Photo: Aida Namukose
Graphic design: Wilna Combrinck

POLICY BRIEF

SMART ID CARDS IN MAURITIUS

Balancing rights and freedoms with national identification needs

SARAH CHIUMBU & CHRISTINA CHAN-MEETOO, JULY 2024

INTEL WATCH

ABOUT THE AUTHORS

Sarah Chiumbu is Associate Professor in the Department of Communication and Media at the University of Johannesburg, South Africa.

Christina Chan-Meetoo is Senior Lecturer in Media and Communication at the University of Mauritius, where she is also the head of the Mediacom Studio.

ABOUT OUR FUNDERS

This brief is an output of an eight-country surveillance research project titled: *Public Oversight of Digital Surveillance for Intelligence Purposes: A Comparative Case Study Analysis of Oversight Practices in Southern Africa*. This research project is supported by the British Academy's Global Professorship Programme (grant no. GP/400069), through the School of Social and Political Sciences at the University of Glasgow.

TABLE OF CONTENTS

SUMMARY

- The Mauritius Cabinet has promulgated three Regulatory instruments to introduce new government identification measures and features (including a Mobile ID in the National Identity Card System). These instruments include the National Identity Card Regulations 2024, the National Identity Card (Card Usage) Regulations 2024, and the National Identity Card (Mobile ID) Regulations 2024.
- In the new ID card system, the smart ID will be linked to a mobile application to serve as an extension of the ID card, allowing online transactions to be made even without the physical card and introducing the option to use an electronic version of the ID Card (Mobile ID) stored in a mobile app (digital wallet) that can be downloaded onto a smart mobile device, replacing the traditional ID Card. A first phase of the new smart ID was launched on 26 February 2024 with only the physical version, while the second phase will concern the digital version.
- This Policy Brief argues that the proposed integration of mobile ID with the current Smart ID should continue to balance the legitimate objectives of effective identification systems and the preservation of individual rights and freedoms.
- The mobile ID system should be in line with the requirements of the Data Protection Act (2017).
- The introduction of the mobile ID system should pass the proportionality test to ensure that only necessary and sufficient characteristics be linked with the biometric sample, and the subject must have adequate control over how his/her data is processed.
- It is noted that Government has announced the decision "that security audits of the MNIC 3.0 system be conducted by an independent body to ensure compliance with safety and confidential parameters" in line with the commitment to the UN Human Rights Committee. This is a welcome measure, which warrants more public dissemination for enhanced citizen literacy with respect to the ID card system.
- Appropriate measures should be taken so that the new mobile ID system cannot be used as a tool for unlawful surveillance. The provisions of section 44 of the Data Protection Act (DPA), which allow the Prime Minister to apply exemptions to the application of the DPA's guarantees for the privacy of personal data for the purpose of safeguarding national security, defence or public security, would benefit from more explication of such exemptions. These should be only possible in very exceptional circumstances and there should be safeguards against any misuse or abuse by any agent, whether the latter is part of the State or acts as an approved third party.
- It is recommended that the government examine case studies from other nations that have used mobile ID card systems. Along with national consultations, the in-depth analysis of these case studies should produce practical guidelines related to different aspects such as technical implementation, security of data, and frameworks to deal with emerging regulatory and ethical issues related to Mobile IDs that may not be adequately covered by the current laws.
- Specific safeguards should include obligations by any app or device developer or vendor to provide full control to citizens over their personal data and how such data is used in any circumstance. This includes a commitment to minimise data sharing, duration of storage (only if absolutely necessary and only for initial registration purposes) and limitations on permissions to access data (only for approved government agencies and/or entities strictly vetted by government).
- The same restrictions which have been applied for the ID card following the Supreme Court judgements and the UN Human Rights Committee should also be in place for the mobile version of the card, whereby data is stored solely on the citizen's device and not on any central database. Any data which is temporarily stored by an entity other than the citizen should be only on a one-time temporary basis.
- Whilst vendors may in effect argue in favour of centralising data storage by advocating ease of use and minimal effort, Government needs to be cautious about arguments used by vendors so as not to allow the occurrence of a breach of existing commitments to protect citizens' sensitive data.
- We note that Government has stated that the mobile version of the ID card is not mandatory and it is hoped that this will remain only an alternative, albeit a welcome addition to the MNIC for citizens who wish to embrace a fully digital life. However, one should be cautious that the mobile version does not replace the physical one altogether in the long run so as not to penalise citizens who may not have or cannot afford continuous and unlimited Internet access.
- Maintaining a balance between individual rights and technological advancement necessitates constant discussion, strong legal frameworks, and a commitment to ethical principles.

INTRODUCTION

In 2024, Mauritius intends to introduce a new Mobile ID into the current national Smart ID card system. Mobile ID, or mobile identification, refers to the use of mobile devices such as smartphones or tablets for personal identification purposes. It includes digital records of a user's personal information and can be used as a valid form of identity both in-person and online. Modern ID systems may be required in today's digital environment for tasks like identity authentication, document verification, and public service management. Global corporations like Apple and Google already use biometrics (voice, face, and fingerprint) and personal data in their digital wallets. Biometric features are also rapidly being incorporated into government-backed projects such as payment systems, identity cards and e-passports across the world and in Africa[1], and Mauritius is no different. Given this trend, it is necessary to ensure that such systems have effective safeguards to protect citizens' data and privacy. Until now, it appears that Mauritius provides a unique case for respecting citizens' rights which has not been found in most countries on the African continent, thanks both to public debates, judicial cases at the local and at the international levels, and a commendable stance by Government to comply with UNHRC advice on the matter. It is hoped that the country can stay on the same path and potentially provide a model for tackling this complex and sensitive issue through regular democratic dialogues.

More specifically, this Policy Brief examines the planned integration of mobile ID with the current Smart ID. It argues that the revised ID card system should balance the legitimate objectives of effective identification systems and the preservation of individual rights and freedoms. In particular, the mobile ID system should be in line with the requirements of the Data Protection Act (2017) which, similar to the General Data Protection Regulation (EU GDPR), recognises sensitive personal data as special categories of data. These categories of data include genetic or biometric data that is uniquely identifying.

SMART IDS: HISTORY AND CONTEXT

Since 1985, the National Identity Card Act required every citizen of Mauritius to apply for an identity card within six months of attaining the age of 18. The Finance (Miscellaneous Provisions) Act 2009 and the National Identity Card (Miscellaneous Provisions) Act 2013 (NIC Act) introduced a new biometric identity card scheme. The Mauritius National Identity Scheme (MNIS) replaced the then laminated national identity card with a new smart biometric card. The MNIS allowed citizens' biometric information (fingerprints and a high-resolution facial image) to be taken and recorded for the purposes of the identity card (Baichoo et al., 2018). In addition, Section 3 of the NIC Act provided for the Registrar of Civil Status to keep a central database containing all personal information stored in the database situated at the Government Online Centre. There was a public outcry over the new Smart ID from civil society organisations and opposition parties. This led to constitutional challenges before the Supreme Court in 2015, one by a private citizen named Maharajah Madhewoo and another by then Opposition Leader Pravind Kumar Jugnauth. The first case questioned the constitutionality of the government collecting fingerprints for the ID card, and the second the storage of fingerprints on a central government database. Madhewoo also contested the constitutionality of the law before the Judicial Committee of the Privy Council, especially in relation to the breach of an individual's constitutional right to privacy. The judgment of *Madhewoo v. the State* [2015] rejected the claim that it was illegal for the government to gather fingerprints to create the new ID cards but held that it was unconstitutional for it to store and retain biometric fingerprint data in one database (Duncan, 2019; Murday, 2023).[2] The same conclusion was reached in Jugnauth's case at the Supreme Court. The Supreme Court's conclusions were seconded by the Privy Council in October 2016 (Baichoo et al., 2018).

1 The World Bank programme ID4D has been supporting 32 African countries for the implementation of digital ID and payment ecosystems according to the 2021 Annual Report accessible at: https://id4d.worldbank.org/about-us

2 Madhewoo v The State of Mauritius and another (Mauritius). Retrieved at https://vlex.co.uk/vid/madhewoo-v-the-state-807431825

Following the Supreme Court's ruling, the government released the National Identity Card (Civil Identity Register) Regulations 2015, which limited the storage of pertinent data to the identity card itself, rather than a central register. According to cabinet papers, the Singapore Corporation Enterprise was tasked by government with the removal of all fingerprint images and minutiae from the Mauritius National Identity Central Database, as well as from all backup tapes. As a result, fingerprint minutiae[3] are taken only for the purpose of issuing identity cards, after which they are deleted and they remain only on the cards in possession of the citizens.

In 2017, the Government re-amended the NIC Act through the Finance Act 2017 to promote the use of the verification functionality of the card using Secure Access Module (SAM) card readers without copying and storing of the data found on the card. This means that the use of the card for identification would only be possible in the presence of the citizen, whereby his/her fingerprint would be compared with the minutiae stored on his/her card. The new process would thus be different from the previous one which required a central database. It should be noted however that no entities have yet been authorised to use card readers for identification to date.

Additionally, to enhance data subjects' control and personal autonomy over their personal information, the Data Protection Act of 2004 was repealed and replaced by the Data Protection Act of 2017. The right to privacy in Mauritius is constitutionally entrenched and citizens have a right to expect that right to be upheld. However, the 2004 Data Protection Act was not suitable for storing and protecting biometric data, and it was promulgated before the adoption of biometric technologies in the country. The Data Protection Act 2017 thus caters for these shortcomings.

Madhewoo, who had challenged the ID card system in the Supreme Court, turned to the UN Human Rights Committee in December 2017 to contest the collection and retention of biometric data on ID cards, arguing that this violates his right to privacy. He maintained that if the smart identity card was misplaced or stolen, fingerprint data might be transferred onto forged cards and that the assignation of the responsibility for storage of the biometric data to citizens constituted a security weakness. On 24 March 2021, the United Nations Human Rights Committee (HRC) found that the current identity card scheme was in violation of citizens' privacy rights under Article 17 of the International Covenant on Civil and Political Rights (ICCPR). The Committee called on the Mauritian government to review the justifications for retaining fingerprint data on identity cards, consider the current data security concern, and provide Madhewoo a workable solution.[4]

Unfortunately, no update on the reply of the Mauritian government nor on the actions taken could be found online, neither on the website of the UN Human Rights Committee, nor on the government's website, nor on any local or international media which did not do any follow up on the issue. It is only recently that a small online local media outlet reported indirectly on the matter while presenting the latest developments related to the national ID card in February 2024[5]. In that article, it was mentioned that Government has announced the decision "that security audits of the MNIC 3.0 system be conducted by an independent body to ensure compliance with safety and confidential parameters" in line with the commitment to the UN Human Rights Committee. This is an undoubtedly a welcome measure, which warrants more public dissemination for enhanced citizen literacy with respect to the ID card system.

3 Fingerprint minutiae are defined in the legislation as "the characteristics of a fingerprint image such as the ridge endings and ridge bifurcations".

4 United Nations Human Rights Office of the High Commissioner (2021) Mauritius: Storing biometric data on identity cards violates privacy – UN Human Rights Committee, Retrieved at https://www.ohchr.org/en/press-releases/2021/07/mauritius-storing-biometric-data-identity-cards-violates-privacy-un-human?LangID=E&NewsID=27329, accessed 5 December 2023

5 https://english.lematinal.media/pm-launched-the-new-identity-card-yesterday-morning/

TIMELINE OF CABINET DECISIONS RELATED TO THE SMART ID

Year	Decision
21 April 2000	Cabinet has agreed to the National Identity Card Act being amended to provide for the issue of new Identity Cards based on Smart Card technology.
26 September 2008	Cabinet has taken note of developments in the implementation of the Smart Card Based Electronic Identification System, commonly referred to as National Identity Cards
21 November 2008	Cabinet has agreed to the setting up of an Inter-Ministerial Committee chaired by the Prime Minister to spearhead the Mauritius National Identity Card Project. The new national ID card would contain, in visual and electronic format, all existing information on the current ID card, as well as new features to combat identity fraud.
26 November 2010	Cabinet has taken note of the status in the implementation of the Mauritius National Identity Card Project. The Mauritius National Identity Card, also known as Smart Card, would provide secure electronic identification and allow the capture of biometric data, thus fencing off any possibility of counterfeiting, tampering or duplicating the cards.
29 July 2011	Cabinet has taken note of the status in the implementation of the Mauritius National Identity Card Project with the collaboration of the Government of Singapore. The Identity Card would be a multi-usage card using the SMART Card Technology. The first ID Card is expected to be issued by early July 2012.
06 July 2012	Cabinet has taken note of the status in the implementation of the Mauritius National Identity Card Project with the assistance of the Government of Singapore. The Singaporean authorities would not only deliver a state-of-the-art identity card with world-class biometric and identity management technology and systems, but also allow Government to improve its services through the Mauritius National Identity Scheme, and benefit from the expertise of world class experts in the fields of e-Government and national security.
14 September 2012	Cabinet has taken note of the status in the implementation of the Mauritius National Identity Card Project under a Government-to-Government configuration with the Government of Singapore. The Singapore Cooperation Enterprise, a government entity, would lead the Project. The Mauritius National Identity Card, a polycarbonate contactless smart card, will comprise secure data, such as civil data, photo, address and fingerprint, stored electronically in the card chip in an irreversible laser engraved format. It is expected that the implementation of the Project would be completed by December 2014.
26 April 2013	Cabinet has taken note of the status in the implementation of the new smart National Identity Card Project. The new Identity Card would be a polycarbonate plastic card with laser-engraved information, such as the name of the holder, ID number, gender, date of birth, date of issue, photograph, signature, and bar code. The Card would also feature a contactless electronic chip which would securely store civil status data, a photograph, address and fingerprint, as well as encoded data, and would have security features to avoid tampering. The issuing of the ID Cards would start in October 2013 and be completed in 2014.
21 June 2013	Cabinet has taken note of progress in the implementation of the Mauritius National Identity Scheme Project. The issue of the new Smart National Identity Card is scheduled from 1 October 2013 and would be completed by December 2014. The Card would contain a printed photograph of the holder, and visible fields, such as name, gender, date of birth, ID number and signature. The chip would contain an encoded photo, civil data, fingerprints and the residential address.
5 July 2013	Cabinet has agreed to the introduction of the National Identity Card (Miscellaneous Provisions) Bill in the National Assembly. The object of the Bill is to make better provisions in relation to matters pertaining to national identity cards.
5 June 2015	Cabinet has taken note of the Judgments of the Supreme Court with respect to the Mauritius National Identity Card (MNIC) Project, and of measures being taken to destroy the databank containing fingerprints and biometric photographs of the new Identity Card to protect sensitive personal data of citizens as announced in Government Programme 2015-2019. The ID Card system is being reviewed to remove the biometric data, including photographs, fingerprint images, and fingerprint minutiae.
21 August 2015	Cabinet has taken note that, following the judgment of the Supreme Court, all biometric data would be deleted from the Mauritius National Identity Card Database and the system would be reviewed and upgraded. Accordingly, the Singaporean team would proceed with the deletion of the data from 24 August to 11 September 2015, and all Identity Card Centres would be temporarily closed. No registration, replacement or issuance of cards would take place during that period.
4 September 2015	Cabinet has taken note that the Singapore Cooperation Enterprise has completed the removal of fingerprint images and minutiae from the Mauritius National Identity Card Database. The backup tapes are also being destroyed. The exercise is being carried out in the presence of a Chief Usher of the Supreme Court. Cabinet has agreed to the extension of the validity period of the old National Identity Card to 31 January 2016, and to the new arrangements being put in place for the registration of new Identity Cards. The issuance of the Identity Card would resume on 14 September 2015.
22 November 2019	Cabinet has taken note of the implementation of innovative digital Government projects in the Ministry of Technology, Communication and Innovation (including the Mobile ID, which would allow citizens to authenticate themselves using their smart phones and, inter alia, promote the uptake of e-services/m-services by providing an electronic digital identity to citizens).

19 February 2021	Cabinet has agreed to the revamping of the Mauritius National Identity Card System (MNIC), as the existing hardware and software of the whole system have reached their end-of-support and end-of-life. The current MNIC would be revamped by state-of-the-art technology with enhanced security features which may be used to provide a wider spectrum of customised e-services.
23 April 2021	Cabinet has taken note of the outcome of the first Steering Committee meeting in the context of the revamping of the Mauritius National Identity Card System (chaired by the Minister of Information Technology, Communication and Innovation).
24 February 2023	Cabinet has taken note of the deployment of an electronic "Know Your Customer" (KYC) feature within the National Authentication Framework (MauPass) by the Ministry of Information Technology, Communication and Innovation. The deployment of an electronic KYC feature would allow the two-factor authentication process to be conducted online through the verification of a live selfie of a citizen against their facial photograph on their National Identity Card or Passport. This will enhance access to the MauPass platform, and facilitate Mauritian nationals abroad (willing to activate their account remotely) to have access to Government e-services and the MoKloud platform.
2 February 2024	Cabinet has agreed to the promulgation of the National Identity Card Regulations 2024, the National Identity Card (Card Usage) Regulations 2024, and the National Identity Card (Mobile ID) Regulations 2024. The Regulations provide for, inter alia: (a) new measures and features in the new National Identity Card System; (b) the required legal framework to enable the use of electronic devices and appropriate software, as prescribed in the schedules, for the electronic reading of data on the ID Card and from the Mobile ID; and (c) the use of the electronic version of the ID Card (Mobile ID) stored in a mobile app (digital wallet) which could be downloaded on a smart mobile device, instead of using the conventional ID Card.

Photo: Aida Namukose

THE NEW AMENDMENTS

The latest amendment of the National ID Act is detailed in Section C.37 of t*he Budget Measure: Explanatory Notes (main provisions to be included in The Finance (Miscellaneous Provisions) Bill 2023)6.* Section C.37 (b) caters for "the introduction of Mobile ID which will be a new feature in the new Mauritius National Identity Card system". On 2 February 2024, Cabinet agreed to the promulgation of three Regulatory instruments: the National Identity Card Regulations 2024, the National Identity Card (Card Usage) Regulations 2024 and the National Identity Card (Mobile ID) Regulations 2024. The regulations include:

(a) Implementing new measures and features in the updated National Identity Card System;

(b) Establishing the necessary legal framework to allow the use of electronic devices and specific software, as outlined in the schedules, for reading data on the ID Card and Mobile ID.

(c) Introducing the option to use an electronic version of the ID Card (Mobile ID) stored in a mobile app (digital wallet) that can be downloaded onto a smart mobile device, as an alternative to the traditional ID Card.[7]

The following are some of the amendments proposed for the new ID card:

- The smart ID will be linked to a mobile application to serve as an extension of the ID card, allowing online transactions to be made even without the physical card.
- Fingerprint minutiae will still be in place for the new card, with temporary storage of data by the issuing authority, such that these will be kept only on the identity card.
- The new ID card will need to include options to use it for other purposes, such as a travel document, driver's license, health card, etc. The choice of options that will be included in the new card will be determined by the Prime Minister's Office.
- People's mobile NFC module will be able to interact to perform a fully digital verification, without the physical ID card. The State has already developed a national authentication framework with MauPass, a two-factor verification method[8]. MauPass has been developed as a single window of authentication service to provide a layered approach towards e-Authentication implementation for all Government and other e-services.[9]

POTENTIAL CONCERNS WITH THE SECOND PHASE OF THE NEW ID CARD

Upon its introduction over ten years ago, the current ID card was referred to as a "one-stop solution". It needed to interact digitally with numerous other government services, hold medical data, and scan drivers' licenses. However, the 2015 Supreme Court judgment prohibited the storage and retention of fingerprints and other biometric data by the State. As a result, the current identity card has almost no digital function. Even though the Mobile ID will have temporary storage of data that will be kept only on the identity card, the introduction of 'Digital Remote ID proofing' raises the possibility that citizens' biometric data may be stored somewhere, which would be in breach of the judgments of the Supreme Court of Mauritius and that of the United Nations Human Rights Committee. This would therefore reintroduce the very problem at the centre of contention in 2015, brought about by the introduction of the Smart ID card.

6 https://www.edbmauritius.org/budget2023/Annex_Budget_2023-2024.pdf

7 Source: Mauritius Cabinet Papers. Retrieved at https://pmo.govmu.org/CabinetDecision/2024/FINAL_Highlights%20of%20Cabinet%20Meeting%20-%20%20Friday%2002%20February%2024_1%20(1).pdf

8 Florian Lepoigneur (2023) New ID card: how about a selfie? LeExpress.mu/ Retrieved at https://lexpress.mu/article/424050/nouvelle-carte-didentite-un-selfie-ca-vous-dit

9 MAUPASS: one place to transact with government. Retrieved at https://oecd-opsi.org/innovations/maupass/

Need to balance the legitimate objectives of identification systems and the preservation of individual rights and freedoms

As the government plans to introduce the second phase of the amended smart ID card with the mobile ID functionality, it is imperative that the judgements from the 2015 Supreme Court and the United Nations Human Rights Committee are respected. Notably, following the launch of the first phase of the new ID card in February 2024, the media reported[10] the Prime Minister stating that "security audits of the MNIC 3.0 system be conducted by an independent body to ensure compliance with safety and confidential parameters" in line with a commitment made to the United Nations Human Rights Committee. Such independent security audits are crucial to ensure that the processes for safeguarding of sensitive data are well established as the use of mobile ID systems brings up several human rights issues that require careful consideration and attention, as detailed below. It is also noted that no mass conversion of the existing 2013 identity card is envisaged[11] and that the two cards will continue to co-exist for the time being as the validity of the previous card has been extended by another 10 years.

The following are some significant human rights issues related to a mobile ID system. These issues must be considered when introducing the digital or mobile version of the national identity card:

- **Balancing utility with privacy**

The new card features a chip that stores electronic data. Card readers will allow institutions like banks and government agencies access to this data. To protect the individual's right to data protection and privacy, it is essential to ensure the security and confidentiality of the collected information. In the world of biometrics, there is a need to ask how we can extract valuable insights from biometric sensitive data while ensuring individual privacy.

- **Proportionality**

As one of the principles of data privacy, proportionality refers to the notion that any data collected should be limited to the smallest amount of data required to fulfill a certain service (Bygrave, 2014). The concept of proportionality in this case establishes the limit to which centralised storage can reasonably override an individual's right to privacy. To maintain proportionality, only necessary and sufficient characteristics must be linked with the biometric sample, and the subject must have adequate control over how his/her data is processed. In the 2015 Smart ID Supreme Court judgement, it was found that the interference resulting from the biometric data collection process for the Smart ID card was proportionate to the public interest (given the goal of safeguarding the public from identity theft). However, it was determined that the MNIC Central Database's indefinite retention and storage of personal biometric data violated citizens' right to privacy, since it was not a reasonable means of achieving the goal of preventing identity theft in a democratic society. This led to the subsequent deletion of the central database. The proportionality test should similarly be passed in the introduction of mobile IDs (should the upgraded system include the possibility of the indefinite storing of sensitive personal data elsewhere than in the citizen's card or personal device being used for identification).

- **Freedom from Unlawful Surveillance**

The new mobile ID system should not be used as a tool for unlawful surveillance. Fear of digital surveillance in Mauritius emerged strongly when the Mauritian Safe City Project (MSCP) was introduced in 2017 leading to the mounting of 4000 cameras across the island. The main players in the MSCP are the Mauritius Police Force (MPF), the national telecommunications operator Mauritius Telecom, and the commercial supplier Huawei—and the responsibility of each does not seem very clear. The success of any Safe City project depends on how data is used and for what purpose. Kasenally (2022) argues that although Mauritius has one of the best data protection laws in Africa as well as a Data Protection Office, section 44 of the DPA (2017) stipulates: "Personal data shall be exempt from any provision of this Act

10 See: https://english.lematinal.media/pm-launched-the-new-identity-card-yesterday-morning/
11 See: https://lexpress.mu/s/les-nouvelles-cartes-didentite-emises-la-semaine-prochaine-531797

where the non-application of such provision would, in the opinion of the Prime Minister, be required for the purpose of safeguarding national security, defence or public security". This clause allows the Prime Minister to reverse the Act's guarantees for the privacy of personal data. According to the Code of Practice for the Operation of the Safe City System(s)[12], this clause applies to MSCP data. There is thus fear of the potential for abuse, misuse, and manipulation of this data. This is because the Supreme Court cases on the biometric ID only dealt with the fingerprints being stored in a central database by the government for the purpose of the National Identity Card but did not focus on the capturing and storage of biometric photos of people when they apply for the card. Following the Supreme Court ruling in 2015, the government destroyed the database for fingerprint images and minutiae, but, according to a media report, they continued to collect biometric photos for the card[13]. The integration of a mobile ID system with the Smart ID card could in essence require the leveraging of biometric data such as fingerprints or facial recognition for enhanced security and biometric authentication.

While no mention of any integration of the MSCP with the MNIS is made in the different documents which are publicly available, when it comes to the deployment and management of mobile identity systems, transparency and accountability are essential. People have the right to be informed about how their data is being used and to hold government and other organisations responsible for any misuse. At present, the various official statements and documents lack clarity on the roles and responsibilities entrusted to the different entities which may have access to sensitive personal data. Integrating mobile ID and smart ID systems may provide such entities, including government agents and other assigned intermediaries, with enhanced power for surveillance. This could be misused to monitor individuals without proper justification or oversight. Mobile devices frequently come with built-in location tracking capabilities. Integrating this information with smart identity systems may result in unlawful tracking or stalking, whether sanctioned or not by the State and courts of justice. The possibility of data interception exists as well. There is a risk that data sent between mobile devices and smart ID systems could be intercepted during the integration process, opening the door to unauthorized access.

12 Available on: https://dataprotection.govmu.org/Documents/Code%20of%20Practice%20for%20the%20operation%20of%20the%20Safe%20City%20System%28s%29%20by%20MPF.PDF

13 Iqbal Ahmed Khan (2021) From biometric ID cards to Safe City cameras, how our civil liberties are impacted. https://lexpress.mu/node/387343/1000

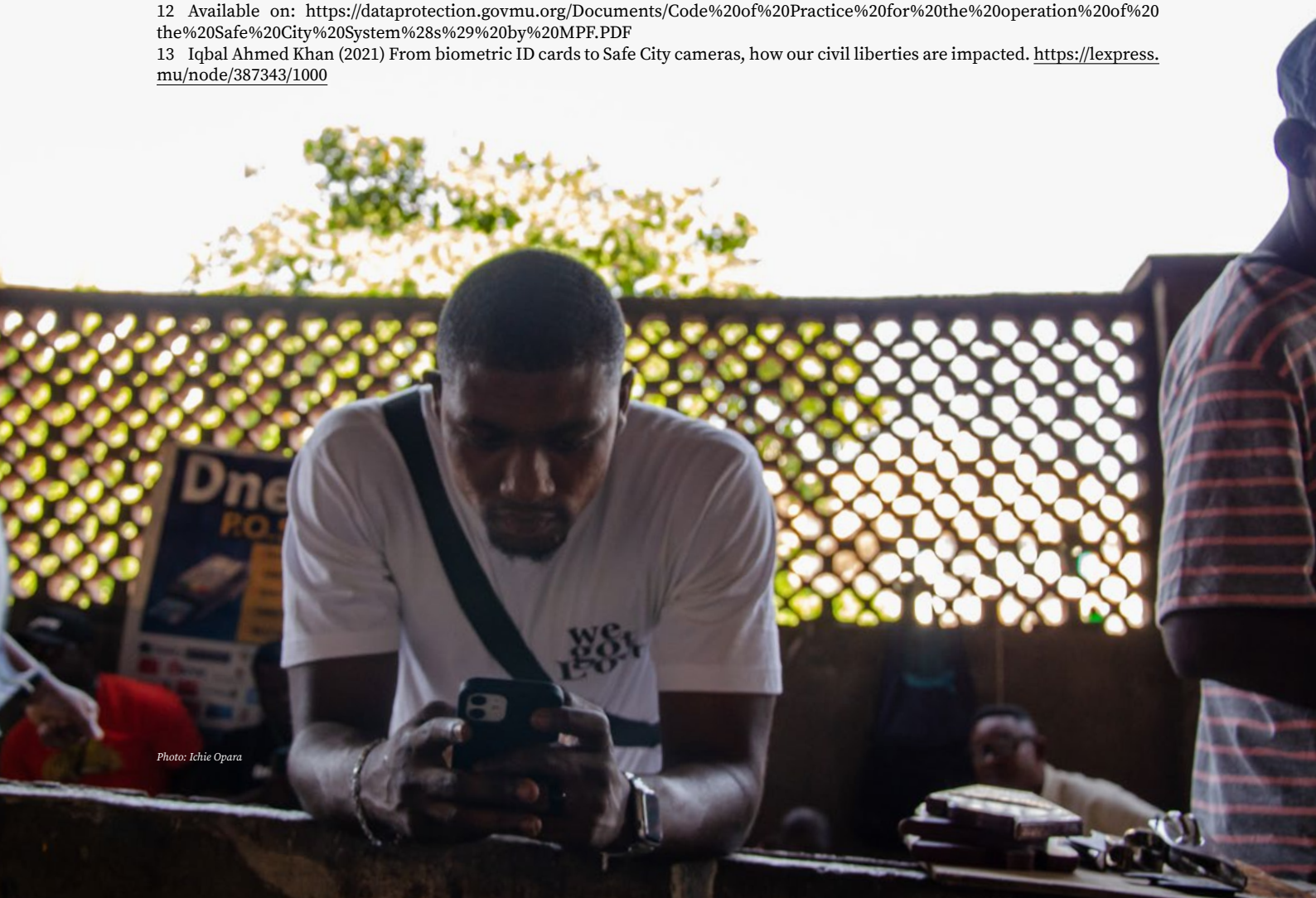

Photo: Ichie Opara

RECOMMENDATIONS

It is recommended that the government examine case studies from other nations that have used mobile ID card systems. Along with national consultations, the in-depth analysis of these case studies should produce practical guidelines related to different aspects such as:

- Technical implementation and maintenance: Proper rules and procedures should be put in place to outline under what conditions developers and implementors of any biometric technologies should access citizens' data. For instance:
  - There should be specific obligations by any app or device developer or vendor to provide full control to citizens over their personal data and how such data is used in any circumstances. Developer code should be open to scrutiny by the independent auditor to ensure that this is fully complied with. Ideally, code should in fact be made fully open and transparent for all users to inspect if they wish to do so.
  - Obligations should include a commitment to minimise data sharing, duration of storage (if absolutely needed and only for initial registration purposes) and limitations on permissions to access data only for approved government agencies and/or entities strictly vetted by government.
  - The same restrictions which have been applied for the ID card following the Supreme Court judgements and the UN Human Rights Committee should also be in place for the mobile version of the card, whereby data is stored solely on the citizen's device and not on any central database. Any data which is temporarily stored by an entity other than the citizen should be only on a one-time temporary basis.
  - Technology vendors often use technical arguments to push for ready-made or easier-to-implement solutions, or solutions with which they are familiar. For instance, they may in effect argue in favour of centralising data storage by advocating ease of use and minimal effort. Governments need to be cautious about such technical arguments used by vendors and should not simply settle for solutions actively promoted by vendors and developers without questioning their merits. These solutions should serve the public good rather than the vendor's profit motive. In this case, the Government of Mauritius should be cautious in its negotiations with technology companies in the development and implementation of the new phases of the national ID system so as not to allow the occurrence of a breach of existing commitments to protect citizens' sensitive data.
- Transparency and communication: Processes in all agencies which are supposed to use any biometric system to improve service to the public should be consolidated and clearly communicated to ensure that they adhere to data protection rules and procedures.
- Security of system and of data: Clearly stringent security measures must be implemented to reduce the risks associated with managing biometric data. Robust access controls, advanced encryption techniques, and safe storage options serve as the cornerstones of data protection strategies. While these may exist, there is insufficient communication about them and the need to enforce such processes for more security. Clear domestic guidelines should be developed and publicly disseminated to prevent unregulated access, sharing, and copying of data, as well as data breaches.
- Ethical considerations: When handling biometric data, ethical factors need to be considered in addition to legal compliance. Although Mauritius has one of the best data protection laws in Africa, it is still important to pay attention to regulatory and ethical issues that may not be covered by the current laws (for example new types of usage of data under the mobile ID system). Collaboration between governments, technology companies, civil society organisations, and academic experts is necessary to develop strong ethical frameworks for mobile IDs.

On a final note, the Government has stated that the mobile version of the ID card is only an additional alternative to the physical ID card and is thus not mandatory. It is hoped that this will indeed remain only an alternative, albeit a welcome addition to the MNIC for citizens who wish to embrace a fully digital life. One should be cautious that the mobile version does not replace the physical one altogether in the long run so as not to penalise citizens who may not have or cannot afford continuous and unlimited Internet access. This may appear conservative, but it is in fact a necessary approach in order not to further widen the digital gap and also to maintain viable options in case of breakdowns or slowing down or even digital deserts which do exist or may exist in our communication systems.

REFERENCES

Baichoo, S. et al. (2018) Legal and ethical considerations of biometric identity card: Case for Mauritius, *Computer Law & Security Review: The International Journal of Technology Law and Practice*, https://doi.org/10.1016/j.clsr.2018.08.010

Bygrave, L. A (2014) 'Core Principles of Data Privacy Law', Data Privacy Law: An International Perspective (Oxford, 2014; online edn, Oxford Academic, 16 Apr. 2014), https://doi.org/10.1093/acprof:oso/9780199675555.003.0005, accessed 12 Jan. 2024

Duncan, J. (2019) Activist Learning and State Dataveillance: Lessons from the UK, Mauritius and South Africa. In Aziz Choudry (ed) *Activists and the Surveillance State Learning from Repression*. Pluto Press

Kasenally, R. (2022) The Trappings of the Mauritius Safe City Project. The Hoover Institution. Retrieved at https://www.scribd.com/document/552653455/The-Trappings-of-the-Mauritius-Safe-City-Project#, accessed on 12 December 2023

Moriarty, B. et al. (2022). Utility-Preserving Biometric Information Anonymization. In: Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W. (eds) *Computer Security – ESORICS 2022. ESORICS 2022. Lecture Notes in Computer Science*, vol 13555. Springer, Cham.

Murday, L. (2023) Mauritius: Moving towards Mass Surveillance. In Ryan Shaffer (ed) *The Handbook of African Intelligence Cultures*. Lanham, Boulder, New York & London: Rowan & Littlefield

Swales L. (2021*) The Protection of Personal Information Act and data de-identification*. *S Afr J Sci*. 2021;117(7/8)