Suite No.2, Art Centre, 22 6th St, Parkhurst, Johannesburg, 2193
PO Box 1560, Parklands, 2121 | Tel: +27 11 78 1278 | Fax: + 27 11 788 1289
Email: info@mma.org.za | www.mediamonitoringafrica.org

11 May 2021

TO: INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA
E-mail: ELetlape@icasa.org.za and TKhomo@icasa.org.za

SUBMISSION BY MEDIA MONITORING AFRICA:

DRAFT AMENDMENT NUMBERING PLAN REGULATIONS, 2016, IN ACCORDANCE WITH CHAPTER 11 OF THE ELECTRONIC COMMUNICATIONS ACT, 2005 (ACT NO. 36 OF 2005)

For more information, please contact:

William Bird, Director, Media Monitoring Africa
Email: williamb@mma.org.za
Tel: +27 11 788 1278

Thandi Smith, Head of Policy, Media Monitoring Africa
Email: thandis@mma.org.za
Tel: +27 11 788 1278

This submission was prepared with the assistance of Power Singh Inc.
For more information, please visit https://powersingh.africa/.

TABLE OF CONTENTS

INTRODUCTION 3
OVERVIEW OF MEDIA MONITORING AFRICA 3
PRIVACY CONSIDERATIONS 4
The importance of the right to privacy 4
Protecting personal information 5
THE PURPOSE OF THE INCLUSION OF BIOMETRIC DATA 7
Lessons from other jurisdictions 8
Less invasive approaches 11
CONCLUSION 12

INTRODUCTION

1. Media Monitoring Africa ("**MMA**") welcomes the opportunity to provide this submission to the Independent Communications Authority of South Africa ("**ICASA**") regarding the Draft Numbering Plan Regulations ("**Draft Regulations**"). MMA notes at the outset that there are serious privacy concerns and an urgent need for ICASA to engage with the Information Regulator before this process proceeds any further. MMA, therefore, urges ICASA to approach the Information Regulator as a matter of priority before taking any further reform steps.

2. Having had regard to the Draft Regulations, these submissions are dealt with in three parts: the importance of the right to privacy; the purpose of the biometric registration; less invasive measures. Accordingly, this submission is structured as follows:

    2.1. ***First***, an overview of MMA;

    2.2. ***Second***, our submissions with regard to privacy and data protection;

    2.3. ***Third***, our submissions with regard to the purpose of the biometric inclusion, with specific reference to concerns raised in other countries; and

    2.4. ***Fourth***, the need to adopt less invasive measures.

3. These are dealt with in turn below.

OVERVIEW OF MEDIA MONITORING AFRICA

4. MMA is a not-for-profit organisation that has been monitoring the media since 1993. MMA is an active member of the South African civil society space and works alongside an array of non-governmental organisations ("**NGOs**") to promote a culture of human rights. MMA also engages in a range of legislative and litigious processes relating to the triad of information rights, which include the rights to privacy, freedom of expression and access to information. In this regard, MMA has dealt with issues pertaining to data protection, online content regulation, cybercrimes and cybersecurity, copyright, public broadcasting, and various other matters relevant to the exercise of rights, both on- and offline. With specific reference to issues pertaining to privacy, MMA has had a number of engagements with the Information Regulator established in terms of the Protection of Personal Information Act 4 of 2013 ("**POPIA**") and has made submissions on the draft regulations published in terms of section 112(2) of POPIA.

5. MMA has engaged with ICASA on a number of previous occasions, including in respect of issues pertaining to editorial independence, spectrum, disability rights and the broadcasting of sports events. In all its work, MMA is guided by the Constitution of the Republic of South Africa, 1996, the public interest and the interests of justice. It is accordingly through this lens that the submissions below should be considered.

6. For more information about MMA, please visit: www.mediamonitoringafrica.org.

PRIVACY CONSIDERATIONS

The importance of the right to privacy

7. The right to privacy is an "important constitutional right"[1] that "embraces the right to be free from intrusions and interference by the state and others in one's personal life".[2] The Constitutional Court has on more than one occasion emphasised the importance of the right to privacy, noting that an "invasion of an individual's privacy infringes the individual's cognate right to dignity, a right so important that it permeates virtually all other fundamental rights."[3]

8. The protection of personal information is a constitutional imperative that gives effect to the right to privacy.[4] Personal information includes, but is not limited to a person's name, address, identity number, biometric data and information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.[5]

9. The Draft Regulations propose the collection and use of biometric data. Collecting personal information, such as biometric data in the absence of safeguards that ensure the integrity and security of personal information poses a threat to sensitive information and may undermine the right to privacy. According to the U.N. High Commissioner for Human Rights, biometric data is—

> "particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. ***Against that background, it is worrisome that some States are embarking on vast biometric data-based projects without having adequate legal and procedural safeguards in place***."[6] (own emphasis).

---

[1] *AmaBhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC and Others* [2021] ZACC 3; 2021 (4) BCLR 349 (CC); 2021 (3) SA 246 (CC) ("*AmaBhungane*") at para 2

[2] Gaertner v Minister of Finance [2013] ZACC 38; 2014 (1) SA 442 (CC); 2014 (1) BCLR 38 (CC) at para 47.

[3] *AmaBhungane* above n 1 at para 28.

[4] Protection of Personal Information Act 4 of 2013 (POPIA) at section 2.

[5] Ibid definition of "personal information" at section 1.

[6] Report of the United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age' (2018) (accessible here: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F39%2F29&Language=E&DeviceType=Desktop&LangRequested=False).

10. As an organ of the state, ICASA is bound by the Bill of Rights[7] and is therefore enjoined to respect, protect, promote and fulfil the rights contained therein.[8] It is necessary to recognise that the Draft Regulations have the potential to constitute a significant limitation of the right to privacy.[9] MMA urges ICASA to ensure that the importance of the right to privacy is expressly articulated in the Draft Regulations and that any limitation of the right is only provided for to the extent that it is reasonable and justifiable in an open and democratic society.[10] In doing so, regard must be had to whether there are less restrictive means available to achieve the same purpose, this will be addressed in more detail below.[11]

11. MMA further emphasis that privacy persevering approaches are not limited to the biometric registration. MMA submits, that any requirements for personal information to be linked to the assignment of a mobile number must be considered in line with the POPIA and must guard against privacy infringements. To this end, MMA records some cautions regarding the mandatory registration of SIM cards. Privacy activists have noted concern that "mandatory SIM card registration eradicates the potential for anonymity of communications, enables location-tracking, and simplifies communications surveillance and interception."[12] MMA further refers ICASA to the 2015 Report of UN Special Rapporteur on Freedom of Expression, David Kaye, who stated that "compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest."[13] MMA is not suggesting that ICASA has nefarious intentions, MMA simply raises these cautions to illustrate the need to ensure that appropriate safeguards are in place particularly when there are mandatory processes that require personal information.

Protecting personal information

12. We note with concern that the Regulations are silent on ICASA's commitment to comply with POPIA to ensure that personal information is processed in compliance with our data protection framework. Such a commitment is necessary to respect, protect, and promote the right to privacy enshrined in section 14 of the Constitution.[14] Inherent in this right is the ability of every individual to determine what information about themselves is made public and to control how that information is collected and used. Biometric data is defined as personal information in terms of POPIA,[15] and its collection, en mass, needs to be managed appropriately in order to ensure compliance with POPIA and safeguard individuals' rights to privacy.

13. MMA further notes that privacy concerns are prevalent in relation to potential data sharing and the identification of the responsible party. In terms of the Draft Regulations, licensees

[7] Section 8(1) of the Constitution.
[8] Section 7(2) of the Constitution.
[9] Section 14 of the Constitution.
[10] Section 7(3), read with section 36, of the Constitution.
[11] Section 36(1)(e) of the Constitution.
[12] Privacy International, '101: SIM Card Registration' (9 January 2019) (accessible here: https://privacyinternational.org/explainer/2654/101-sim-card-registration).
[13] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (2015) (accessible here: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/32).
[14] The Constitution of the Republic of South Africa, 1996.
[15] POPIA at section 1.

are required to collect biometric data. In terms of the Regulations, a "licensee" means a person or entity that has an individual electronic communications services (l-ECS) using numbers from the numbering plan.[16] While ICASA is not responsible for the collection or processing of the data, ICASA, through the Draft Regulations is a public body which has determined the purpose for processing the personal information. POPIA defines a ''responsible party'' as "a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information".[17] Apart from the 2013 Number Audit Submission Format, it is also not entirely clear from the Draft Regulations what information will be shared between ICASA and licensees, and who will ultimately be responsible for the data. The lack of clarity around the responsible party and the extent of data sharing creates complications for ensuring safety and accountability when it comes to securing the personal information of mobile users.

14. Moreover, the Draft Regulations' lack of reference to POPIA, and the lack of guidance on the eight conditions under which personal information may legally be gathered and processed is concerning. MMA reminds ICASA that these conditions must be met when processing personal information. Every requirement for the lawful processing of personal information, as detailed in POPIA, must be considered and their implementation should be detailed in the regulatory framework for numbering plans.

15. MMA submits that requiring personal information for purposes of mobile registration must be limited to what is strictly necessary for purposes of registration. Collecting unnecessary data raises concerns over the purpose and use of the registration information. Unless the use of the data can be demonstrated to help address the issues that mandatory SIM registration was introduced to address, it should not be collected. In this regard, consideration should be had to the principle of minimality included in section 10 of POPIA which provides that the processing of personal information should not be excessive.

16. MMA further reminds ICASA of the role of the Information Regulator. Section 39 of POPIA establishes the Information Regulator as an independent juristic person, accountable to the National Assembly. The Information Regulator has jurisdiction throughout the Republic[18] and is responsible for, among other things, promoting an understanding and acceptance of the conditions for the lawful processing of personal information and of the objects of those conditions. Notably, the Information Regulator is empowered to provide advice, upon request or on its own initiative, to a public or private body on their obligations under the provisions, and generally on any matter relating to the operation, of POPIA.

17. Moreover, MMA records that the importance of protecting personal information is gaining traction among various public bodies, particularly those seeking to employ digital or technical measures. For example, the Department of Home Affairs ("**DHA**") Draft Official Identity Management Policy explicitly records the DHA's commitment to comply with POPIA.[19] While some concerns have been raised with the Draft Official Identity

[16] Numbering Plan Regulations, 2017 at section 1.
[17] POPIA at section 1.
[18] Section 39(a) of POPIA.
[19] Department of Home Affairs, 'Official Identity Management Policy', (2020) (accessible at:

Management Policy, the inclusion of POPIA, and the role of the Information Regulator are important inclusions and signal an acceptance of the need to safeguard personal information and a commitment to respect, protect and promote the right to privacy. More recently, the Domestic Violence Amendment Act ("**DVA Act**") now includes specific references to the protection of personal information, POPIA, and the Information Regulator.[20] Notably, the DVA Act requires the Director-General to work in consultation with the Information Regulator to issue directives concerning the development of an integrated electronic repository for domestic violence protection orders.[21]

18. MMA welcomes the efforts of these public bodies and the recognition by the legislature to incorporate protections for personal information and implores ICASA to consider a similar approach.

19. **Accordingly, and given the importance of the right to privacy, and the need to ensure the safety and security of the personal information of mobile users, MMA recommends that ICASA urgently request advice from the Information Regulator on the Draft Regulations and halt any further developments of these regulations until such advice is received and considered.**

THE PURPOSE OF THE INCLUSION OF BIOMETRIC DATA

20. The Explanatory Note on the Draft Regulations states that "The hijacking of mobile numbers is a small but integral part of a wider form of fraud where sensitive data is diverted or comes under the control of criminal elements." The note goes on to state that the association of mobile numbers with the biometric data of a subscriber will assist to curb the hijacking of assigned subscriber mobile numbers." The Explanatory Note further records that "there are several jurisdictions that have linked mobile numbers with biometric data of subscribers thus this form of authentication is in practice and is a possible remedy to ensure that subscribers do not lose control of their assigned mobile numbers." MMA makes several submissions in response to these statements and the inclusion of section 6A(5) – (10).

21. MMA is concerned by the lack of data and evidence to support ICASA's position. The lack of reference to the data that informs this position curtails the ability of members of the public to fully understand the purpose of the inclusion of biometric data, which in turn hinders their ability to consent to the use of their biometric data.

22. MMA refers ICASA to a 2016 report of GSMA that states that there is no empirical evidence that mandatory SIM registration directly leads to a reduction in crime.[22] Privacy International notes concern with the lack of evidence to support the crime reduction reasons proffered by states introducing mandatory SIM card registration. This they argue calls into question the need and justification for such practices that may impede privacy

https://www.gov.za/sites/default/files/gcis_document/202101/44048gon1425.pdf).

[20] Domestic Violence Amendment Act 14 of 2021 at sections 2B and 6A.

[21] Ibid at section 6A.

[22] GSMA, 'Mandatory registration of prepaid SIM cards Addressing challenges through best practice' (April 2016) (accessible here: https://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf).

rights.[23] Privacy International further explains:

> "SIM registration has not been effective in curbing crime but instead has fueled it: states which have adopted SIM card registration have seen the growth of identity-related crime and have witnessed black markets quickly pop up to service those wishing to remain anonymous. Moreover, SIMs can be illicitly cloned, or criminals can use foreign SIMs on roaming mode, or internet and satellite telephones, to circumvent SIM registration requirements. In Pakistan, requiring SIM card registration resulted in the emergence of black markets for unregistered SIM cards, and a rise in identity fraud."[24]

23. Accordingly, and without providing access to such data, it is unclear to MMA what informed ICASA's assumptions about hijacking mobile numbers, and if these are reasonable inferences. On ICASA's own version, they have been presented with "concerns" and that "hijacking of mobile numbers is a **small** but integral part of a wider form of fraud". Given the potential privacy violations of the proposed inclusion, it is imperative that clearer guidance is given as to the purpose of the inclusion in order to understand whether it is reasonable and justifiable.

24. Moreover, ICASA's explanation that the association of mobile numbers with the biometric data of a subscriber "**will assist**" to curb the hijacking of assigned subscriber mobile numbers is similarly unsubstantiated save for a reference to jurisdictions that have adopted a similar approach. This will be addressed further below. MMA reiterates the need for ICASA to articulate the evidence to support this proposition. In the absence of viable evidence, it becomes difficult to understand any reasonable justification for the potential incursions on people's right to privacy.

25. **Accordingly, MMA urges ICASA to source reliable and accurate data on the extent of the hijacking of mobile numbers, make such evidence publicly accessible, and provide a clearer justification as to the purpose of the proposed inclusion.**

Lessons from other jurisdictions

26. MMA is concerned that the reference to other jurisdictions is misleading. According to reports, a recent study by the GSMA found that more than 150 nations require mobile phone customers to register for a pre-paid SIM card, however, only a handful of these countries require the registration to be linked to biometric data.[25] These countries include Bahrain, Bangladesh, China, Nigeria, Oman, Pakistan, Peru, Thailand, Singapore, Tajikistan, Tanzania, Thailand, Uganda, United Arab Emirates, and Venezuela.[26]

---

[23] Privacy International, 'SIM Card Registration' (accessible here: https://privacyinternational.org/learn/sim-card-registration).
[24] Ibid.
[25] P Bell, 'Liberty vs Security: The Battle Over SIM Registration' TeleGeography (28 May 2020) (accessible here: https://blog.telegeography.com/liberty-vs-security-the-battle-over-sim-registration).
[26] Ibid.

27. While there are jurisdictions that have adopted this approach, it is important to understand which jurisdictions have opted for this, their human rights framework, their data protection framework, and what concerns have arisen with regards to this approach. MMA lists some examples highlighting some of the concerns that have arisen in states where SIM registration is linked to biometric data.

    27.1. **Nigeria**: The Nigerian Communications Minister has issued a directive mandating citizens to link their mobile numbers to their identity numbers, or risk being blocked from accessing telecommunications services. Human rights activists have raised concern with this approach noting that the country's lack of adequate data protection laws leaves their personal information open to abuse.[27] It appears that Edo Civil Society Organizations (EDOCSO), a coalition of civil rights groups in Edo State has attempted to litigate the issue, arguing that the government's efforts to link biometrics-backed digital IDs to mobile SIM cards violate the right to privacy.[28]

    27.2. **Bangladesh**: The biometric registration program introduced in Bangladesh requires mobile phone operators to collect the fingerprints of every customer who owned a mobile SIM that is connected to their network. Authorities explained that the purpose of the biometric SIM registration was linked to crime prevention.[29] Some privacy concerns have been raised, as have concerns regarding the unintended consequence that the "policy will likely lead to a decrease in authorized mobile phone use and could generate an increase in unofficial sales of SIM cards."[30]

    27.3. **Venezuela**: In Venezuela, in order to buy a prepaid SIM card or take out a contract for mobile services, the telecommunications company selling the service must collect a copy of the individual's passport or identity card, take prints of the individual's right index finger and thumb, obtain a signature, and record the individual's address. Venezuelan law further requires the company to create an electronic registry containing this information about all its customers; the company must retain information about each customer for the period the customer receives the service and for three months after the customer terminates the service. In its Stakeholder Report for the Universal Periodic Review 26th Session on Venezuela, Privacy International noted that the—

[27] K Iruoma, 'Privacy concerns hobble Nigeria's digital ID push' Thomas Reuters Foundation News, (5 Augusts 2021) (accessible here: https://news.trust.org/item/20210805104557-zunak).
[28] A Macdonald, 'Nigeria's move to link digital identity numbers to SIM cards sparks lawsuit' Biometric Update (2 February 2021) (accessible here: https://www.biometricupdate.com/202102/nigerias-move-to-link-digital-identity-numbers-to-sim-cards-sparks-lawsuit).
[29] S Ahmed et al, 'Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh' (2017) (accessible here: https://www.researchgate.net/publication/316652373_Privacy_Security_and_Surveillance_in_the_Global_South_A_Study_of_Biometric_Mobile_SIM_Registration_in_Bangladesh).
[30] Z Rahman, 'Bangladesh Will Demand Biometric Data From All SIM Card Users' Global Voices (22 December 2015) (accessible here: https://advox.globalvoices.org/2015/12/22/bangladesh-will-demand-biometric-data-from-all-sim-card-users/).

> "compulsory SIM card registration and the retention of information about mobile phone users in a centralised database threaten the right to privacy in Venezuela card registration undermines the ability of users to communicate anonymously and disproportionately disadvantages the most marginalised groups in a society. It can have a discriminatory effect by excluding users from accessing mobile networks. It also facilities surveillance and makes tracking and monitoring of users easier for authorities, concerns that are especially acute in countries with conflict, political instability, and civil society suppression. Meanwhile, placing extensive mandatory data retention requirements on telephone companies contravenes international human rights standards; mandatory and indiscriminate retention of communications data is a serious interference with the right to privacy that goes beyond what is strictly necessary to respond to legitimate law enforcement needs."[31]

27.4. **Mexico**: On 25 April 2022, the Supreme Court of Justice of Mexico declared the National Register of Mobile Phone Users (PANAUT) unconstitutional.[32] This followed the approval of a decree for a new biometric mobile phone registry. The Court found that the registry would violate human rights and would not adequately safeguard sensitive data. "The national registry of mobile phone users is not a necessary measure in a democracy since it does not maintain a balance between the need for data in limited circumstances and the right to privacy," The Court further found that there is no direct relationship between the creation of the registry and the reduction of a crime.

28. MMA brings the above examples to ICASA's attention to highlight concerns that have arisen elsewhere and may be applicable in a South African context. MMA highlights the above to illustrate that not only has the link between crime prevention and biometric registration been found to be insufficient but that only a handful of countries have adopted this approach, (some in a concerning manner) illustrating that this is likely to be an invasive measure that may infringe on the privacy rights of people in South Africa without reason and justification.

29. **MMA submits that the purpose of the inclusion of biometric data must be reassessed and considered in line with our constitutional and international law obligations. To this end, MMA recommends that in addition to engagement and advice from the Information Regulator, ICASA must conduct a thorough assessment of the human rights implications of the proposed biometric registration. It is imperative that ICASA halt this regulatory reform process to ensure that it minimizes any unjustifiable limitations on constitutionally**

[31] Privacy International, 'Stakeholder Report for the Universal Periodic Review 26th Session on Venezuela' (accessible here: https://hrp.law.harvard.edu/wp-content/uploads/2016/04/venezuela_upr2016.pdf).

[32] Access Now, 'Mexico's president can prevent a privacy disaster: veto the new biometric mobile phone registry' (25 April 2022) (accessible here: https://www.accessnow.org/mexicos-new-biometric-mobile-phone-registry/).

protected rights, and to minimise any unintended consequences from the Draft regulations.

Less invasive approaches

30. In addition, on ICASA's own version, biometric registration is "**a possible remedy**", suggesting that there are other available remedies, many of which may be less restrictive. MMA acknowledges that ICASA seeks to maintain a registration process and acknowledges that there are interests relating to crime prevention that need to be addressed. However, MMA submits that those interests and considerations should be balanced against constitutionally protected rights.

31. MMA refers ICASA to some privacy-preserving approaches, which may not be directly applicable, but provide useful illustrations of alternative and less restrictive and invasive processes that can achieve similar registration based-outcomes:

    31.1. **Tokenization** enables unique identifiers for purposes of registration.[33] Tokenization substitutes a sensitive identifier such as ID number or biometric data with a non-sensitive equivalent such as a token that has no extrinsic or exploitable meaning or value. The World Bank explains that tokenization is not a new technology.[34] In credit and debit card systems, for example, tokenization has long been used to replace data on the card, with a unique randomly generated token that can be used to represent the card data in transactions but does not reveal the original card data. This means that the number of systems with access to the original card data is dramatically reduced, and with it, the risk of fraud should a system become compromised. Moreover, and as noted by the World Bank, tokenization can protect privacy by ensuring that only tokens, rather than a permanent identification number or other PII, are exposed or stored during a transaction.

    31.2. **Digital ID:** In Estonia, it is not mandatory to register user details when purchasing a SIM card. The country relies heavily on the use of digital identification, with each citizen issued with a digital ID that is used to access a wide range of e-services including health care, travel, banking, taxation, motoring, and even voting.[35] Notably, Estonia ranks second in Freedom House's freedom on the net as a country where Internet freedom continues to thrive with high rates of access, privacy, and expression.[36]

    31.3. **KYC processes**: In a financial services context, the Know Your Customer (KYC) process is a process that requires organisations, to varying degrees, to verify a client's identity when opening an account and periodically over time. In other

[33] GSMA, '10 Principles for good ID: A 2021 refresh' (4 March 2021) (accessible here: https://www.gsma.com/mobilefordevelopment/blog/10-principles-for-good-id-a-2021-refresh/).
[34] World Bank, 'Tokenization' (accessible here: https://id4d.worldbank.org/guide/tokenization).
[35] Bell above n 25.
[36] Freedom House, 'Estonia: Freedom on the Net' (2021) (accessible here: https://freedomhouse.org/country/estonia/freedom-net/2021).

words, banks must ensure their clients are genuinely who they claim to be.[37] GSMA notes that the KYC process, can a be useful risk-based approach, and can, provided appropriate data protection frameworks are in place, preserve the privacy rights of mobile users.[38]

32. **MMA implores ICASA to consider various privacy-preserving approaches, which will likely require input from the Information Regulator.**

33. A final point relates to timing. Law and regulatory reform processes in relation to digital IDs and the Regulation of Interception of Communications and Provision of Communication Related Information Act are underway and may have a bearing on mobile registration processes, this is something ICASA should consider.

34. **Accordingly, and in line with alternative options, timing considerations, and the importance of the right to privacy, MMA suggests that ICASA consider the various processes underway, and engage with relevant stakeholders to better coordinate processes.**

CONCLUSION

35. MMA reiterates its appreciation for the opportunity to provide this submission and would welcome the opportunity to make oral submissions should the need arise. MMA submits that it has genuine concerns with the current Draft Regulations and recommends that the implementation of these regulations be halted pending engagements with the Information Regulator and the conclusion of a human rights impact assessment on the proposed biometric registration. Further, MMA recommends that ICASA consider alternative and less invasive means to enable access to mobile services. It is clear that there is much work that still needs to be done to ensure a rights-based and privacy-preserving approach. MMA stresses that these are important issues that must be dealt with as a matter of urgency and urges ICASA to prioritise engagements with the Information Regulator. MMA remains willing and available to provide any further information that may be of assistance to ICASA and would welcome an opportunity to make an oral submission if the opportunity is available.

MEDIA MONITORING AFRICA
11 MAY 2022

[37] GSMA above n 22.
[38] Ibid.