

REGULATORY

One database for all your identification information? Privacy considerations

5 July 2023 4 min read

The Department of Home Affairs (**Home Affairs**) recently published the Draft National Identification and Registration Bill (**Draft Bill**). The Draft Bill aims to provide for, amongst others, the establishment of a population register and identification database. This will include a biometric national identity system that will enable a single view of a person in the population register and identification database.

The proposed approach by Home Affairs will in no doubt increase the risk to individual privacy particularly through data breaches (i.e. where the personal information of a person has been accessed or acquired by an unauthorised person). A single centralised database containing such valuable information will always be a target for cyber criminals. As such, we explore the idea of the proposed consolidated identification database and explain why it may or may not be a good idea.

South Africa currently has three databases for recording people within the country namely:

- The national population register – which is used to affirm the identity, status and rights of citizens.
- The biometric National Identity System (**NIS**) – which aims to enhance access to a variety of services for citizens and foreign nationals living in South Africa. In particular, the NIS will be a single integrated source of biographic and biometric information.
- The Visa Adjudication System – which centralises the adjudication of long term visas within Home Affairs.

The Draft Bill seeks to consolidate these three databases into one registry.

There is no doubt that having such valuable and sensitive information in one place will create a very significant (and possibly vulnerable) target for cyberattacks. That is not to say that a centralised database for identification information does not present benefits. However, the question must be asked as to whether or not government is well placed to deal with the challenges that often face not only public bodies but private bodies as well, who hold valuable information.

In a previous [article](#) we detailed how shocking it was for many South Africans to learn of the rape of several women near Krugersdorp in July 2022. To make matters worse the victims had to deal with their personal information such as names, residential addresses and occupations appearing on social media platforms. Upon investigation by the Information Regulator it was found that the South African Police Service had unlawfully shared the personal information of the victims on WhatsApp groups. This led to the information being leaked and widely shared on various social media platforms, which constituted a data breach.

In another instance which occurred in 2021 the Department of Justice and Constitutional Development (**DoJ**) suffered a data breach when all of its information systems were encrypted by cybercriminals who gained access to their information systems. This affected bail services, emails, child maintenance services, the issuing of letters of authority, and many other DoJ enabled services.

Transnet was also hit by a data breach in July 2021 which affected Transnet Port Terminals (**TPT**), the entity which operates container handling facilities across the major ports in the country. This caused Transnet's ports to shut down which meant that TPT could not perform any of its obligations under multiple commercial agreements. More importantly, it meant that many goods related industries in South Africa were affected for the duration of Transnet's "downtime" caused by the breach.

What we see from the above is that government entities and departments are often targeted for cyberattacks. As such, the question must be asked as to whether government can provide enough assurance to a whole population that their information will be safe in this one database. Without the necessary assurance and confidence in the proposed system, it will only be a matter of time before another

government-related data breach is added to the ones discussed above. What is more at stake this time is that it will be many more millions of people who will be affected, along with their most personal, sensitive and ultimately valuable information.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)