A biometric is a measure of identity based on a physiological (fingerprint, face, eye iris or retina) or behavioral (speech or signature) characteristic. It is an effective personal identifier because it is unique to and embodied in each person, so it cannot be forgotten, lost or stolen like other conventional identification methods.

The recent advancements in recognition technology coupled with increases in digital storage capacity and computer processing speed have made biometric technology feasible in many applications, from controlling access to a building or restricted area, to large scale identification systems such as the one being implemented in India to allow more effective delivery of targeted government programs.

Biometric technology can also improve access to credit and insurance markets, especially in countries without a unique identification system, like Malawi. In these places, identity fraud—the use of someone else’s identity or a fictitious one—to gain access to services unavailable to the individual is rather common. Lenders tell anecdotes of past borrowers purposefully defaulting and trying to obtain a fresh loan from the same or another institution, and although less common in developing countries because markets are less developed, one could imagine sick individuals without coverage using the insurance policy of their healthier friends or relatives. The response of lenders and insurance companies has been to restrict the supply of such services.

In the case of credit, biometric technology can make the threat of future credit denial credible because it makes it easier for financial institutions to withhold new loans from past defaulters, and to reward responsible past borrowers with increased credit. As a result, individuals may take out smaller loans or avoid borrowing altogether; borrowers may have greater incentives to ensure that production is successful, either by exerting more effort or choosing less risky projects, and—whenever production could cover the loan repayment—may be less likely to default intentionally or opportunistically.

To look at the impact of biometric technology, Giné, Goldberg and Yang (2009) implemented a field experiment using smallholder paprika farmers that applied in 2007 for an agricultural input loan. Farmers in the study were randomly allocated to either a control group or a treatment group where each member had a fingerprint collected as part of the loan application\(^1\). Both treatment and control groups were given a training session on the importance of credit history in ensuring future access to credit.

\(^1\) The authors chose fingerprint recognition over face, iris or retina recognition because it is one of the cheapest, best known and most widely used technologies. Fingerprinting technology has been commercially available since the early 1970s and there are more than 75 companies ensuring a very competitive market.
The study shows that for the subgroup of farmers with the highest ex ante default risk, fingerprinting led to increases in the repayment rates of about 40 percent. By contrast, fingerprinting had no impact on repayment for farmers with low ex ante default risk. This higher repayment rates are due to fingerprinted borrowers requesting smaller loan sizes and devoting more land and other inputs to paprika.

A rough cost-benefit analysis of the pilot experiment suggests that the benefits from improved repayment greatly outweigh the costs of equipment and fingerprint collection.

**Challenges in the implementation of biometric systems**

Despite the encouraging results from the pilot in Malawi and the success of biometric technology in controlled laboratory environments, there are still a few concerns and challenges when collecting and using such information in actual environments and when trying to establish an identification system at a national level.

- **Not everyone can be enrolled in a fingerprint-based identification system.** Fingerprints can be unrecognizable due to cuts or burns or extreme weight gain or loss. In addition, older individuals may have poor fingerprints, or the operation of fingerprint readers may be jeopardized due to arthritis. In some areas recovering from years of conflict, individuals may lack fingers altogether. In other cases skin pigmentation obfuscates the possibility of getting readable prints. In the most comprehensive study to test the process and customer attitude during the recording of biometric information, the UK Passport Service Trial reports an enrolment success rate of 100 per cent for the 9,250 non-disabled participants and 96 per cent for the 750 disabled participants. Interestingly, the enrolment rate is much lower among the black population. In Malawi, only about 2 per cent of the sample of 1,600 fingerprinted farmers had the left thumbprint recorded, rather than the required right thumbprint.

- **The accuracy of biometric technology remains to a large extent untested.** Biometric companies report very high accuracy rates from highly controlled trials which typically use artificially generated data. However, because the performance of a technology depends greatly on the context, trials using real life data are far less impressive. For example, the UK Passport Service Trial reports that only 80 per cent of the cases could be correctly verified, younger individuals being more successful than older. In Malawi, everyone selected during demonstration sessions was correctly identified.

- **Individuals may have a negative attitude towards providing their biometrics.** People may be reluctant to place their fingers on the scanners due to hygiene concerns. More importantly, there is the widespread public perception that fingerprinting is linked to the criminal justice process. Related, in conflict affected countries stricken by ethnic infighting, individuals may refuse to provide biometrics for fear of persecution by authorities or others that gain illegal access to such biometric records. Finally, during the Parliamentary debates concerning the ID Cards Bill in the UK, 55 per cent of respondents of a poll thought that the collection of
biometric information was an infringement of civil liberties. In Malawi, the authors did not encounter any resistance from the farmers, perhaps because it was a very novel technology.

- **The cost of collecting biometrics can be high.** The estimates are sparse and detailed cost-benefits analyses have not been systematically conducted. However, the costs of using different types of biometric technology starting from basic fingerprinting techniques to voice and iris recognition software can be prohibitively expensive. In India there are legitimate concerns that the costs of rolling out biometric technology may mean a huge opportunity cost for the provision of social benefits for over 700 million Indians living in poverty. In the UK, a critical report by several researchers at LSE found that the government underestimated the implementation of the ID Cards Bill. The report suggests that the ten-year rollout would be between £10.6 billion and £19.2 billion, excluding public or private sector integration costs.

- **Biometric technology is not infallible.** While biometric technology can be a big step forward to combating issues of identity theft, fraud, and money-laundering efforts, it is essentially a technological application. As is the case with any other technology, it can be hacked, infiltrated, or runs the risk of having data fall into the wrong hands. Since biometric technology in only at present being piloted on a large scale in some pockets of the world, legitimate concerns on privacy do arise. For example, it is possible to imagine that workers on the ID database will be corrupted, threatened or blackmailed. After all, the perpetrators of 80 per cent of all computer security lapses are not hackers, but employees.

- **It is important that a common platform is used if biometrics data is merged with other datasets.** Biometric data is stored in formats that may not be compatible with the information systems of other government agencies so an effort must be made to have compatibility if it has to serve as the basis for a national identification system.

Despite these concerns, biometric technology presents an exciting and innovative opportunity for increased access to financial markets and better public service delivery. Whether it can be scaled up effectively and be used to resolving identification and authentication issues remains to be seen.


Xavier Giné (xgine@worldbank.org) is senior economist in the Research Development Group (DECRG) at the World Bank.