United Nations CCPR/C/131/D/3163/2018

International Covenant on Civil and Political Rights

Distr.: General
21 July 2021
Original: English

Advance unedited version

Human Rights Committee

Views adopted by the Committee under the Optional Protocol, concerning communication No. 3163/2018*,**,***

Communication submitted by:	Maharajah Madhewoo (represented by counsels, Pete Weatherby, Erickson Mooneapillay and Sanjeev Teeluckdharry)
Alleged victim:	The author
State party:	Mauritius
Date of communication:	15 December 2017 (initial submission)
Document references:	Decision taken pursuant to rule 92, transmitted to the State party on 26 March 2018 (not issued in document form)
Date of adoption of Views:	24 March 2021
Subject matter:	collection and retention of biometric data on identity cards
Procedural issue:	victim status
Substantive issue:	privacy
Article of the Covenant:	17
Article of the Optional Protocol:	1

* Adopted by the Committee at its 131st session (1–26 March 2021).

** The following members of the Committee participated in the examination of the communication: Tania Abdo Rocholl, Wafaa Ashraf Moharram Bassim, Yadh Ben Achour, Arif Bulkan, Mahjoub El Haiba, Shuichi Furuya, Marcia V.J Kran, Kobauyah Kpatcha Tchamdja, Carlos Gómez Martínez, Duncan Laki Muhumuza, Photini Pazartzis, Hernán Quezada, Vasilka Sancin, José Manuel Santos Pais, Changrok Soh, Hélène Tigroudja, Imeru Tamerat Yigezu, and Gentian Zyberi.

*** Individual opinions by Committee members Furuya Shuichi and Gentian Zyberi (dissenting) are annexed to the present Views.

1. The author is Mr. Maharajah Madhewoo, a Mauritian national born in 1954. He claims to be a victim of a violation by the State party of his rights under article 17 of the International Covenant on Civil and Political Rights ("the Covenant"). The Optional Protocol entered into force for the State party on 23 March 1976. The author is represented by counsel.

Facts as submitted by the author

2.1 An identity card scheme was introduced in Mauritius by the National Identity Card Act 1985 ("the 1985 Act"). Under that law, a Registrar was required to keep a Register of all Mauritian citizens under the Minister responsible for civil status. The particulars on the Register were sex, name and other such details as "reasonable or necessary". Every citizen was required to apply for the identity card within six months of becoming 18, upon which they had to allow themselves to be photographed. Every card had a number, a photograph, the holder's signature and the date of issue. In "reasonable circumstances", any person could request production of an identity card, but there was no requirement to produce it. The 1985 Act also provided for fines of 10,000 Mauritian rupees and imprisonment for up to six months for wilful misuse of identity cards.

2.2 The Finance (Miscellaneous Provisions) Act 2009 ("the 2009 Act") expanded the information required to be provided on an application for an identity card, including fingerprints and other biometric information, and the information on the card itself, including full names, maiden names where applicable, date of birth, and "such other information as may be prescribed". The 2009 Act increased penalties for non-compliance to 100,000 rupees and imprisonment up to five years.

2.3 A number of additional amendments followed, pursuant to the relevant Minister's mandate to make regulations on smart identity card readers and their use by public and private entities. The National Identity Card (Miscellaneous Provisions) Act 2013 ("the 2013 Act") amended the 1985 Act, stipulating that a person empowered by law to ascertain the identity of a person could request sight of one's identity card, and requiring production thereof. A new section was added to make the collection and processing of biometric information subject to the Data Protection Act. Moreover, the National Identity Card (Particulars in Register) Regulations 2013 ("the 2013 Regulations") provided for information gathered from the applicant to be recorded on the Register.

2.4 The author challenged the constitutionality of the implementation of the new biometric identity card as per the 2013 Act, claiming, inter alia, a breach of article 9 of the Mauritius Constitution on the protection of privacy.[1] In its judgment of 29 May 2015, the Supreme Court held that the new scheme interfered with the rights protected under article 9 (1) of the Constitution. However, the Supreme Court considered the law providing for the scheme concerning fingerprints and other biometric data to be sufficiently precise and accessible to be "under the authority of any law" as required by article 9 (2) of the Constitution. It further considered that the provision had been made "in the interests of … public order" and was therefore a "permissible derogation" from article 9 (1) of the Constitution, based on evidence from State officials that the provision of fingerprints prevented an applicant from making multiple applications for an identity card. The Court considered that the author had not shown that the introduction of the requirement for all persons applying for an identity card to allow their fingerprints and other biometric data to

[1] The relevant part of article 9 reads:
"(1) Except with his own consent, no person shall be subjected to the search of his own person or his property or the entry by others on his premises.
(2) Nothing contained in or done under the authority of any law shall be held to be consistent with or in contravention of this section to the extent that the law in question makes provision –
(a) in the interests of defence, public safety, public order, public morality, public health, town and country planning, the development or utilisation of mineral resources or the development or utilisation of any other property in such a manner as to promote the public benefit;
(b) for the purpose of protecting the rights or freedoms of other persons;
(…)
Except so far as that provision or, as the case may be, the thing done under its authority is shown not to be reasonably justifiable in a democratic society."

be taken and recorded was not reasonably justifiable in a democratic society, given the pressing social need of protection against identity fraud, considered "vital for proper law enforcement" in Mauritius. The author had also argued before the Supreme Court that despite the legitimate aim, there were insufficient reasons to establish that indefinite storage of such data was proportionate. He had argued that further exemptions in the Data Protection Act allowed for an alarming degree of access, including for the mere purpose of obtaining legal advice, and the lack of provision of any judicial oversight to such access. The Supreme Court considered that there is also a public order justification for storing and retaining such data. However, examining whether such storage and retention is reasonably justifiable in a democratic society, the Supreme Court considered expert evidence showing that biometric data retention was insecure and notoriously difficult to protect even if present technical challenges were rectified. Thus, the Supreme Court held that indefinite storage and retention of biometric data under the Data Protection Act was disproportionate to the aim pursued and was not reasonably justified in a democratic society.

2.5 In response, the authorities issued the National Identity Card (Civil Identity Register) Regulations 2015 ("the 2015 Civil Register Regulations") to revoke the 2013 Regulations and omit the addition of full biometric information to the Register. According to the Ministry of Technology, Communication and Innovation, all biometric data were destroyed and deleted from the Register in September 2015, and fingerprint data are now retained only as long as it takes to issue the identity card, after which it is deleted.

2.6 The National Identity Card (Amendment) Regulations 2015 ("the 2015 Amendment Regulations") amended the 2013 Regulations to add the following statement to the declaration to apply for an identity card: "I have no objection that my fingerprint minutiae be processed and recorded for the purpose of producing my identity card. I understand that this information will be erased permanently from the Register once the identity card has been printed." According to the author, the addition of the statement was inappropriate, as non-application is a criminal offense, and there is thus no choice to apply whether or not one objects.

2.7 The Judicial Committee of the Privy Council dismissed the author's appeal to the Supreme Court's judgment on 31 October 2016. However, it noted that the destruction of biometric data after the issuance of identity cards may affect the ability to prevent identity fraud by multiple applications using other identities and documents. It also noted that future requirements by the executive of other biometric data to be added to the identity card may raise new issues of proportionality.

2.8 Further changes have been made pursuant to the Finance (Miscellaneous Provisions) Act 2017 (Act 10 of 2017), not yet in force at the time of the submission of the communication. Under this Act, prescription of data to be included on the identity card remains the power of the executive.

The complaint

3.1 The author claims that the National Identification Card Act, as amended, engages his rights under article 17 of the Covenant, given its involvement of the compulsory use and retention of sensitive personal data, whose production to State officials can be required. He submits that the Act fails the requirements of legality, proportionality and necessity[2].

[2] The author also notes the absence of international consensus on the requirement for compulsory national identification schemes or the personal information they contain, as well as widespread privacy concerns regarding such schemes. He submits that a distinction should be drawn between the retention of basic information such as names, addresses, dates of birth and gender on the one hand, and of sensitive, personal information, such as fingerprints or DNA, on the other, European Commission of Human Rights, Filip Reyntjens v. Belgium, application No. 16810/90; Friedl v. Austria, 15225/89 He also submits that measures interfering with the right to privacy must be lawful, necessary and proportionate, European Court of Human Rights, S. and Marper v. The United Kingdom, application Nos. 30562/04 and 30566/04, 4 December 2008; Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others, 24 August 2017.

3.2 The author acknowledges that the identity card scheme is provided for by domestic law, but submits that the domestic provisions are not concordant with the aims and objectives of the right protected under the Covenant. First, certain provisions enable the Minister to expand the requirements of the Act without further provision.[3] The author argues that the delegation to the executive of the prescription of what sensitive data is collected and recorded on the Register and the identity card is arbitrary and far too open-ended and uncertain to comply with the aims and objectives of article 17 of the Covenant. The State party has been planning to enlarge the ambit of the schemewithout further legislative scrutiny despite the importance of considering risks to privacy.[4] According to the author, the proposed expansion of the smart card system to cover health records causes particular concern.[5]

3.3 Second, there is no judicial or other independent supervision of the workings of the scheme, of the additional prescription of private information or of collection, destruction, recording or access to information recorded on the Register or the identity card.

3.4 Third, the collection and recording of private information is subject only to the safeguards of the Data Protection Act. In the present case, the Supreme Court concluded that the level of protection provided by the Data Protection Act was insufficient and that it was unlawful for the State party to store biometric data beyond the issuance of the identity card. The scheme was changed to shift the retention of the fingerprint data from the authorities' systems to the individual by requiring the data to be included on the identity card itself, instead of abandoning the collection and retention of fingerprints and biometric data or rectifying the legislative and technical shortcomings identified by the Supreme Court. This modification, according to the author, renders ineffective the aim of the Act to prevent multiple applications by comparing biometric data with previous applications. Moreover, the modification exacerbates the shortcomings identified by the Supreme Court, as citizens now compulsorily retain sensitive data in a vulnerable form for the State party's authorities.

3.5 Further, the author contends that the scheme is not proportional. He argues that the sole justification by the State party for making the provision of fingerprint data compulsory and for citizens to produce the identity card to a State official is public order. He accepts that the scheme has the legitimate aim of preventing identity fraud and, possibly, of assisting with the verification of identity. However, in justifying the effectiveness of the scheme, the State party's authorities referred primarily to the ability to check applications against the database of biometric data, which is the very aspect that the Supreme Court found unlawful. Thus, the inclusion of biometric data on the identity card does not prevent applications for multiple identity cards with the same fingerprints in any way.[6] Inclusion of fingerprints on a fraudulently obtained identity card indeed lends it greater legitimacy. Even with the advantage of rendering it more difficult for stolen or lost identity cards to be used, a simple database of identity cards lost or stolen would achieve a similar objective without the intrusion of collecting and storing biometric data. Moreover, the carrying of an identity card and assignation of the responsibility for storage of the biometric data to citizens has the security weaknesses identified by the State party's authorities in their justification of the scheme itself, namely the loss or theft of a significant number of identity cards. Expert

[3] The author refers to:
Section 3 (2) (b) of the National Identity Card Act requires a register to be kept, including "such other reasonable or necessary information as may be prescribed";
Section 5 (2) of the Act specifies what information shall be recorded on the identity card itself.
Section 5 (2) (h) (now f) allows "such other information as may be prescribed";
Section 10 of the Act provides for the Minister to make such regulations "as he thinks fit for the purposes of this Act".

[4] European Court of Human Rights, S. and Marper v. The United Kingdom, paras. 71-75.

[5] European Court of Human Rights, L.H. v. Latvia, application No. 52019/07.

[6] The author refers to the following reasoning of the Judicial Committee of the Privy Council: "The absence of the fingerprints and minutiae from the register after an identity card is issued may affect adversely the Government's ability to prevent identity fraud, for example, if someone were to apply more than once for an identity card using different names and documentation. The extent to which an interference with a fundamental right can achieve a legitimate aim is a consideration in any assessment of its justification."

evidence submitted to the Supreme Court showed that the fingerprint data could likely be copied onto falsified identity cards.

State party's observations on admissibility and the merits

4.1 By note verbale of 1 June 2018, the State party informed that it did not wish to contest the admissibility of the communication.

4.2 By note verbale of 21 September 2018, the State party submitted its observations on the merits. It observes that the author cannot claim an infringement of his rights, as he has not had his fingerprints taken.

4.3 The State party observes that the right to the protection of personal data, including in the context of processing fingerprints, is not absolute and must be considered in relation to its function in society.[7] It also observes that the Supreme Court held that the provisions on the processing of fingerprints, disclosed an interference with the author's rights under article 9 (1) of the Constitution. However, the Supreme Court considered that such was permissible under article 9 (2) of the Constitution as being in the interest of public order. It also considered that the author had failed to show that the interference was not reasonably justifiable in a democratic society. The Supreme Court found that the taking of fingerprints was necessary and proportionate to the aim of establishing a secure identity protection system and of protecting against identity fraud.[8] The Judicial Committee of the Privy Council, noting that "it will be slow to interfere with an evaluation of [the justification of an interference with a fundamental right] by a local court which is more familiar with the circumstances in its society than the Board can be", upheld the Supreme Court's reasoning.

4.4 The State party submits that the taking and storing of fingerprints is warranted to achieve the pressing social need of protecting against identity fraud, by assisting authorities in verifying citizens' identities, eliminating fraudulent practices and to maintain law and order. The State party argues that the Supreme Court, in light of the need to balance all interests involved when restricting rights,[9] struck a fair balance between the public interest and the prejudicial effects on the author's private life. It argues that the Supreme Court rightly held that the interference in the present case was motivated by a legitimate aim, was not disproportionate or intolerable interference on the author's right to privacy, and was thus justified in the circumstances. The State party concludes that the interference is "not manifestly without reasonable foundation".[10]

4.5 The State party disputes that the restriction is not provided for by law. It notes that the author challenged the implementation of the biometric identity card as per the National Identity Card Act before the Supreme Court, but that the latter dismissed his challenge. The State party argues that the author's apprehensions are based on hypothetical considerations and that he would be free to bring a case to the Supreme Court again, should the scheme be expanded in the future.

Author's comments on the State party's observations

5.1 On 20 December 2018, the author submitted his comments on the State party's observations. He notes that his claim of a violation relates to a statutory obligation under the National Identity Card Act, to which he is subject as a national of Mauritius. The Act criminalises the failure to apply for an identity card and the author is thus subject to arrest

[7] European Court of Justice, Eugen Schmidberger, Internationale Transporte und Planzüge v. Republic of Austria (C-112/00); Michael Schwarz v. Stadt Bochum (C-291/12), paras. 33, 45, 50-51, 62-64, 66; X. v. Commission of the European Communities (C-404/92 P), para. 18; European Court of Human Rights, S. and Marper v. The United Kingdom, application Nos. 30562/04 and 30566/04, 4 December 2008, para. 101; High Court of Justice, Queen's Bench Division, Administrative Court sitting in Birmingham, R. (on application of R.) v. Chief of Constable [2013] EWHC 2864, para. 37.

[8] The Court referred, inter alia, to: S. and Marper v. The United Kingdom, application Nos. 30562/04 and 30566/04, 4 December 2008; Leyla Şahin v. Turkey, application No. 44774/98.

[9] Schmidberger v. Republic of Austria, paras. 79-81.

[10] R. (on application of S.G. and others (previously J.S. and others) v. Secretary of State for Work and Pensions [2015] UKSC 16, para. 37.

and conviction in the event of non-compliance. The author argues that he is therefore a victim under article 1 of the Optional Protocol.

5.2 The author argues that the State party confuses judicial oversight with access to courts to challenge the constitutionality of the Act. He notes that it was the Supreme Court itself that found that the lack of provision for judicial oversight to control access to data within the scheme was "objectionable". He also notes that in several Concluding Observations, the Committee has referred to the importance of safeguards in schemes where interference with privacy may be permitted as proportionate to the legitimate aim pursued.[11]

5.3 On proportionality, the author does not contest that the Committee should show respect to the approach of the national authorities and courts, but argues that domestic law and policy is not determinative, and that the level of scrutiny depends on the context. He argues that the State party's invocation of the judgment of the European Court of Human Rights in *Şahin v. Turkey* is misplaced, as that case concerned respect for religious freedom. The balance of rights between those practicing different religions and none was found to be highly dependent on location, leading the Court to accord a wide margin of appreciation to national authorities. The author submits that the present case is different as it concerns a measure to combat identity fraud, which occurs the world over. He submits that the other cases cited by the State party concern schemes that are either non-compulsory or relate to very specific and pressing legitimate aims, or both. However, the present case concerns a blanket, general and compulsory provision, whose proportionality must, by definition, be far more difficult to establish than a specific or narrowly targeted interference. Moreover, the State party's authorities have publicly stated that they aim to extend the scheme, and thereby the interference with privacy.

Issues and proceedings before the Committee

Consideration of admissibility

6.1 Before considering any claim contained in a communication, the Committee must decide, in accordance with rule 97 of its rules of procedure, whether it is admissible under the Optional Protocol.

6.2 The Committee takes note that the State party does not contest the admissibility of the communication. It also takes note, however, of the State party's argument that the author cannot claim a violation of his rights under the Covenant, on the ground that he has not had his fingerprints taken. The Committee further takes note of the author's argument that, as a Mauritian national, he is subject to a statutory obligation to have an identity card requiring the taking and recording of fingerprints, non-compliance with which amounts to a criminal offence. Therefore, the Committee considers that the author has substantiated his victim status, for the purpose of admissibility, and that article 1 of the Optional Protocol does not preclude it from examining the communication.

6.3 The Committee has ascertained, as required under article 5 (2) (a) of the Optional Protocol, that the same matter is not being examined under any other procedure of international investigation or settlement.

6.4 The Committee notes that the author brought a claim to the Supreme Court of Mauritius and appealed to the Judicial Committee of the Privy Council and that there is no information on file concerning remedies that the author failed to exhaust. Accordingly, the Committee considers that article 5 (2) (b) of the Optional Protocol does not preclude it from examining the communication.

6.5 The Committee considers that the author has sufficiently substantiated his claims as raising issues under article 17 of the Covenant and notes, as stated previously, the State party's observation that it does not contest the admissibility of the communication. Accordingly, the Committee declares the communication admissible, and proceeds with its consideration on the merits.

[11] Concluding Observations on the Russian Federation (1995) (CCPR/C/79/Add.54), para. 19; Concluding Observations on Jamaica (CCPR/C/79/Add.83), para. 20.

Consideration of the merits

7.1 The Committee has considered the present communication in the light of all the information made available to it by the parties, as provided under article 5 (1) of the Optional Protocol.

7.2 The Committee notes that it appears undisputed between the parties that the mandatory taking and recording of the author's fingerprints would constitute an interference with his privacy. The Committee notes the author's claim that the amended National Identity Card Act violates his rights under article 17 of the Covenant because it is unlawful and arbitrary. It also notes that the State party disputes the author's allegations.

7.3 The Committee recalls that interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.[12] Likewise, the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law.[13] The Committee further recalls that an interference is not "unlawful", within the meaning of article 17 (1) of the Covenant, if it complies with the relevant domestic law, as interpreted by the national courts.[14] The Committee notes that the interference complained of in the present case, i.e. the processing and recording of fingerprints, is provided for by section 4 (2) (c) of the National Identity Card Act.[15] The Committee also notes that the Supreme Court found that "there is a law providing for the storage and retention of fingerprints and other biometric data regarding the identity of a person".[16] The Committee considers that the author's argument concerning the scope of certain provisions in the Act does not allow it to conclude that the processing of his fingerprints is not provided for by law. Thus, the Committee cannot conclude that the interference with the author's privacy is unlawful.

7.4 The Committee recalls that the introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law "must comply with the provisions, aims and objectives of the Covenant, and should be, in any event, reasonable in the particular circumstances" [17] Accordingly, any interference with privacy and family must be proportionate to the legitimate end sought and necessary in the circumstances of any given case.[18] The Committee further recalls that effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant.[19]

7.5 In the present case, the Committee notes the State party's observation of the need to balance the protection of personal data with the pressing social need of preventing identity fraud. It further notes that the State party argues that its Supreme Court had rightly held that the taking of fingerprints is warranted to prevent fraud. The Committee also notes that the State party's authorities have shifted the retention of the fingerprint data from the authorities' systems to individual identity card holders by requiring such data to be included on the card itself. The author, as well as the Judicial Committee of the Privy Council, have noted that this change renders the objective of making comparisons with previously submitted biometric data ineffective and thus affects the ability of the State party's authorities to prevent identity fraud. The Committee notes that the State party has not responded to this specific point, nor explained how the storage and retention of fingerprint data on individual identity cards can effectively prevent identity fraud.

[12] General Comment No. 16, para. 3.

[13] Ibid., para. 10.

[14] Van Hulst v. The Netherlands, para. 7.5.

[15] "Every person who applies for an identity card shall— (…) (c) allow his fingerprints, and other biometric information about himself, to be taken and recorded (…)."

[16] Supreme Court of Mauritius, Madhewoo M. v. The State of Mauritius and Anor, 2015 SCJ 177, p. 29.

[17] See general comment No. 16, para. 4.

[18] See Toonen v. Australia (CCPR/C/50/D/488/1992), para. 8.3; Andrea Vandom v. Republic of Korea (CCPR/C/123/D/2273/2013), para. 8.8.

[19] Ibid.

7.6 Moreover, given the nature and scale of the interference arising out of the mandatory processing and recording of fingerprints, the Committee finds that it is essential "to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness".[20] The Committee notes that the author refers, in this regard, to the Supreme Court's finding that storage and indefinite retention of fingerprint data in a central database was unconstitutional. As a result, the State party's authorities have ceased storing and retaining fingerprint data in this particular way. Nevertheless, the State party has not responded to the author's claim that retention of fingerprint data on identity cards exacerbates the security lacunae identified by the Supreme Court. Specifically, the author has pointed out that the assignation of responsibility for such storage to card holders carries with it risks of loss and theft of fingerprint data, given the ease with which they could be copied onto falsified cards.[21] Thus, given the lack of information provided by the State party concerning the implementation of measures to protect the biometric data stored on identity cards, the Committee cannot conclude that there are sufficient guarantees against the risk of abuse and arbitrariness following from potential access to such data on identity cards. In light of the abovementioned concerns about the ability of the scheme to help prevent identity fraud, the Committee considers that the security concerns cannot be regarded as reasonable. Therefore, and notwithstanding the possibility of grounds and circumstances in which the processing of biometric data would not give rise to an arbitrary interference in the sense of article 17 of the Covenant, the Committee considers, in the particular circumstances of the case, that storage and retention of the author's fingerprint data on an identity card, as prescribed by the National Identity Card Act, would constitute an arbitrary interference with his right to privacy, contrary to article 17 of the Covenant.

8. Accordingly, the Committee, acting under article 5 (4) of the Optional Protocol, is of the view that the facts before it disclose a violation by the State party of the author's rights under article 17 of the Covenant.

9. In accordance with article 2 (3) (a) of the Covenant, the State party is under an obligation to provide the author with an effective remedy. Accordingly, the State party is obligated to provide sufficient guarantees against the risk of arbitrariness and abuse of the author's fingerprint data as may arise from the issuance of an identity card to him, and to review the grounds for storing and retaining fingerprint data on identity cards, in light of the present views. Additionally, the State party is under the obligation to take steps to avoid similar violations in the future.

10. Bearing in mind that, by becoming a party to the Optional Protocol, the State party has recognized the competence of the Committee to determine whether there has been a violation of the Covenant and that, pursuant to article 2 of the Covenant, the State party has undertaken to ensure to all individuals within its territory or subject to its jurisdiction the rights recognized in the Covenant and to provide an effective and enforceable remedy when it has been determined that a violation has occurred, the Committee wishes to receive from the State party, within 180 days, information about the measures taken to give effect to the Committee's Views. The State party is also requested to publish the present Views and disseminate them broadly in the official language of the State party.

[20] European Court of Human Rights, S. and Marper v. The United Kingdom, para. 99.

[21] The author refers to expert evidence submitted in the domestic proceedings concerning the radio frequency identification (RFID) technology with which the biometric data are stored. The expert explains that the biometric data can easily and without physical contact be copied, without the card holder's knowledge, with RFID readers that can easily be bought online.

Annex 1

Individual Opinion of Mr. Shuichi Furuya (Dissenting)

1. I am unable to concur with the View's conclusion that the author has substantiated his victim status for the purpose of admissibility and that article 1 of the Optional Protocol does not preclude the Committee from examining the communication.

2. According to article 1 of the Optional Protocol, the Committee can receive and consider "communications from individuals who claim to be victims of a violation … of any of the rights set forth in the Covenant." In this respect, the Committee has settled its jurisprudence that "a person can only claim to be a victim in the sense of article 1 of the Optional Protocol if he or she is actually affected. It is a matter of degree how concretely this requirement should be taken. However, no individual can in the abstract, by way of an *actio popularis*, challenge a law or practice claimed to be contrary to the Covenant. If the law or practice has not already been concretely applied to the detriment of that individual, it must in any event be applicable in such a way that the alleged victim's risk of being affected is more than a theoretical possibility."[1] Accordingly, "any person claiming to be a victim of a violation of a right protected under the Covenant must demonstrate either that a State party has, by act or omission, already impaired the exercise of his right or that such impairment is imminent, basing his arguments for example on legislation in force or on a judicial or administrative decision or practice."[2]

3. In applying this principle, the Committee has accepted the communications at the stage that the authors' rights have not actually been impaired yet, but just at risk of being impaired by certain legislations. However, even in such cases, it has recognized that "where an individual is in a category of persons whose activities are, by virtue of the relevant legislation, regarded as contrary to law, they may have a claim as 'victims'".[3] In fact, the Committee has acknowledged the victim status only for the defined category of persons, such as Muslims and non-Western migrants[4], sexual minorities[5], language minorities[6] and women having foreign husbands[7], even if a legislation in question may be in theory applied to all the nationals of the State party.

4. In addition, the Committee has requested authors to demonstrate the specific consequence of the legislation which would personally affect those authors. For instance, in *Toonen v. Australia*, the Committee found admissible because "the author had made reasonable efforts to demonstrate that the threat of enforcement and the pervasive impact of the continued existence of these provisions on administrative practices and public opinion had affected him and continued to affect him personally"[8]. On the other hand, in *Andersen v. Denmark*, it found the communication inadmissible in light of the fact that "the author has failed to establish that the statement made … had specific consequence for her or that the specific consequences of the statements were imminent and would personally affect the author."[9]

5. In the present case, it is clear that the author's rights under the Covenant have not been impaired yet since the author has not had his fingerprints taken nor been accused of the non-compliance with relevant legislations. Nevertheless, the View finds that the author has substantiated his victim status due to the fact that "as a Mauritian national, he is subject to a

[1] Aumeeruddy-Cziffra et al. v. Mauritius (CCPR/C/12/D/35/1978), para. 9.2.
[2] Andersen v. Denmark (CCPR/C/99/D/1868/2009), para. 6.4; Beydon et al. v. France (CCPR/C/85/D/1400/2005), para. 4.3; Aalbersberg et al. v. the Netherlands (CCPR/C/87/D/1440/2005); Brun v. France (CCPR/C/88/D/1453/2006), para. 6.3.
[3] Ballantyne et al. v. Canada (CCPR/C/47/D/359/1989 and 385/1989/Rev.1), para. 10.4.
[4] Rabbae et al. v. the Netherlands (CCPR/C/117/D/2124/2011), para. 9.6;
[5] G. v. Australia (CCPR/C/119/D/2172/2012), para. 6.5.
[6] Raihman v. Latvia (CCPR/C/100/D/1621/2007), para. 7.4.
[7] Aumeeruddy-Cziffra et al. v. Mauritius, supra note , para. 9.2 (b)(2).
[8] Toonen v. Australia (CCPR/C/50/D/488/1992), para. 5.1.
[9] Andersen v. Denmark, supra note 2, para. 6.4.

statutory obligation to have an identity card requiring the taking and recording of fingerprints, non-compliance with which amounts to a criminal offence" (para. 6.2). In my view, however, the author has not demonstrated that he belongs to a defined category of persons whose activities are, by virtue of the relevant legislation, regarded as contrary to law. Nor has he made every effort to demonstrate the specific consequence or personal effect of the legislation on him. Without such demonstration, granting the victim status merely because of his Mauritian nationality is tantamount to accepting an *actio popularis*, which undoubtedly deviates from the jurisprudence of the Committee.

6. Accordingly, I have to conclude that the author does not have the victim status for the purpose of admissibility and therefore the communication is inadmissible under article 1 of the Optional Protocol.

Annex 2

Individual Opinion of Mr. Gentian Zyberi (Dissenting)

1. I am not agreed with the conclusion of the Committee, finding a violation of Article 17 in this case. I find this decision a missed opportunity to provide some guidance, since to my knowledge this is the first case where the Committee has addressed issues concerning the inclusion of biometric data in personal ID cards and the right to privacy under Article 17.

2. The gist of the Committee's rationale for the decision is contained in paragraph 7.6. First, the Committee notes that given the lack of information provided by the State party concerning the implementation of measures to protect the biometric data stored on identity cards, it cannot conclude that there are sufficient guarantees against the risk of abuse and arbitrariness following from potential access to biometric data on identity cards. Then, and without much explanation, the Committee holds that in the particular circumstances of the case, storage and retention of the author's fingerprint data on an identity card, as prescribed by the National Identity Card Act, would constitute an arbitrary interference with his right to privacy, contrary to article 17 of the Covenant.

3. The Committee does not really explain why the storage and retention of the author's fingerprint data on an identity card constitutes an arbitrary interference with his right to privacy. Nor has the Committee in its short analysis referred to any good practices concerning the inclusion or not of biometric data, including fingerprints, in national ID cards. Given the complexity of the matter, it would have been prudent for the Committee to ask for third party submissions, to elucidate the key issues put before it. Article 17 was drafted at a time when advanced biometrics technology was not available and national ID documents did not include personal biometrical digital data. In more recent years, many countries are including biometric data, including fingerprints, in personal ID cards.[10] This inclusion serves different purposes, including prevention of identity fraud, countering terrorism, and other public security purposes. At the same time, several challenges have arisen, which include issues of accountability, privacy, data management, enrollment, coverage, cost, and harmonization of ID programs.

4. While these new biometric ID technologies are increasingly being used by many States, there are no firm guarantees that such ID cards cannot be falsified or potentially misused. While acknowledging some of the problems, the Mauritius authorities have emphasized the need to balance the protection of personal data included in ID cards with the

[10] For EU member States, see Regulation (EU) 2019/1157 of 20 June 2019, Article 3(5). See also the decision of the Belgian Constitutional Court of 14 January 2021 (in Dutch, at https://www.const-court.be/public/n/2021/2021-002n.pdf). See also International Telecommunication Union, Review of National Identity Programs (FG-DFS, 05/2016), p. 8 (key findings), and pp. 14-16 (providing a list of States and whether the national IDs contain fingerprints or not); World Bank Group, The State of Identification Systems in Africa (Country Briefs), 2017; Asian Development Bank, Identity for Development in Asia and the Pacific, 2016.

pressing social need of preventing identity fraud and public security. The National Identity Card Act (Section 9, Offences) protects against abuse and arbitrariness following from potential access to biometric data on identity cards by making such offences punishable by a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding five years. This part of the law is meant to protect individuals, as the author, from potential misuse by criminals of personal ID cards or the biometric data contained therein. Cases decided by the European Court of Human Rights concern the retention of personal data (fingerprints, DNA, photos, etc.) in databases for an indefinite period of time,[11] or after the discontinuation of criminal proceedings.[12] So far, there are no cases relating to the storage and retention of fingerprints in relation to ID cards, despite many States party to the European Convention on Human Rights having a national ID system that includes fingerprints in such IDs.[13]

5. While I share the general concern of the Committee that such technologies should be well-regulated, in order to ensure that they are not misused by a State or third parties, by concluding that the simple storage and retention of the author's fingerprint data on an identity card, as prescribed by the National Identity Card Act, would constitute an arbitrary interference with Article 17, the Committee has interpreted Article 17 in an overbroad manner.

6. The complaint was seemingly moot, given that the person was not forced to give his fingerprints. Several aspects of the case had been decided at the domestic level by the Supreme Court and the Privy Council and identified shortcomings had been subsequently addressed by the State authorities. Moreover, it is not clear whether certain issues the author raised with the Committee, had been adequately raised and exhausted at the domestic level. The better course for the Committee, given the facts of the case, would have been to find no violation of Article 17.

[11] S. and Marper v. the United Kingdom (Applications nos. 30562/04 and 30566/04); Gaughran v. the United Kingdom (Application no. 45245/15).

[12] *M.K. v. France* (Application no. 19522/09).

[13] See Guide to the Case-Law of the of the European Court of Human Rights, Data Protection, 31 December 2020 (Council of Europe/European Court of Human Rights, 2021), on case-law concerning the storage and retention of fingerprints, including paras. 24, 29, 111, 192, 200.