Protection of Personal Information in South Africa: A Framework for Biometric Data Collection Security

Phiwa Mzila
Modeling and Digital Sciences, Information Security
CSIR
Pretoria, South Africa
pmzila@csir.co.za

***Abstract*—The use of biometric technology as a means to improve national security and reduce fraud has been adopted by many countries including South Africa. This technology involves the collection of biometric data which is attributed as part of one's personal information. Like many other countries, South Africa, in 2013 officially approved and enacted the Protection of Personal Information Act, which gives guidelines that should be followed when processing personal information. The Act regards biometric data in the same way as any other personal data. As such the processing of biometric data is regulated in the personal information protection act of the country. The responsible party for the collection of personal information needs to implement strict and appropriate measures to protect personal data against unauthorised access. In areas where biometric systems are implemented, biometric data cannot be collected without the knowledge of the concerned person. Designers of biometric systems must engage with appropriate biometric security experts to ensure that security vulnerabilities are appropriately tackled, especially if existing systems are migrated to the internet. This is particularly important because once a biometric data is compromised; it cannot be replaced like passwords and tokens. In this paper we proposed a framework for biometric data collection security using South Africa as our case study. The framework aims to bridge the gap between the collectors of biometric data, biometric security experts and the law enforcement agency for compliance with the protection of personal information act.**

Keywords - privacy; personal information; security; compliance; biometric data.

I. Introduction

The adoption and use of biometric systems world-wide has gained massive momentum. Biometric systems are mostly used for authentication, which comprises of verification and identification. Verification involves the presenting of an actual biometric image and in order to assert whether or not it belongs to a specified person, whereas identification involves the presenting of an actual biometric image and then asking the system to search for a match from a database. As prominent as they are, biometric systems also create a lot of anxiety as far as privacy and security are concerned. Such privacy and security risks come in the form of attacks on databases storing biometric data. When biometric data is compromised, the identity of the person is exposed, and it can then be used for any malicious activities. This behavior can lead to the violation of some policies that are put in place by the authorities of the country such as in the Protection of Personal Information Act (POPI) in South Africa.

Biometric data may be collected and used for various purposes. For example, in South Africa, the collection of biometric data at major border gates is aimed at securing the movement of people in and out of the country. Furthermore, this is done to accurately identify people and determine whether they pose a risk to South Africa. By using biometrics, South Africa's immigration prevents the use of fraudulent documents, protects visitors from identify theft and stops criminals and immigration violators from entering the country. In other cases biometric data is collected from places such as residential complexes, learning institutions, work places for control of access to high security and restricted areas and governmental organs such as police departments and home affairs.

In the process of biometric data collection, written policy and clear guidelines should be developed to ensure proper use of the biometric data collected. This should include among others, awareness, protection mechanism, and penalties for failure to comply.

In South Africa, there is the POPI act, biometric data subjects, responsible parties (data collectors), biometric experts from research and development (R&D) institutions such as CSIR, universities and Centres for Excellence, but there is still no proper framework that integrates all these entities together in ensuring a harmonized protection of biometric data that is being collected by different organizations for different purposes.

Throughout this research work, biometric technologies that improve national security capabilities in access control, identity verification, and online transaction security in a manner that is compliant with the South African POPI act, are analysed. To achieve this objective, relevant South African departments responsible for national security, border control and security, and the law enforcement and financial institutions, are studied. In this paper, we propose a framework for biometric data security in South Africa that incorporates the protection of personal information (POPI) Act and biometric template protection schemes.

II. Biometric Data as Personal Information

According to the POPI act of South Africa, examples of personal data for an individual could include, among others, photos, voice recordings, video footage, and biometric data[1].

A general biometric system will operate as depicted in Fig. 1. At the presentation of biometric modality, the scanner captures an image and performs feature extraction, from which a template is created. A biometric template is a mathematical file representation of location of unique biometric extracted features from a chosen modality image. This file can be anything from a binary mathematical file to a statistical model [2]. Biometric templates are then stored in the database, not the actual image of a biometric image.

There are arguments [3] that the data stored in biometric systems are not personal data because of the two reasons:

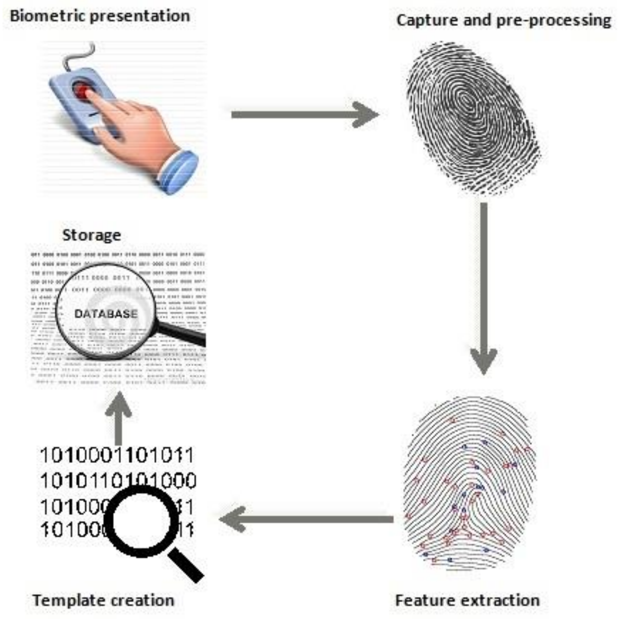

Figure 1. General biometric system

- The stored biometric data are just meaningless binary numbers, and therefore are not personally identifiable information; and
- A biometric image cannot be reconstructed from the stored template.

If we look at the first argument, having these binary numbers linked to other personal identification particulars there is no denying that they are capable of identifying an individual. After all, the purpose of collecting the data and transform them into numbers is to identify and verify a person whose information is associated with the numbers. This is similarly true in the second scenario. A reconstructed template will ultimately reveal the identity of a person. Hence, no matter how the templates are constructed, they are be considered to be the personal data when combined with other identifying particulars of a data subject, hence should be treated with the most privacy and protected just like any other personal information as mandated by POPI Act.

III. Collection of Biometric Data in South Africa

Biometric data may be collected for different reasons, but whatever the reason might be, a responsible party should ensure that the process is lawful and compliant with the POPI act. Let’s consider the following four classified areas in which biometric data is being collected in South Africa: border gates, banking, physical access control and governmental organs. A common major concern in all these four areas is that there is no mechanism implemented for securing users collected biometric data, and by so imposing high risk of fraud and cyber-crime.

A. *Border gates*

The South Africa government launched its biometric collection pilot at all ports of entry as part of country’s project to modernize its Enhanced Movement Control System (EMCS) towards the end of 2015. By using biometrics, South African border gates want to prevent the use of fraudulent documents, protect visitors from identity theft and to stop criminals and immigration violators from entering the country. In the wake of the recent terrorist acts, the country has now enforced the implementation of this initiative which aims to counter-act such malicious events while assuring safety for all [4].

B. *Banking*

The top five banks in South Africa are all exploring biometric initiatives to prevent bank fraud activities. As a result, the South African Banking Risk Identification Centre (SABRIC) was developed together with Online Fingerprint Verification System. The joint initiative will allow banks to access the Home Affairs National Identification System (HANIS) to verify the identity of the enrolled and active clients using their fingerprints. This electronic identity verification system is commended for having the capacity to combat bank-related identity fraud and corruption. It contributes to a positive environment in which the citizens feel safe about their and are indeed secure in the hands of the various banking institutions.

Fingerprints data retrieved from HANIS by banks will not be stored in the databases of banks. The Department of Home Affairs will continue being the only guardian of the HANIS database. Banks will not have a full access to data in the database, but only the ability to verify the identity of a client through information in the database [5].

C. *Physical Access Control*

South Africa is one of the fast developing countries. Organizations are becoming increasingly security conscious, with a growing attention to advanced physical access control and robust access control technologies such as biometric systems. The adoption of biometric systems in physical access control places such as residential complexes, homes and working places is taking a steady growth in South Africa.

The biometric system approach that is employed mostly in physical access control setup is 1 to 1, which is verification. Responsible parties, for example in residential complexes, use fingerprint scanners to capture and collect fingerprint images in huge volumes during enrolment for later use as an access control protocol in the complex. This process is repeated for every new resident moving in. Biometric data subjects are not made aware, let alone being guaranteed that their fingerprints will be securely stored. Furthermore, responsible parties do not assure biometric data subjects what happens with processed data once the contract ends and the resident has to vacate the complex. Is the data deleted or kept in the database? If it is kept in the database, the question then is for how long? Will it not be cross matched in other applications for malicious activities? This conveys biometric security in physical access control under scrutiny, especially in South Africa.

D. Governmental Organs

South Africa's Home Affairs National Identification System (HANIS) was developed as a verification service, which is an initiative that uses fingerprints to verify the identity of active clients and prevent identity fraud, irregular insurance claims and related crimes. This system uses a National Population Register database of fingerprints for all registered citizen of the country. This database can be accessed by all organs of government for different purposes, such as vetting for State Security Department, grant payments for South Africa Social Security Agency and crime investigation for Police Department.

IV. POPI ACT OF SOUTH AFRICA

A. Overview

In this paper and in POPI Act, unless the context indicates otherwise, ''biometrics'' means a technique of personal identification that is based on physical, physiological or behavioral characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition To promote the protection of personal information processed by public and private bodies[1].

POPI binds every entity that is involved in the processing of personal information .It can be any public or private body or any person alone in conjunction with others determines the purpose of and means for processing personal information. In simple terms, the purpose of the POPI Act is to ensure that all South African institutions follow the right procedures when processing(collect, share, store or access) one's personal information by holding them accountable should they abuse or compromise it. The POPI act basically considers one's personal information to be precious goods and therefore aims to bestow upon all citizens of South African, as the owners of their personal information, firm rights of protection and control over the following:

- when and how to share their personal information (requires consent)
- the type and extent of their information to share (must be collected for valid reasons)
- transparency and accountability on how their data will be used (limited to the purpose) and notification if/when the data is compromised
- providing access to their own information as well as the right to have data removed and/or destroyed upon request
- who has access to their information, i.e. there must be adequate measures and controls in place to track access and prevent unauthorised people and companies, from accessing their information
- how and where their information is stored (there must be adequate measures and controls in place to safeguard their information to protect it from theft, or being compromised)
- the integrity and continued accuracy of their information (i.e. their information must be captured correctly and once collected, the institution is responsible to maintain it) [1].

Personal information is widely stated and could include but not limited to list in Table 1.

TABLE I. CLASSIFICATIN OF PERSONAL INFORMATION

Personal Information	
Contact details	Email, telephone address etc.
Demographics	Age, sex, race, birthdate, ethnicity etc.
History	Employment, financial, educational, criminal, medical etc.
Opinion	Opinions of and about the person
Biometrics	Fingerprints, iris, palm, veins, DNA, face, behavior, etc.
Correspondence	Private correspondence

The POPI act lists eight core mandatory information processing principles [6]:

1) *Information quality:* The responsible party must take reasonably practical steps that the personal information is complete, accurate, not misleading, updated and taking into account the purpose for which it is collected

2) *Purpose specification:* Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. The responsible party must take necessary steps to ensure those data subjects are aware of the purpose for which their data is being collected.

3) *Accountability:* The responsible party must ensure that the eight mandatory information processing principles are complied with.

4) *Processing limitation:* Processing must be lawful and personal data may only be processed if it is adequate, relevant and not excessive given the purpose for which it is processed.

5) *Further processing limitation:* This is where personal data is received form a third party and passed on to the

responsible party for further processing. In these circumstances, the further processing must be compatible with the purpose for which it was initially collected.

6) Openness: Personal data may only be processed by a responsible party that has notified the information protection regulator.

7) Security safeguarding: The responsible party must secure the integrity of personal data in its possession or under its control by taking prescribed measures to prevent loss of, damage to or unauthorised destruction of data.

8) Data subject participating: A data subject has the right to request a responsible party to confirm, free of charge, whether or not the responsible party holds personal data, including information about the identity of third parties, who have, or have had, access to the information.

B. Collecting of Personal Information

Under the POPI Act, responsible parties processing personal information from data subject [1]:

- can only collect personal information directly from the owner of the information
- should acknowledges the owner before they collect personal information and obtain his or her consent
- should have adequate reason for collecting this information
- should provide enough transparency on the purpose and intended use of this information
- may only share this information with authorised parties

Responsible parties have a strong mandate by POPI that after the information has been collected from data subject the following two obligations should be followed:

- They should only use the information for lawful purposes that the data subject agrees to. Any further processing must be compatible with the original purpose.
- Access to this information should be limited to authorised parties only and only for as long as they need to perform their duty. Once the third party has completed his or her part, unless authorised for other duties, he or she may no longer have access to this information.

V. Biometric Data Protection Schemes

To comply with POPI, responsible parties need to provide an assurance that collected data is securely stored and protected from hackers and fraudsters in their databases. Traditionally, biometric data (captured image), during enrolment is transformed into unreadable format or file called template as shown in Figure 1. The template is then stored in the database. From a naked eye, a biometric template should be secure enough since it is a mathematical representation of the actual image, making it to be difficult to recreate the original biometric image when associated with other information of the same person, the personality of the person can be revealed. But recent studies [7][8][[9] have successfully proved that, it is indeed possible to reconstruct the original biometric image from a mere biometric template.

Researchers have proposed different schemes in order to secure biometric templates. These schemes should meet four desirable properties for protection biometric templates [10]:

1) Diversity: To ensure privacy, secure template must not allow cross matching

2) Revocability: Compromised template should be revoked and it must be possible to reissue a new template from the same biometric data.

3) Security: It should not be possible to generate the original template from the secured template.

4) Performance: The operation of the protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

Biometric data protection schemes can broadly be classified into two, namely: cryptosystem based approach and feature transformation based approach.

A. Cryptosytem Based Approach

Biometric cryptosystem approach is also known as helper data based method because in this approach some public information about the biometric template is stored. Helper data does not reveal any significant information about the original biometric template. Cryptosystem can be classified either as key binding type or as key generating type. If the key is obtained by binding a key independent of the biometric features with the biometric template is known as key binding approach. If the helper data is derived from the template and the key is directly generated from the helper data and query biometric features is key generation biometric cryptosystem [11].

B. FeatureTransformation Based Approach

In a typical feature transformation based approach, also known as cancellable, during enrolment, the original template is transformed using transformation function (f), and thus the original biometric data are not required to be kept in the biometrics system to ensure user privacy. During the probe stage, a user submits his query biometric data (x) and auxiliary information (p) to the same transformation function (f). The matching module will then match the transformed template with the transformed query (f(x,p)). In the event of a compromise, a renewed template can be simply generated with fresh auxiliary information. An advantage of this approach is that it is possible to generate multiple templates using the same piece of biometric data, since these templates show that there is no correlation that exist between them [12].

VI. Proposed Framework

A. Framework for Biometric Data Collection Security

POPI defines biometric data as personal information. It further imposes an obligation towards businesses and those that are responsible for collection of personal information to apply reasonable security measures to protect it. In the case of biometric data, techniques and methods used for the protection of biometric data (templates) must meet the four properties: security, diversity, performance and revocability [9] as explained in the previous section.

In this paper we propose a framework where an ideal biometric data protection scheme is the solution for responsible parties from various sectors such as industries, government, academics and societies for ensuring that the biometric data which they process is properly secured. This framework will ensure the protection of privacy in biometric data and also enforce compliance with the POPI act of South Africa. Figure 2 depicts a proposed framework as the structure that can close the gap which currently exists in the adoption of biometric systems across different sectors in country. The framework consists of three main entities: compliance, ideal secure scheme and responsible parties.

1) *Compilance:* These are the key principles highlighted by the POPI act as mandatory to all responsible parties.

2) *Ideal secure scheme:* These are four properties of an ideal biometric data protection technique responsible for securing the proccessing of bimetric information, e.g., capturing, collection, storing and accessing of biometric data.

3) *Responsible parties:* These are the orgnisations, industries, academic institutions and societies that are proccessing biometric information and are responsible for its safety and privacy. They need to comply with the POPI act by implementing the ideal bimetric data protection scheme.

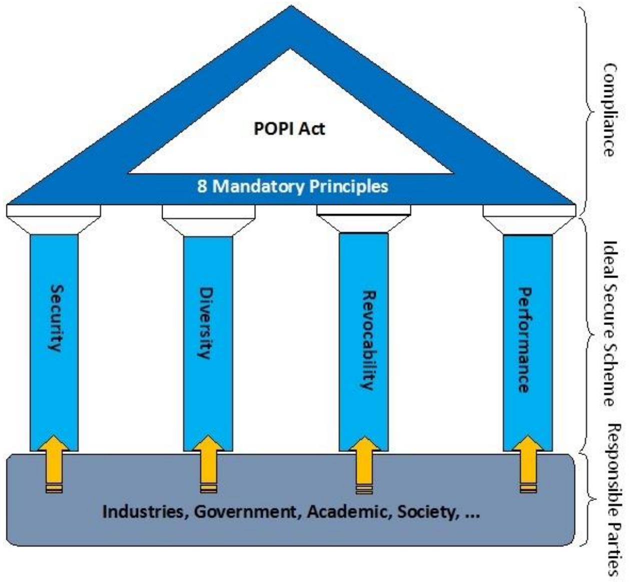

Figure 2. Proposed Framework

B. *Rationale of Biometric Data Security*

Consequences of stolen biometric data can be very severe. In most biometric applications, biometric data is stored in central databases as templates, otherwise smart cards, mobile devices, and tokens can also be used to store it. This poses several risks about privacy and security such as identity theft and cross matching.

An adversary can create a fake modality to spoof biometric systems. He can also track activities of a victim in other biometric applications. Unfortunately a biometric modality is hard or impossible to change. Compromise of biometric data is permanent. Renewing or revocation of biometric identities is infeasible [13].

VII. Conclusion

The exposure of biometric information can result in serious security and privacy concerns. It has taken a long period of time for experts in law enforcement to realize the significance of considering the protection of biometric information in drafting legislation documents that govern the country. South Africa, for example, passed the protection of personal information act in 2013.

The POPI gives various mandates and instructions to everybody who collects and processes personal information to follow prescribed practices in the act. Furthermore, the POPI provides the list of rights to data objects (public) about their personal information. One of the critical personal information a human being possesses is biometric information. The responsibility of ensuring that this biometric information is properly secured wherever it is stored is purely assigned to responsible parties.

Considering the impact a compromised biometric data can have in the society, such as identity theft and cyber-crime, in this paper a framework for biometric data collection security has been proposed. This framework enables existing solutions that securely protect stored biometric data, in the form of templates to support the adoption of the POPI in different sectors such as industries, government organs, academics and societies where responsible parties are employed. The proposed introduction of four properties regarding privacy and security fills the gap and projects an ideal solution that supports the eight principles of the POPI act.

References

[1] Republic of South Africa Government Gazette: Protection of Personal Information Act, 2013.

[2] R. Das: What a biometric template is. [Online], Available from: http://www.biometricupdate.com/author/ravi-das/ 2016.05.18

[3] R. B. Woo, “Challenges posed by biometric technology on data privacy protection and the way forward,” The Privacy Commissioner for Personal data, Hong Kong, 2010.

[4] J. Lee, “South Africa plans entry biometrics at every port of entry by August 2016,” Biometric Update [Online], Available from: http://www.biometricupdate.com/201512/south-africa-plans-entry-biometrics-at-every-port-of-entry-by-august-2016 2016.05.18

[5] M. Gigaba: Department of home affairs budget vote 2015/2016, Republic of South Africa Government Services. [Online], Available from: http://www.gov.za/speeches/minister-malusi-gigaba-home-affairs-dept-budget-vote-201516-6-may-2015-0000/ 2016.04.08

[6] LexisNexis Risk Solutions: POPI Safeguarding right to Privacy[Online]. Available from www.lexisnexis.com/risk 2016/05/20.

[7] M. Bromba, “On the reconstruction of biometric data from template data,” Bromba Biometrics, 2006.

[8] A Kholmatov, B. Yanokoglub, “Realization of correlation attaxck against fuzzy vault scheme,” In Proceedings of SPIE Security, Forensics, Steganography, and Watermarking of Multimedia Contents, vol. 6819, 2008.

[9] W. J. Scheirer, T. E Boult, “Cracking fuzzy vaults and biometric encryption,” In Proceedings of the Biometrics Symposium, 2007.

[10] R. Tigga, A. Wanjari, “A Survey on Template Protection Scheme for Multimodal Biometric System,” International Journal of Science and Research (IJSR), 2013, ISSN:2319-7064.

[11] P.Poongodi, P. Betty, “, A study on biometric template protection techniques,” International Journal of Engineering Trends and Technology (IJETT), vol.7, 2014.

[12] Y.J. China, T.S. Onga, A.B.J. Teohb, K.O.M. Goh, “Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion,” Information Fusion, vol 18, p. 161-174, 2014, doi:10.1016/j.inffus.2013.09.001.

[13] P. Tuyls, J. Goseling, “Capacity and Examples of Template Protecting Biometric Authentication Systems,” BioAW, LNCS3087, p.158-170, 2004.