amaBhungane
Centre for Investigative Journalism

The Media Mill, 7 Quince Street,
Milpark, Johannesburg 2092
+27 10 493 3320
admin@amabhungane.org
www.amabhungane.org
@amaBhungane
facebook.com/amaBhungane

The Independent Communications Authority of South Africa

By email: ELetlape@icasa.org.za

TKhomo@icasa.org.za

11 May 2022

To Whom It May Concern:

Submissions on the draft Amendment Numbering Plan regulations, 2016, in accordance with chapter 11 of the Electronic Communications Act, 2005 (Act No. 36 of 2005)

1. Introduction

1.1. The amaBhungane Centre for Investigative Journalism (amaBhungane) welcomes the opportunity to make submissions on the draft Amendment Numbering Plan regulations, 2016 (draft regulations).

1.2. AmaBhungane is an independent, non-profit company founded in 2010 to develop investigative journalism so as to promote free, capable and worthy media and open, accountable, just democracy. As amaBhungane practises investigative journalism, we are ideally placed to identify legal, policy and practical threats to the information flows that are the lifeblood of our field. We have worked on information rights matters of direct benefit to investigative journalists and the public at large since 2010.

1.3. AmaBhungane has also advocated against excesses in government surveillance, most notably as reflected in our litigation concerning the constitutionality of the RICA Act. Our concerns about certain provisions in that Act were confirmed by the Constitutional Court in 2021. We maintain the view that the Constitution demands that surveillance (being the "close monitoring" of people) whether by state or private actors must be conducted *only where absolutely necessary* and where sufficient safeguards are in place against abuse or excesses in surveillance. This is in order to protect the privacy and freedom of the South African public.

1.4. We view the biometric data registration regime contained in proposed in regulation 6A (5) to (10) (biometric provisions) of the draft regulations as firstly, not an effective long-term solution to addressing the identified nuisance, and secondly, encroaching on the privacy of SIM card purchasers in an unjustifiable manner. It is therefore undesirable as a method to prevent unauthorised SIM swaps and should be rejected as policy choice. We expand on this further in our submission.

1.5. We confirm that we are available to make oral submissions should an opportunity to do this be provided.

1.6. Kindly direct any queries in relation to these submissions to chereset@amabhungane.org.

2. **Registration of biometric information upon SIM purchase will not solve unauthorised SIM swaps**

2.1. The use of one-time passwords (OTPs) has pushed mobile network operators (MNOs) into the role of authenticators of user identity for a variety of purposes – web-based sales transactions, access to applications and customer accounts, and online banking. By providing the OTP sent to the customer's registered mobile number, it is taken that the user themselves have authorised the transaction. While there are benefits to this process, this has led to MNOs assuming a role that extends beyond their original purpose of facilitating communication between users.

2.2. That this method of verification of identity creates opportunities for fraud in the form of unauthorised SIM-swap transactions should give pause for thought as to whether SIMs should be used *at all* as a verification mechanism, and whether better, safer methods can be devised.

2.3. That question is beyond the scope of this submission. We only seek to emphasise that linking biometric data to SIM cards upon registration only further entrenches this undesirable verification method, making it more difficult to move away to newer, better verification methods. It does so without *solving* the problem of unauthorised SIM swaps, only alleviating them to a limited extent and only for a limited time.

2.4. The weaknesses of biometric data as a verifier of identity have been well-documented. These include:

2.4.1. *Human error*: when data-collection procedures are not adequately established or implemented, it may not match future verification scans, obviating their usefulness. In the South African context, mobile operators would have to conduct many hours of training of all their shop-floor employees to ensure that they capture biometrics correctly.

2.4.2. *Natural change:* Human bodies change over time, such as due to age, creating discrepancies with the recorded data. Daily manual labour may also potentially alter fingerprints.

2.4.3. *Correcting errors:* Where such errors happen, correcting them can be a long and difficult. What will suffice as proof that the person presenting themselves is, in fact, the person on record, if the biometrics do not match? The answer to the question (thorough examination of identification documents? An affidavit?) should be considered in the first place as the relevant authentication method instead of biometrics.

2.4.4. *Fraud*:

2.4.4.1. Fingerprints can be lifted from many materials that people touch daily. An internet search for "how to fake fingerprints" is replete with results. In India, over 1000 silicon moulds of fingerprints were used to obtain food rations that were part of a social assistance programme fraudulently.[1] Researchers at Cornell University have also been able to create "master fingerprints" (similar to a master key) that are capable of matching with a

[1] https://mg.co.za/article/2020-02-21-biometric-data-poses-grave-risks-to-privacy/

number of real ones.[2] Advances in deepfake technology have also placed the reliability of voice biometric verification into question.[3]

2.4.4.2. In addition to the manual methods above, biometric data files can also be hacked. This happened in the US Office of Personnel Management in 2015, where over 5.6 million fingerprints of former and current government employees were stolen.[4] There are also risks in transmitting and storing biometric data. Encrypted information can be hacked, and may not necessarily be safe once they arrive in local, foreign, or cloud servers.

2.4.5. Given the many vulnerabilities described above, perhaps the most important reason not to rely on biometrics as a verifier of identity is this: **once stolen, biometric information – whether fingerprint, voice, facial features or the like – cannot be changed.** This is unlike the case of knowledge-based identifiers such as passwords.

2.4.5.1. While it may be tempting to say in this context that the user will simply have to purchase a new SIM, this does nothing to cure the potential damage should the stolen data be applied to other, non-SIM related purposes. These include access control at buildings, in-person bank transactions, and at border control points as a condition for entry to certain countries.

2.4.5.2. Making biometric data collection mandatory as a condition of SIM purchase takes away consumer choice. A consumer may value keeping their biometric data private *more* than mitigating the risk of online accounts being stolen using SIM swaps – or, they may wish for other measures to be used that are less invasive into their privacy, such as password protection. Across the board biometric data collection robs such consumers of the ability to opt out of incursions into their privacy.

2.5. It is well established that as new cybersecurity technology is developed, bad actors are swift to devise mechanisms to evade or break through the safeguards. Biometrics are therefore not a permanent solution to the issue of identity theft. It is, at best, a temporary deterrent, until it becomes redundant due to bad actors being able to overcome protections. While this may be the case with many cybersecurity applications, the difference is that biometric data remains with the person for the rest of their life. During this time, the potential for harm to individuals is considerable.

2.6. The best way to guard against the theft/abuse of biometric data is simple: do not collect it in the first place, and do not rely on it as a method of identity verification.

2.7. When biometric data is used for other applications (such as immigration, SASSA grants, access control, banking etc) some may argue that using biometric verification for one more purpose – being SIM identification – is inconsequential.[5] But that argument cannot stand for the following reasons:

[2] Bontrager, Roy, Togelius et al. "DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution".

[3] https://www.securitynewspaper.com/2021/06/14/how-to-hack-banks-voice-recognition-system-voice-biometrics-with-deepfake-voice-cloning/.

[4] https://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/.

[5] For instance, fingerprints are collected by Home Affairs when applying for an identity document.

2.7.1. Using biometrics for identification linked to SIM cards will create massive databases of biometric information housed in a few MNOs. South Africa has some 109.1 million mobile subscribers spread across five main MNOs.[6]

2.7.2. The protection of this data will be left solely to those MNOs. The regulations do not contemplate comprehensive measures to protect the data collected, nor is there any provision for inspection of such measures by ICASA or any other authority, nor any penalty for breaches where measures are insufficient.

2.7.3. While the subregulation (8) of the draft regulations provides that the biometric data collected is used for the sole purpose of authentication for SIM swaps, there is no guarantee that MNOs will not use that information for commercial purposes. There is no corresponding offence in the regulations, and even if there were, it is unclear who would enforce it and how. Authorities are not privy to the internal workings of commercial enterprises, including how they store and manage their vast swathes of data.

2.7.4. Biometric information therefore:

2.7.4.1. cannot verify identity with certainty;
2.7.4.2. is vulnerable to fraud; and
2.7.4.3. could potentially be used by MNOs for commercial purposes without oversight.

3. There are several alternative means to prevent unauthorised SIM swaps that do not involve the collection of biometric data

3.1. Several proposals to counter SIM swaps that can address the harms of unauthorised SIM swaps without the need to collect biometric data have been made by jurisdictions at the forefront of technological development, such as the United States of America. They also include countries with advanced privacy protections from which South Africa has drawn guidance, such as Europe.

3.2. Rather than assuming that biometrics or any other form of technology will serve as a silver bullet to stop SIM swap fraud, these proposals turn to easily-implementable solutions that will not require costly infrastructure to be installed by MNOs to collect and store biometric data, nor advanced training of staff to collect biometric data accurately.

3.3. The proposals include the following:

3.3.1. *Back-end identity verification*: This can include checking the most recently provided postal address associated with the account, cross-checking the ID card presented in store with previous copies maintained under the subscriber's profile and examining the customer's recent contacts with the MNO's customer representatives.

3.3.2. *Identity verification via password:* This has the benefit of being able to be changed if stolen. Further, if the customer no longer has the original SIM (such as due to theft or destruction), this can be used to confirm identity without use of an OTP.

[6] https://www.geopoll.com/blog/mobile-penetration-south-africa/.

3.3.3. *OTPs:* In-store verification can also be achieved by sending an OTP to the number that is sought to be swapped. OTPs can also be sent to email addresses associated with the account in respect of contract customers.

3.3.4. *Notification and delay requirements:* Prior to the SIM swap being executed, customers can be notified via SMS, phone call and/or email about the proposed SIM swap, and the customer can be provided with a specified time period within which to contact the MNO and block the swap if unauthorised.

3.3.5. *Port-freeze requirements:* This gives the customer the option, in advance, to block SIM swaps on their account.

3.3.6. *Regular and targeted training of employees:* The European Union Agency for Cybersecurity, ENISA, recently reported that 84% of cyber-attacks rely on social engineering, and that "SIM swapping relies greatly on social engineering of MNOs' employees".[7] ENISA proposes that regular cybersecurity awareness training tailored to the audience and specific topics should be implemented for employees as well as third-party employees. Records of such training should be maintained.

3.3.7. *Encourage cooperation between MNOs and banks*: This can be achieved by using an application programming interface or other notification methods provided by the MNOs to check whether a SIM swap has recently been performed. This can trigger additional checks by the bank before transactions are processed.

3.3.8. *Avoid remote SIM swapping processes*: Remote/online SIM swaps should be avoided. Stores should have mandatory processes to follow to effect SIM swaps, and notification mechanisms set up to notify other outlets of MNOs where a failed SIM swap is attempted at one of their branches.

3.3.9. *Consumer education*: MNOs can conduct awareness campaigns (whether directly or through the media) notifying customers of the dangers of SIM swaps and ways to keep their accounts safe.

3.4. The benefit of these and other proposals is that they can be used in conjunction with each other, enhancing their effectiveness, and tailored to the South African landscape. Should they prove ineffective, other solutions can be tested and adopted. This is unlike biometric verification which loses all effectiveness as a verifier of identity in the event that a user's data is stolen.

4. There are principled reasons to reject further attempts to develop surveillance architecture

4.1. For the reasons set out above, it is apparent that biometric data collection is undesirable as a means to prevent unauthorised SIM swaps, and better alternatives are available.

4.2. It bears emphasising that on principle, there are good reasons to reject attempts to further entrench biometric data verification in the lives of South Africans.

4.2.1. "Surveillance creep" refers to the phenomenon where surveillance systems expand over time to find new uses and become pervasive in more areas of life.

[7] https://www.enisa.europa.eu/publications/countering-sim-swapping/@@download/fullReport.

This process chips away at the privacy of members of the public, while at the same time desensitising them to this process. The result is that the public accepts more and more incursions into their privacy. Such privacy is given up for what is touted as improvements in safety and security but which can often marginally effective at best.[8]

4.2.2. The reality is that this process involves a significant power imbalance. Whether it be cameras in public places, biometric data collection, or tracking of online activity, the public being monitored have no control over the data collected about their lives. They do not know who has access to it, whether it is handed over to others, whether it is protected from misuse, or whether it is used for purposes beyond for which it was collected. They cannot demand to see what has been collected, nor that it be destroyed.

4.2.2.1. While data protection and privacy laws such as the Protection of Personal Information Act, 2013 exist, it is often extremely impractical for members of the public to exercise them, due to time and resource constraints, lack of awareness and the sheer volume of surveillance. Regulators charged with enforcing these laws (in South Africa, the Information Regulator) lack capacity to do so. Additionally, in many cases, subjects are not aware that they are being monitored in the first place.

4.2.2.2. It is not feasible for members of the public to opt out of biometric data collection by not purchasing SIM cards. Mobile telecommunications are ingrained into modern life. It is extremely difficult for a consumer to opt out of such surveillance by not purchasing a SIM card.

4.3. In addition to the above, there is also the risk that South Africa could become a testing ground for biometric technology "with China and the US leading the way in piloting such technologies and offering them on a trial or discounted basis. This is arguably part of a geopolitical strategy to develop surveillance norms."[9] There is also a risk that South African biometric data could be " exported and monetised by private foreign actors or states", which has already happened in Zimbabwe.

5. <u>Conclusion</u>

5.1. The growing tolerance for the acceptance of biometric data verification should not be left uninterrogated. Biometric data is extremely personal to the individual – facial features, the shapes of ears, the colours in irises – while at the same time very public. We generally do not shield our faces from public view, nor can we wipe every fingerprint we leave.

5.2. When biometrics as a form of identity verification is shown to:

5.2.1. be subject to myriad vulnerabilities,

5.2.2. have limited usefulness, with redundancy fast approaching due to improved methods to fake biometric markers;

[8] The Aadhaar centralised biometric identity verification system is a cautionary tale in function creep. See https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized.

[9] Allen and Van Zyl, "Who's watching who? Biometric surveillance in Kenya and South Africa". https://enact-africa.s3.amazonaws.com/site/uploads/2020-11-11-biometrics-research-paper.pdf.

5.2.3. have no way of being updated once compromised to ensure ongoing security protection;

5.2.4. advance surveillance creep and unwarranted incursions into people’s privacy, and

5.2.5. not be the only means by which to prevent unauthorised SIM swaps, with other less resource-intensive solutions being adopted by other countries;

it is clear that the proposed biometric provisions of the draft regulations represent the incorrect policy choice to address the issue of unauthorised SIM swaps.

5.3. **We therefore maintain the view that the biometric provisions be deleted from the draft regulations in their entirety, and that a public consultation process be opened to solicit inputs from the public on potential mechanisms to address the issue.**