USAID
FROM THE AMERICAN PEOPLE

BIOMETRICS IN ELECTIONS

GEORGIA: DE-DUPLICATION OR VOTER REGISTER AND VERIFICATION OF VOTER IDENTITY USING BIOMETICS

FEBRUARY 2011

Biometrics in Elections

Georgia: De-duplication or voter register and verification of voter identity using biometrics

Ole Holtved
Civil/Voter Registration Expert

9 February 2011

This report is made possible by the support of the American people through the United States Agency for International Development (USAID). The contents are the sole responsibility of the International Foundation for Electoral Systems and do not necessarily reflect the views of USAID or the United States Government.

Table of Contents

Introduction

1. This report is a result of a brief consultancy on behalf of IFES Georgia with financial support courtesy of USAID. The views and opinions expressed herein are those of the author and should not be attributed to neither IFES nor USAID.

2. The consultancy took place over four days in the period 25 to 28 January 2011 in Tbilisi, Georgia. The author conducted meetings with several stakeholders key to the electoral process in Georgia, including representatives from political parties both in opposition and ruling, the Central Election Commission (CEC), the Civil Registration Authority (CRA), and the international community. The consultations culminated in a roundtable held at the Courtyard Marriott Tbilisi on 28 January 2011.

3. This report will cover lessons learned from registration projects around the globe. Every country is unique and there is no single best solution that applies everywhere. The specific context in which each country conducts a registration, including the history of identification and past elections, must be taken into consideration when planning any new registration activities. There is however commonalities between registration exercises across countries and continents from which valuable lessons can be drawn, both about what has gone wrong and what has gone right.

4. Without in any way claiming to understand all intricacies of the context in Georgia after only four days on the ground, this report will attempt to provide some guidance on what options might be worth exploring further and what risk various options may entail.

Biometrics in Elections

5. Biometrics has been used in civil and voter registration around the world for more than a decade. This chapter will look at the motivation for the use of biometrics, the technologies used, their pros and cons, the resource implications, and the lessons learned.

Motivation

6. Biometrics can basically be used for two main purposes:

   - De-duplication or registries, i.e. finding multiple occurrences of the same person in a register; and
   - Identification, e.g. in access control systems, for logging in on a computer, or for identifying a voter in a polling station on election day.

7. In the vast majority of countries where biometrics have been used in civil/voter registration, the motivation for using biometrics has been to de-duplicate the register. Often these countries have had no reliable register beforehand or the identification documents have been of such standard that falsification has been easy.

8. People register multiple times for several reasons. It can be for the purpose of voting several times, it can be to obtain other services several times (e.g. pensions), it can be to "cheat the system" and flaunt it, or it can simply be due to misunderstandings. A common occurrence is that the registration process has not been designed to easily allow for a change of address, wherefore people when moving re-register without having their old record deleted. Any registration process design should keep in mind sustainability and the long term maintenance of the system.

9. The use of biometrics for identification on election day is not a common motivation for civil/voter registration. There are no cases known to this author of countries employing biometrics on election day. A few countries use barcode or card readers on election day to check that the voter belongs to the polling location in question, but these do not include biometric checks. It is solely a means to replace a paper voter list and the time it takes to find a person on the list with a faster, electronic solution. The check that the ID card belongs to the person holding it is usually a simple visual check that the face of the person corresponds to the photo on the ID card.

Technologies

Fingerprints

10. Fingerprinting is the type of biometrics that has been used the longest. For more than a century criminal forensics have compared fingerprints on paper to prints found at crime scenes.

11. No two prints are identical. Twins do not have identical prints. The left and right hand prints of a person are not identical. You can't tell a person's age, gender or ethnicity from their fingerprints.

12. The way it works is that various points and features of each print are measured in relation to each other. Determining these points is called to create the print's "template". There is no international standard for developing a template. Various manufacturers use

different proprietary methods to develop the templates, wherefore it is important to keep not only the template, but also the original image of the fingerprint in order to avoid being bound to one service provider.

13. How many points are required to create a template is up to the registration authority to decide. If only a few points are required then a later database matching will create a lot of "false positives", i.e. matched fingerprints that in reality belong to different people. If too many points are required then it becomes very difficult to register people. Dirty or callused fingers can make it very hard to get a print of sufficient quality.

14. De-duplication is made using an Automated Fingerprint Identification System (AFIS). Based on matching parameters set by the operator it will scan the database to find potential matches. Again, if the match criteria are set low too many false positives will be displayed, and if the match criteria are set too high very few matches will be displaced, with the risk that actual duplicate records are not found.

15. The AFIS system works by comparing each print with every other print in the database. For a database of one million prints this means that each print will have to be checked against 999,999 other prints. Totally that's roughly 1,000,000,000,000 comparisons that the computer will have to run.

16. If for every person out of one million not one but all ten prints are captured then the number of comparisons to check increase to 100,000,000,000,000.

17. A common misconception is that when a vendor states that an AFIS server can run e.g. 50,000 matches per second then that means that a million prints can be checked in 20 seconds. As can be seen from the numbers above this is not the case. A million comparisons would take such a server 20,000,000 seconds, i.e. 231 days running around the clock. With ten prints it would take the same server 63 years to do all the comparisons.

18. The number of comparisons to run can be cut down in various ways. If the computer keeps a record of which checks have already been done then the number of checks can be cut in half since comparing fingerprint B to print A is unnecessary if A has already been compared to B. Another option is to limit the check geographically based on how far it is believed that a voter could move on election day, thus potentially allowing double registration but making double voting logistically impossible. Voters have been known to cross fingers, wherefore limiting comparisons to only checking same type of fingers (i.e. right thumb against all other right thumbs) is only advisable where the registration officials are trusted not to make this happen.

19. As hardware becomes faster the above is less of an issue, but still very important to bear in mind when planning. A small pilot will not in itself test the overall time required as the matches are only run on a small number of records.

20. During enrolment – the initial registration of a person – the number of fingerprints to capture must be decided. If only one print is captured then potentially that person could register ten times using ten different fingers (if the registration officials do not prevent it). Capturing a fingerprint is by far the slowest part of the enrolment process and blocks using the computer for other purposes while it is being done. Very importantly the computer should have software installed that can instantly check whether a template of sufficient quality can be developed. In practice, due to the quality requirement, calloused fingers, dirty fingers etc, capturing each print usually takes minutes rather than seconds. Capturing ten prints would mean that enrolment of each voter could take 10-20 minutes. This should obviously be tested in a pilot that includes the most difficult

types of registrants, e.g. those conducted manual labour. The time required can be minimized through good procedures and training, including mandatory cleaning of fingers before reaching the computer. Registration kits should include the necessary cloths and/or wet wipes for cleaning.

21. Current trend is to capture four prints: thumbs and index fingers of both hands.

Facial recognition

22. Facial recognition has several benefits to fingerprints. First of all, voters have only one face compared to ten fingers. Secondly, a photo is usually taken anyway. People are generally also less resistant to having their photo taken compared to fingerprints (with specific cultural differences, e.g. in relation to women in particular countries reluctant to revealing their face).

23. Developing a suitable biometric template from a photo does raise the requirements to the environment in which the photo is taken. Photos taken in poor light or with shadows across the face can pose problems. As for fingerprinting it is highly advisable that the registration computer has software that can determine on the spot whether a suitable template can be developed. This obviously adds to the cost of the kit.

24. The main problem with facial biometrics is that it is not nearly as constant as the fingerprints (or iris and others). The template is developed measuring various points such as ears, mouth, chin, nose etc. This requires the registrant to have a completely neutral expression. For identification such as logging in on a computer this is feasible because the user can change facial expression until recognized, but for de-duplication it is quite possible to cheat the system by deliberately using different expressions, e.g. flaring nostrils, raising eyebrows, smiling more or less. It requires a lot of training of the registration officials to counter this. Ideally facial enrolment entails taking several pictures of the person where the computer can then calculate an average, but this obviously increases the time it takes to register each person.

25. Generally it is not advisable to use facial recognition as the only biometrics for de-duplication. It can however be very useful as an additional supplement to fingerprints, cutting down on the number of false positives that require a human assessment.

Iris scan

26. The iris is as unique as a fingerprint, it is not prone to wear in the same way a fingerprint is, and people only have two irises compared to ten fingers.

27. The equipment required to capture iris scans is however still expensive compared to for example fingerprint scanners. This will likely change over time, making iris scan a more viable option both for registration and later identification.

28. Registration officials have to be trained to check for contact lenses as these could obscure the image and potentially enable multiple registrations.

Signature

29. Often the registrant is required to sign a registration form. This can be on an electronic signature pad. In principle a signature can also be measured and a template developed in the same way as the biological features above. However, as it is very possible to train oneself to fraudulently replicate someone else's signature, and even simpler to alter your own signature while attempting double registration, signatures are not suitable for de-duplication.

Registration in Practice

30. Civil and/or voter registration has been done in many countries around the world, under very different cultural, organizational and motivational circumstances. There are however significant similarities both in terms of what kind of activities are required in order to implement a successful registration, and in terms of how these projects unfold in reality.

Time

31. A registration timeline could entail the following activities:

- Feasibility study and decision in principle
- Legislation (drafting and passing)
- Pilot project
- Procurement
- Training
- Public information campaign
- REGISTRATION PERIOD
- Data processing, including de-duplication
- Display and adjudication
- ID card production
- Distribution of ID cards

32. It is noticeable that the registration period – the period during which data is captured in the field – is often the shortest element of the registration timeline.

33. In some countries (for example Somaliland and Nepal) the registration period has been staggered (i.e. conducted in different regions at different times as opposed to simultaneously throughout the country), which means that registration equipment and staff can be utilized better. This obviously results in a longer overall timeline, but a more economical use of resources.

34. The elements of the timeline that often end up taking the longest – often not planned and thus causing delays – are the initial stages relating to decision making process, political agreement, identification of funding, and passing of legislation. The complexity of these activities should not be underestimated.

35. Another activity that often takes longer than anticipated is the procurement process. Developing an accurate specification, conducting the tender, negotiating agreements and having goods delivered can be very time consuming. Specialized equipment may require manufacturing time if it is not readily available in the quantities required, it takes time for shipment, and quite often import and customs clearance take quite a lot of time.

36. The biggest risk to the timeline lies in insufficient registration – whether qualitatively or quantitatively. If not enough people register during the planned registration period then there may be an enormous pressure on the registration body to either extend the registration period (if the problem is detected early during the registration) or undertake

another field exercise to capture the missing registrants. This obviously delays the entire timeline and adds significantly to the cost.

37. The reasons for low registration turnout can be:

- Lack of motivation and incentive for people to register;
- Poor public information about time, place, purpose, data protection;
- Access to registration including distance and opening times;
- Capacity failures relating to equipment or staffing;
- Boycott for political, ethnic or other reasons;
- Financial reasons related to obtaining required documentation or reaching the registration location;
- Absence from location and lack of absentee registration facilities;
- Intimidation of registrants or other security concerns.

38. All of the factors above can cause registration to be lower than expected. Note that the expectation is often based on unreliable sources except where a census has been conducted recently. The perception alone of a low registration can cause pressure to extend registration or make special provisions for including persons in the voting process through different means. Worst case scenario the voter list is abandoned completely.

39. Insufficient quality of the data obtained during the initial registration can also cause delays. If biometric data is of insufficient quality for de-duplication then data processing may take longer. If the data assigning voters to a polling location is not accurate then the voter list may not be usable on election day.

40. For an accurate estimate of a realistic timeline a detailed plan must be developed. In general, registering an entire population is a long and complicated process, not least politically, that usually takes no less than two years.

Cost

41. The cost of a registration exercise is even more difficult to generalize. Focus is often on the computer, but the largest part of the budget often relate to manpower and logistics. Below is a list of some of the items to consider when preparing a registration budget.

- Registration kit, including computer, camera, fingerprint scanner
- Software for registration kit including biometric suitability check
- Kit container/suitcase
- UPS, generator, other power supply
- Backdrop and appropriate light source for photo
- Consumables, including materials for receipt, fuel
- Preferably a printer to create a printed, legally binding record and provide the registrant with a receipt/temporary ID
- Manpower
- Training

- Voter education
- Logistics
- Facilities (registration center)
- Servers, server software, server facility
- Passports are very expensive. ID cards are cheaper.
- Printing of lists for display and verification
- Adjudication process

Other Anti-Fraud Measures

42. In the concrete context of biometrics, the emphasis regarding fraud is on a person voting multiple times. There are a number of other anti-fraud mechanisms that can help minimize double voting (and other types of fraud) that it might be worth considering as alternatives or supplements to the use of biometrics.

De-duplication through voter list scrutiny, display, alphanumeric matching

43. The "old fashioned" way of removing fraudulent entries in a register, including duplicates, is to publicize the lists and rely on the public at large and political parties in particular to scrutinize the lists and make official objections to entries they consider fraudulent.

44. Political parties can be given lists either on paper or electronically. For the public at large lists can be put on display at the registration/polling locations. Generally the attendance at such events is however relatively low. Political parties are often more engaged in this form of scrutiny than the individual registrants/voters.

45. Another way of de-duplicating a register, predating biometrics, is to try to find duplicates based on the alphanumeric information. This will often be quite successful in removing unintentional duplicates such as a person registering twice because s/he has moved. A person deliberately trying to defraud the system will however attempt to change his/her information so much that matching becomes difficult. Complicated algorithms including phonetic matching are required and do not guarantee good results.

Quality of the ID card, photo voter list

46. Once the registration is completed and de-duplication performed, an important anti-fraud measures is the ID card. If the ID card is easy to forge then identity theft or impersonation can be easy. A photo ID with significant security features such as holograms, microprint and invisible print will make it significantly harder to vote on behalf of someone else.

47. A simple and increasingly popular measure against impersonation is to print photos on the voter list. With photos of a reasonable quality a person attempting to vote on behalf of someone else can be easily detected, not only by the election officials but also by observers and agents. When photos were taken with Polaroid cameras a photo voter list required an expensive scanning process, but since photos are now almost always stored electronically anyway, printing these on the electoral roll is very easy. The only added cost relates to the fact that more pages need to be printed since each record takes up more space. The benefit achieved is very high at a very low cost, and with a very high degree of transparency.

Indelible ink

48. If there is a risk that the register still contains duplicates even after various de-duplication efforts, or if it is perceived that impersonation is a real risk (for example due to availability of fake ID cards), then a risk of multiple voting may still exist. A typical countermeasure against double voting under such circumstances is the use of indelible ink to mark voters. A person who is found to already be marked will not be allowed to vote again.

49. Indelible ink comes in two varieties, an invisible ink that becomes visible under ultraviolet (UV) light, and a visible ink that is hard to wash off.

50. Invisible ink is difficult to wash off only because it is difficult for the marked person to see where to wash. It does not contain as strong means to remain on the finger as the visible ink. In broad daylight you need to be very close to see the ink light up under UV light, making observation difficult. It is also difficult to see if an UV lamp is turned on or off at all, making it possible for corrupt election officials to remove batteries or simply refrain from turning on the lamp. They may also dilute the ink or replace it with water.

51. Visible ink with an appropriate percentage of silver nitrate will stick to the fabric of a person's nail at the cuticle for a week or more. There are however several conditions that all have to be taken into account, requiring proper procurement, good training, and good implementation. Each batch of ink should be tested for the specified level of silver nitrate. Since silver nitrate is metal particles, they will over time settle at the bottom of the ink bottle, making it necessary to shake the bottle ever so often during election day. The finger of the voter must be clean and dry before the ink is applied. The ink must be allowed to dry before the voter leaves the polling station (and before they touch the ballot, potentially leaving invalidating stains). The ink must be applied to the cuticle, i.e. where the nail meets the skin. If these conditions are met then silver nitrate ink is extremely effective at preventing double voting. There are numerous rumours about ink being washed off, but the fact remains that ink is still widely used today, and it is because it works.

Observation

52. Probably the most important countermeasure against fraud is observation, both by political party agents and by independent observers. Observation is a crucial aspect of establishing and maintaining transparency throughput the electoral process, not only during polling and counting, but also during registration.

Electoral Dispute Resolution

53. Of a different nature than the technical measures above such as de-duplication and inking, but crucial nevertheless is the existence of a fair and efficient electoral dispute resolution mechanism. Registrants, agents and observers must have easy access to lodge complaints and objections, and these must be dealt with fairly, transparently and timely. A mechanism that is too bureaucratic or expensive will render all other mechanisms ineffective. Similarly, a mechanism where disputes are only finalized long after the election is over will also not create an electoral environment free of fraud.

Voter Lists in Georgia

54. Georgia has a voter list that is derived from the civil register. It seems to be a widely accepted fact that in the past the voter lists had various problems with erroneous records, including duplicates. There are differing opinions on the quality of the register as it stands today. Some stakeholders have raised concerns about the possibility of persons voting multiple times under the current system of registration and voting.

55. In elections perception is everything. If any part of the electoral process is perceived as being flawed to an extent that could change the overall outcome of the election, then the results may not be accepted or respected. For a country to have a stable and effective government, the government need not only be elected, but also be perceived as having won the election fairly.

56. It is therefore essential that the electoral process is trusted by all stakeholders. In this specific context it is essential that the voter lists in particular are seen as trustworthy and that the electoral process, including verification of voters on election day is seen as being able to eliminate (or at least minimize) the ability to vote multiple times.

Proposals

57. To this extent a group of political parties currently in opposition have prepared a proposal for de-duplication of the register, locking of the database of voters, and identification of voters in the polling station on election day using biometrics. The proposal will not be repeated here in detail.

58. The proposal is complex and extremely well thought through from a technical perspective, weighing various factors. The proposal is at a conceptual stage and the evaluation of it therefore the same. Without going into deep technical details, it is the opinion of the author of this report that each of the three aspects of the proposal – de-duplication, database protection, and identification – are feasible from a purely technological perspective. A more accurate determination of the technical feasibility would require the development and assessment of detailed specifications for each component.

59. While developing the proposals further, the timeline and budget should also be scrutinized in more detail. The timeline and budget should encompass all the aspects mention in the previous chapter of this report in order to give a more accurate picture of what can be expected. The timelines and budgets in the current proposals may be accurate in isolation, but do not encompass all the elements mentioned above.

De-duplication

60. De-duplication using biometrics is certainly feasible and – as mentioned in the previous chapter – a common international practice. De-duplication using facial biometrics only will not yield as accurate a result as using fingerprints, but it is likely to be an improvement over alphanumeric de-duplication. It is even likely that it may provide a higher return on investment than a fingerprint solution, as such a solution would be quite costly in terms of primarily the time required for enrolment and secondly in terms of equipment.

61. The secondary issue of how to ensure that a de-duplicated register remains free of duplicates relates to the trust in the registration authority and the election management

body. Traditionally – and quite successfully – such issues are dealt with through a combination of measures, the most central one being transparency. By providing electoral stakeholders access to scrutinize the voter lists these stakeholders can observe and compare how the lists are being used on election day. An increase in number of records on a voter list between scrutiny and election day would raise a flag, and observers would satisfy themselves that the identity documents provided by the voters are legitimate, correspond to the records on the voter list, and where applicable that the voters have not previously been marked with indelible ink.

Identification

62. The second and third aspect relating to the use of a password protected database deployed on computers in polling stations requiring facial recognition of voters before voting is a novel and yet untested methodology.

63. As mentioned above, this should in theory be feasible from a purely technological perspective. The operational feasibility is however a different issue.

64. Several countries have now used electronic voter lists on election day. They have typically worked offline with a pre-loaded copy of the voter list for that locality and the main purpose has been to facilitate finding a person on the list. There is a significant technological difference between scanning a barcode on an ID card and requiring positive identification using biometrics.

65. Fingerprints for identification work reasonably well, and finding a person within a small subset of voters would not take long; not longer than finding a person on a paper list. Facial biometrics for identification are harder to use and require very controlled lighting conditions. Before embarking on relying on such technology significant testing and piloting should be undertaken.

66. Employing biometric identification kits on election day will be expensive and will require significant training of the operators. It will also require a technical support setup entailing technicians, spare parts and help lines.

67. Observation of the identification process would have to be carefully considered. As mentioned previously, observation is a crucial element in building trust in the electoral processes. It is probably easier to make observers understand how printed lists are compared to ID cards and how to look out for (visible) ink than it is to make them understand how a computer and camera ensures the fairness of the elections. It takes only a few legitimate voters being rejected by the device for the trust to be jeopardized. Observers and agents should be trained to have a good understanding of the identification process.

68. Even if in principle technologically feasible and operationally well prepared with proper contingencies, it would be prudent to consider viable alternatives to reach the same objective. In this context the objective seems to be to minimize double voting. (In other countries the main concern can be to curtail voting by foreigners.) As mentioned above, well proven methods including and combining observation, photo voter lists, photo IDs and (visible) indelible ink may overall have a more positive effect, taking into account cost, risk, public understanding and perception. It would be prudent to analyze and test this before settling on a course of action.

Risk management

69. The more complex technology is employed, the more risk is inherent. If cost benefit analyses justify the cost and risk involved in implementing new technological solutions, then appropriate risk management plans should be implemented to mitigate these new risks.

70. All new technology should be thoroughly field tested and piloted, including the associated procedures, processes and training.

71. Until the new technology has proven a high degree of reliability in full scale implementation (e.g. several country wide elections) it would be appropriate to have redundancy, particularly when it comes to the extremely time sensitive election day. A backup procedure could be to use paper voter lists and indelible ink, bearing in mind that ink then need to be applied to all voters within logistically feasible double voting radius.

Conclusion

72. The use of biometrics for de-duplication of the voter register is a common methodology used in many countries.

73. The use of biometrics for identification of voters in polling stations on election day is not a common practice. There are significant operational obstacles and risks associated with such an undertaking. The benefits should be weighed against the costs and risk, with a view to what alternative methods to avoid double voting might be employed.

74. The most important element in achieving credible and accepted elections is trust. Trust is achieved through transparency and inclusion. Notably all stakeholders must embrace inclusion and participate actively.

75. In broad terms, simplicity is better for transparency than complexity.

76. When new technologies or other elements are introduced, all processes and procedures should be carefully reviewed in view of these new elements. A change of how voters are identified will require changes to many aspects such as training and voter education.

77. Training is in general crucial, particularly of registration and election officials, but also of agents, observers and any other stakeholders involved in the process.

78. Any new system should be tested through a pilot before full scale implementation, and sufficient time should be taken to adjust plans based on the findings of the pilot.

79. A risk assessment should be made and appropriate mitigation and contingency plans should be prepared.

■