

Icasa linking SIM cards to biometrics - how new regulations aim to keep consumers safe

Linking biometric data to SIM cards has been proposed by the Independent Communications Authority of South Africa (Icasa). New regulations would require all South Africans to provide their biometric data to mobile service providers to obtain a new cellphone number or action a SIM swap.



Source: [Unsplash](#)

The proposals are included alongside other draft regulations published by the regulator which close for public comment on Wednesday, 11 May 2022. Icasa's proposal calls for biometric data such as fingerprint mapping, facial recognition, and retina scans to be bound to a consumer's SIM card.

Amid privacy concerns around protecting biometric data, Gur Geva, co-founder and CEO of iiDENTIFii, says the objective of the new proposals is to prevent serious crime and protect consumers from the financial and emotional trauma of identity fraud where associated phone numbers are used.



Gur Geva, co-founder and CEO of iiDENTiFi | image supplied

“Criminals who use a multitude of mobile numbers in illegal activities including fraud, money laundering, terrorism and kidnapping would have a harder time hiding from law enforcement should new regulations come into effect. And because biometric data cannot be copied, consumers would have an added layer of protection against their cell number being used in identity theft or to authenticate fraudulent payments.”

Geva says the technology behind binding biometrics to SIM cards is well-established and, crucially, is safe and secure.

“Biometric technology is already a common security feature offered by financial service providers like banks and insurers to protect consumers. The proposed regulations are far more sophisticated than current Rica laws in terms of protecting South Africans against fraud.”

The communications regulator says stricter security measures are required to curb the hijacking of mobile phone numbers either through porting or via a SIM swap transaction, among other instances of fraudulent activity.

“How biometric data is managed by mobile operators would still be subject to strict privacy laws laid out in the Protection of

Personal Information Act (PoPIA) and the General Data Protection Regulation (GDPR) guidelines. Raw biometric data wouldn't be stored so citizens can rest assured their information is encrypted and non-transferable," he says.



Icasa looks into the subscription broadcasting services market

10 May 2022



There is concern that biometric data can be used for various other means once captured by the mobile service provider, but in reality, there is very little difference between what is being asked of the mobile service providers and what customers have had to provide to financial institutions, explains Geva.

"Biometric authentication, together with liveness detection, is a powerful weapon in the fight against identity fraud which is on the increase and costs the South African economy at least R1bn each year."

The move towards biometrics has several other important benefits beyond combatting identity fraud.

"Government departments like Home Affairs and Social Development would be able to ensure grants, documents, and other communication reaches the intended recipient. There are also massive opportunities within the digital payments space as remote biometrics enable access to services that have the potential to make a meaningful impact on financial inclusion. As most South African adults own a mobile phone, biometrics takes the friction out of the payment process, making transactions easy, instant, and secure," says Geva.

He adds that biometrics technology is being used extensively to modernise ID systems in over 30 countries across the globe as governments look to increase efficiencies in key processes within social services, tax management, and border control while eliminating instances of ID duplication fraud.

For more, visit: <https://www.bizcommunity.com>