%	0.66%	0.64%			1.68%
2 fingers, labeled			2.38%	2.10%			
2 Fingers, unlabeled			2.77%	2.42%			
1 finger, labeled			4.15%	3.05%			
1 finger, unlabeled			5.09%	4.73%			
2 irises, dual camera x 2 fingers, labeled			0.0131%	0.0113%			

References

- Breckenridge K. and S. Szreter (eds). 2012. *Registration and Recognition: Documenting the Person in World History*. Oxford University Press/British Academy.
- Gelb, A. and Clark, J. 2013. "Identification for Development: The Biometrics Revolution." CGD Working Paper 315, Washington, DC: Center for Global Development.
<http://www.cgdev.org/content/publications/detail/1426862>
- Jain Anil K. 2011. "Biometric Authentication".
http://www.scholarpedia.org/article/Biometric_authentication.
- Phillips P., W. Scruggs, A. O'Toole, P. Flynn, K. Bowyer, C. Schott and M. Sharpe. 2007. "FVRT and ICE 2006 Large Scale Results". NISTIR 7408, National Institute of Standards and Technology, Gaithersburg MD.
- Ramakumar R. 2010. "The Huge UID Project in India: A Sceptical Note". In Kumar A. and Zhang D. (eds) *Ethics and Policy of Biometrics*. Springer.
- UIDAI, 2012a. "The Role of Biometric Technology in Aadhaar Enrollment".
- UIDAI. 2012b. "The Role of Biometric Technology in Aadhaar Authentication: Authentication Accuracy Report". March
- UIDAI. 2012c. "The Role of Biometric Technology in Aadhaar Authentication: IRIS Authentication Accuracy, POC Report". September.
- UNICEF. 2012. *The State of the World's Children*.
- Watson, C., C. Wilson, M. Indovina and B. Cochran 2005. "Two Finger matching with Vendor SDK Matchers". NISTIR 7249, National Institute of Standards and Technology, Gaithersburg MD.
- Wayman, James L., A.Possolo and A. J. Mansfield. 2010. "Fundamental issues in biometric performance testing: A modern statistical and philosophical framework for uncertainty assessment." Presentation to IBPC Conference, NIST, March.
- Zelazny, F. (2012) "The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries." CGD Policy Paper 008. Washington, DC: Center for Global Development.
http://www.cgdev.org/files/1426371_file_Zelazny_India_Case_Study_FINAL.pdf