# SUBMISSION TO THE UNITED NATIONS SPECIAL RAPPORTEUR ON EXTREME POVERTY AND HUMAN RIGHTS IN RESPONSE TO THE CALL FOR SUBMISSIONS ON DIGITAL TECHNOLOGY, SOCIAL PROTECTION AND HUMAN RIGHTS

SUBMITTED JOINTLY BY THE ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS, DERECHOS DIGITALES AND MEDIA MATTERS FOR DEMOCRACY

**Submitted electronically by Deborah Brown, Global Advocacy Lead, Association for Progressive Communications | deborah@apc.org**

*This submission was prepared with the assistance of ALT Advisory. For more information, please visit: https://altadvisory.africa/.*

**INTRODUCTION**

1. The Association for Progressive Communications (APC),[1] Derechos Digitales[2] and Media Matters for Democracy[3] welcome the opportunity to provide this submission on the human rights impacts of the introduction of digital technologies in the implementation of national social protection systems (NSPS). In particular, we focus on selected aspects raises in issues 3 and 4 of the call for submissions.[4]

2. As a point of departure, we recognise that digital technologies can have a role to play in delivering social protection benefits efficiently. However, caution must be exercised by all stakeholders to ensure that the use of such technologies are cognisant of the existing and potential risks. In practice, these technologies are often presented as a solution to a problem that has not been clearly defined, and raises concerns of creating new challenges or exacerbating existing ones.

**HUMAN RIGHTS IMPLICATIONS AND BALANCING COMPETING RIGHTS**

3. It is well-established that the collection and processing of the data required to implement NSPS – including personal data – directly implicates the right to privacy. However, as set out in General Comment No. 19[5] (GC19) on the International Covenant on Economic, Social and Cultural Rights (ICESCR), the right to social security plays an important role in supporting the realisation of many other rights.[6]

4. In particular, where states make it a mandatory requirement that NSPS benefits can only be accessed with a digital identification card (DIC), persons who have not obtained this are excluded from the right to social security and the contingent rights. For example, this might result in a person being excluded from a public health facility which impacts the right to health in article 12 of the ICESCR.[7]

---

[1] For more information about APC, visit: https://www.apc.org/. Further, in respect of APC's work in the Women's Rights Programme, please visit: https://www.genderit.org/.

[2] For more information about Derechos Digitales, please visit: https://www.derechosdigitales.org/.

[3] For more information about Media Matters for Democracy, please visit: http://mediamatters.pk/.

[4] This submission is structured as follows: (i) the human rights implications and the balancing of competing rights; (ii) practical challenges in accessing digital technologies in NSPS; (iii) potential for exploitation in the use of digital technologies; (iv) potential for bias and exclusion in the use of algorithms; (v) the need for appropriate policy and regulatory frameworks; (vi) the need for meaningful engagement, impact assessments and review; and (vii) the impermissibility of retrogressive measures. For ease of reference, we have also included a bundle of relevant resources with this submission.

[5] Committee on Economic, Social and Cultural Rights, 'General Comment No. 19: The right to social security', 4 February 2008, accessible at https://www.refworld.org/docid/47b17b5b39c.html.

[6] GC19 at para 28. This is not unique to the right to social security: for example, where a form of digital identification is required to vote, persons without this are rendered unable to exercise their right to vote in terms of article 25(b) of the International Covenant on Civil and Political Rights. This has the potential to lead to further disenfranchisement, social division, inequality and marginalisation.

[7] For more on sexual and reproductive rights, see Tarryn Booysen, 'Role of internet in realising sexual and reproductive rights in Uganda: Interview with Allana Kembabazi' in *GenderIT.org*, 6 December 2016, accessible at https://www.genderit.org/node/4865/; for more on the right to work, see Radhika Radhakrishnan, 'Harnessing the internet to realise labour rights in Cambodia: Interview with Alexandria Demetrianova' in *GenderIT.org*, 6 December 2016, accessible at https://www.genderit.org/node/4867/; for more on social protection and the future of work, see Christina Behrendt and Quynh Anh Nguyen, 'Innovative approaches for ensuring universal social protection for the

5. In terms of balancing competing rights, the three-part test for the justifiable limitation of any right is well-established under international law: (i) the limitation must be provided for in law; (ii) it must pursue a legitimate aim; and (iii) it must be necessary and proportionate to the aim pursued.

6. This requires appropriate safeguards to ensure that the balance is appropriately struck without there being a complete abandonment of rights. Further, the use of digital technologies for social security should done in a manner that causes the least interference with other rights. Affected persons should not be placed in the invidious position of having their vulnerability exploited by it being made compulsory for them to relinquish certain rights – such as privacy – in order to fulfil the basic needs that are realised through the provision of social security. Such safeguards include:

    6.1. The use of the digital technologies should not be mandatory to access NSPS. Provision should be made for persons to opt-out and rely on traditional methods, particularly until such time as there has been public consultation and education.

    6.2. Persons should not be penalised if they do not access their social security benefits using the digital technologies.

    6.3. A cut-off period should not be imposed for registration on digital platforms or application for DICs.

    6.4. Robust data protection safeguards should be implemented and enforced, including requirements that the data collected and processed is done for a specific and explicitly-defined purpose, appropriately secured and that data subjects are able to access, rectify and object to any processing.

7. While digital technologies may facilitate access to NSPS, these technologies can also be monopolised by certain groups, resulting in widening – rather than narrowing – income and other gaps.[8]

**CHALLENGES IN ACCESSING DIGITAL TECHNOLOGIES**

8. In countries with low levels of digital literacy, affected persons may be prevented from exploiting the full potential of the internet. This disproportionately affects persons who – due to levels of poverty, unemployment and education – are more likely to be digitally illiterate and to face obstacles in accessing the services.[9] Digital literacy is critical to the

---

future of work' in *International Labour Organization*, 2018, accessible at https://www.ilo.org/global/topics/future-of-work/publications/research-papers/WCMS_629864/lang--en/index.htm.

[8] Ilcheong Yi, 'Beyond a production- and productivity-centred view on technological progress' in *Social Protection and Human Rights*, 28 March 2019, accessible at https://socialprotection-humanrights.org/expertcom/beyond-a-production-and-productivity-centred-view-on-technological-progress/.

[9] Tarryn Booysen, above n 7. This includes, for example, women, elderly persons, persons with disabilities, transgender persons and migrants.

effective implementation of any digital technology to access the services, ensure online safety and avoid being victims of cybercrimes.

9. The associated costs must also be considered, in particular the costs of a device and data. In this regard, any NSPS platform should, to the extent possible, consider not relying on smartphone technology, or minimising data costs through zero-rating. Efforts should further be made to create a consistent framework and interface across different platforms to avoid confusion amongst users. Further, contingency must be made for persons in rural areas with poor or inconsistent electricity and network coverage, who are hindered in their access to NSPS platforms.

10. By way of illustration, it has been recorded that: "Polish citizens still prefer to take care of administrative matters by visiting offices. Statistics indicate that the most important reasons for not using e-services in Poland were (among others) the concerns about protection and security of personal data (6%), lack of knowledge and skills (4%), the problem with the e-signature (2%), and limitations associated with access to websites (1%)."[10] Similarly, in Kenya, the following concerns have been raised regarding registration with the National Identification Scheme (NIS): fear and confusion; exclusion and discrimination; lack of trust in the system; data protection; and digitised discrimination.[11]

11. In addition to the practical challenges, it is also relevant to consider the psychological impact on persons who are unable to – or effectively denied – access owing to their inability to use the technology. This has the potential to lead to disempowerment through lack of access or being dependent on another to facilitate access. Additionally, removing the human element and support structures to help navigate a complex social benefit system may be uncomfortable for persons and result in them losing their benefits.[12]

**POTENTIAL FOR EXPLOITATION IN THE USE OF DIGITAL TECHNOLOGIES**

12. GC19 sets out the obligations on states parties to the ICESCR: the obligation to respect, protect and fulfil. Of particular relevance to the use of digital technologies in NSPS:

    12.1. The obligation to protect requires states to prevent third parties, including corporations, from interfering with the enjoyment of the right to social security.[13]

---

[10] Jedrzej Niklas, 'E-government in the welfare state: Human rights implications of the digitalisation of social policy in Poland' in Alan Finlay and Deborah Brown (eds) *Global Information Society Watch 2016*, 2016 at p 182, accessible at https://www.giswatch.org/en/economic-social-and-cultural-rights-escrs/key-considerations-economic-social-and-cultural-rights-. This has resulted in at least 40% of the most poor people in Poland not receiving the financial assistance to which they are entitled because of lack of competencies, knowledge and administrative challenges. For a comprehensive discussion on the challenges experienced in the implementation of two digital technology solutions for NSPS in Poland, see pp 183-187.

[11] Liz Orembo, 'What lies behind the fears of digital identity? The experience of the Huduma Number in Kenya' in *GenderIT.org*, 30 May 2019, accessible at https://www.genderit.org/feminist-talk/what-lies-behind-fears-digital-identity-experience-huduma-number-kenya.

[12] Esther Shein, 'The dangers of automating social programmes' in *Communications of the ACM*, vol. 16, October 2018, pp 17-19, accessible at https://cacm.acm.org/magazines/2018/10/231360-the-dangers-of-automating-social-programs/fulltext. This can occur, for example, when a line of questioning ends in the system but has not allowed the person to complete the explanation.

[13] GC19 at para 45.

Where NSPS are operated or controlled by third parties, states retain the responsibility of administration and ensuring equal, adequate, affordable and accessible social security.[14]

12.2. The obligation to fulfil requires states to take positive measures to, among other things, adopt a national social protection strategy and plan of action to realise the right, and will cover social risks and contingencies.[15] Further, it obliges states to take steps to ensure that there is appropriate education and public awareness concerning access to social security schemes.[16]

13. The Guiding Principles on Business and Human Rights (Guiding Principles) – through the respect, protect and remedy framework – are also relevant. In particular, with regard to the duty to protect, states are required to, among other things, clearly set out the expectation that all business enterprises in their territory respect human rights throughout their operations; enforce laws that require business enterprises to respect human rights; and exercise adequate oversight to meet their international human rights obligations when they contract with, or legislate for, business enterprises to provide services that may impact on the enjoyment of rights.[17] Although the Guiding Principles have had varying degrees of impact, it remains an important tool to guide states and corporations in their interactions, and states should be encouraged to incorporate these principles into any legislation or contract regulating their engagement with third party providers of digital technologies for NSPS.

14. In addition to the Guiding Principles, we submit that the following should also be required:

14.1. States engaging with third parties regarding digital technologies should do so through a competitive procurement process.

14.2. All agreements entered into must impose clear and enforceable obligations, and be made publicly-accessible.

14.3. Data protection principles should be made mandatory, including privacy by design and for data processing to be done lawfully, proportionately and securely.

[14] GC19 at para 46.

[15] GC19 at para 48.

[16] GC19 at para 49. This is particularly important in rural and deprived urban areas, or among linguistic or other minorities.

[17] United Nations Human Rights: Office of the High Commissioner, 'Guiding principles on business and human rights', 2011 at pp 3-12, accessible at https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf.

15. The World Bank identifies four considerations for implementing public-private partnerships for digital technologies: (i) inclusion; (ii) reliability; (iii) data protection; and (iv) sustainability.[18] Precautions are necessary to avoid risks relating to information regulations, control of digital databases and the potential for political or commercial manipulation of personal data.[19] Data should also be appropriately secured against breaches.[20]

16. A particular concern that arises is the sharing of NSPS data with other government agencies or third parties for purposes different to those for which it was originally collected, and without notification to the affected persons. While information may initially be collected in silos, when combined this may appear to create a holistic picture that can be used to make assumptions about a person without their knowledge, and in a manner that is not necessarily complete or correct. Further, certain NSPS make render the linking of different silos of information mandatory, for example through the requirement of linked bank accounts into which benefits are paid.

17. Another concern is the use of NSPS data for surveillance.[21] For example, in countries where access to NSPS requires persons to submit biometric data and photographs, this can be used to create police profiles. This leads to a likelihood of persons living in poverty – and therefore reliant of NSPS – being more likely to be targeted and arrested when, for example, exercising their civil and political rights, including criticising the government or protesting a lack of service delivery.[22]

18. As such, all processing of personal data must be done in a transparent manner that appropriately caters for the rights of affected persons, including the right to be notified, to be able to access the data held, to be informed of the purpose for which it is held and of any third parties with whom it is shared, to be able to rectify incorrect data, and to object to processing in appropriate circumstances.

---

[18] World Bank Group, 'Identification for development: Practitioner's guide (Draft for consultation), June 2019, p 115, accessible at http://id4d.worldbank.org/. As explained in the report, inclusion requires that where registration is outsourced, fee structures should incentivise universal coverage, including of remote and hard-to-reach populations; reliability requires that clear standards and oversight mechanisms must be in place to ensure quality in implementation; data protection requires that private companies involved in the identification system must be trusted and subject to national laws regarding privacy and data protection; and sustainability requires that requests for proposals should be structured in a way that ensures competition and avoids vendor and technology lock-in.

[19] Stephen Devereux and Katharine Vincent, 'Using technology to deliver social protection: Exploring opportunities and risks' in *Development in Practice*, vol. 20, 2010, accessible at https://gsdrc.org/document-library/using-technology-to-deliver-social-protection-exploring-opportunities-and-risks/.

[20] Digital Rights Foundation, 'DRF condemns yet another breach of NADRA database and demands strong data protection legislation', 28 May 2018, accessible at https://digitalrightsfoundation.pk/drf-condemns-yet-another-breach-of-nadra-database-and-demands-strong-data-protection-legislation/. As noted, in May 2018, the National Database and Registration Authority (NADRA) of Pakistan was hacked, and resulted in the loss of a significant amount of confidential data that was subsequently sold online.

[21] Surveillance in this regard takes a number of forms, including a person's whereabouts and behaviour. The scope of such surveillance is constantly increasing with the growing use of such technologies in public spaces and facial recognition technologies. For a practical illustration see, for example, Derechos Digitales, Fundación Datos Protegidos and Privacy International, 'Identification schemes' in *State of privacy: Chile*, January 2019, accessible at https://privacyinternational.org/state-privacy/28/state-privacy-chile.

[22] For an example of this from the United States of America, see Nathalie Méchal, 'First they came for the poor: Surveillance of welfare recipients as an uncontested practice' in *Media and Communication*, vol. 3, 2015 at pp 56-67, accessible at https://www.cogitatiopress.com/mediaandcommunication/article/view/268/268.

**POTENTIAL FOR DISCRIMINATION AND EXCLUSION IN THE USE OF ALGORITHMS**

19. Algorithmic discrimination and bias threatens to erode fair and equitable NSPS.[23] For example, when the Albanian government revised the cash benefit scheme – apparently to better target the poor and increase efficiency – this was done by creating a database and relying on a formula to determine who would benefit.[24] However, this scheme led to hundreds of low-income families being excluded, and raised concerns of being a way to reduce the persons receiving these benefits without having to provide reasons for the exclusion.[25]

20. It has been noted that, because machine-learning systems seek patterns in the data, it will use patterns in objectionable data to create predictive models for the future based on that data; this requires such technologies to be constantly trained and tested to guard against this.[26] If not, this risks a decision-making process that is discriminatory, lacking transparency and non-compliant with international human rights law.[27]

21. A key challenge is the under-representation of certain groups, including women, in the data.[28] In order to strike the correct balance between inclusion and data privacy, it has been suggested that feminist data practices, for example, include "efforts to expose and level algorithmic discriminations; increased attention to the rights and agency of those represented in the data; firm opposition to all non-consensual collection and use of data; and adequately safeguarding the data, privacy and anonymity of [affected persons]".[29] Such data practices may similarly be appropriate for other excluded groups.

**APPROPRIATE REGULATORY AND POLICY FRAMEWORKS**

22. States opting to rely on digital technologies in NSPS need clear, rights-based and transparent regulatory and policy frameworks to guide the development and use of such technologies in a manner that safeguards fundamental rights. While comprehensive data protection laws are a useful start, they are not the complete solution.[30] States should

---

[23] Nicole Shephard, 'Algorithmic discrimination and the feminist politics of being in the data' in *GenderIT.org*, 5 December 2016, accessible at https://www.genderit.org/node/4864/. As explained, the notion of algorithmic discrimination describes "instances where the outcomes of algorithmic decision making disadvantage, exclude, or disproportionately single out women, racialised groups, queers, trans folks, religious minorities, the poor and so on". See, also, Betsy Williams, Catherine Brooks and Yotam Shmargad, 'How algorithms discriminate based on the data they lack: Challenges, solutions and policy implications' in *Journal of Information Policy*, vol. 8, 2018 at pp 78-118, accessible at https://www.jstor.org/stable/10.5325/jinfopoli.8.2018.0078?seq=1&cid=pdf-reference#references_tab_contents.

[24] Vasilika Laçi, 'Using the internet to secure the rights of Roma and Egyptian communities in Albania' in in Alan Finlay and Deborah Brown (eds) *Global Information Society Watch 2016*, 2016 at p 182, accessible at https://www.giswatch.org/en/economic-social-and-cultural-rights-escrs/key-considerations-economic-social-and-cultural-rights-.

[25] Vasilika Laçi, above n 24. The explanations given to people left out of the scheme included, for example, that they were not eligible for cash benefits because they did not own a television set at their home.

[26] Esther Shein, above n 12.

[27] Jedrzej Niklas, above n 10 at p 187.

[28] Nicole Shephard, above n 23.

[29] Nicole Shephard, above n 23.

[30] Not all countries have such a law, and those that do have markedly differing levels of enforcement. Some countries also attempt to exclude the state from the ambit of data protection compliance; see, for example, section 3(5)(c) of the

develop specific regulatory and policy interventions that clearly build or supplement a rights-based framework into existing NSPS frameworks. This should include obligations on the state and third parties, justiciable rights, and appropriate safeguards for lawful processing of personal data in line with global best practice.

**MEANINGFUL ENGAGEMENT, IMPACT ASSESSMENTS AND REVIEW**

23. Meaningful engagement with persons directly affected by digital technologies in NSPS is imperative to ensuring that measures are suitable to the need, effective and will be utilised. This must not just be a tick-box exercise leading to predetermined outcomes.[31] It should also be conducted through the medium most accessible to the affected persons.[32]

24. Approaches to obtaining consent need to be overhauled. Persons accessing social security benefits typically live in low-income environments and require the benefits provided by the state to sustain themselves and their families. The likelihood is that consent would be granted out of concern of losing the benefits, notwithstanding the other rights that may be implicated. For example:

    24.1. In Chile, a biometric identification system was implemented for the school meal programme, requiring learners to provide their fingerprints to obtain the meal benefits.[33] While the Supreme Court ruled that the use of biometrics of minors must be subject to the consent of their parents or legal guardians,[34] the practical implication is that the children being fed is being made contingent on this consent being provided.

    24.2. In India, the Supreme Court ruled that Aadhaar enrolment could not be mandatory for the provision of public services.[35] There are now two options for obtaining the gas cylinders provided: the primary option is for the consumer who has an Aadhaar number; and the secondary option is introduced for the consumer who does not.[36] However, persons who had already linked their Aadhaar number

---

draft Data Protection Bill, 2018 in Pakistan, accessible at https://moitt.gov.pk/userfiles1/file/PERSONAL-DATA-PROTECTION-BILL-July-18-Draft.pdf.

[31] Albeit developed in a different context, the concept of 'free, prior and informed consent' is also relevant, and encompasses that "[t]he principles of consultation and consent together constitute a special standard that safeguards and functions as a means for the exercise of … substantive rights. It is a standard that supplements and helps effectuate substantive rights". See UN-REDD Programme, 'Guidelines on free, prior and informed consent', 2013, accessible at https://www.uncclearn.org/sites/default/files/inventory/un-redd05.pdf.

[32] For example, online consultations have limited utility for persons who are not digitally literate or do not have effective online access. Regard should also be had to the Responsible Data Principles, which include considerations of power dynamics; diversity and bias; precaution; standards and behaviour. See Responsible Data, 'RD 101: Responsible Data Principles', January 2018, accessible at https://responsibledata.io/2018/01/24/rd-101-responsible-data-principles/.

[33] NEC, 'NEC provides biometric identification solution for JUNAEB national school meal programme in Chile', 8 March 2017, accessible at https://www.nec.com/en/press/201703/global_20170308_03.html.

[34] Derechos Digitales, Fundación Datos Protegidos and Privacy International, above n 21.

[35] Kieran Clark, 'Estimating the impact of India's Aadhaar scheme on LPG subsidy expenditure' in *International Institute for Sustainable Development*, 16 March 2016, accessible at https://www.iisd.org/gsi/subsidy-watch-blog/estimating-impact-indias-aadhaar-scheme-lpg-subsidy-expenditure.

[36] Ministry of Petroleum and Natural Gas, 'PAHAL direct benefits transfer for LPG (DBTL) consumer scheme', undated, accessible at http://petroleum.nic.in/dbt/whatisdbtl.html.

prior to the amendment out of concern of losing the benefit are now unable to change to the secondary option.

25. In the context of data protection, consent has been explained by the Information Commissioner's Office as "giving people genuine choice and control over how you use their data. If the individual has no real choice, consent is not freely given and it will be invalid. This means people must be able to refuse consent without detriment, and must be able to withdraw consent easily at any time."[37] It is submitted that denying access to NSPS if unwilling to consent to the collection of personal data would be inimical to a rights-based approach.

26. Human rights impact assessments should be independently conducted and made publicly-accessible before the implementation of any digital technologies in NSPS. This is consonant with the Guiding Principles, which provides that such assessments should include all internationally-recognised human rights as a reference point as business enterprises may potentially impact any of these rights.[38] All determinations regarding the implementation of such technologies should be keenly informed by these assessments. Additionally, this implementation should be subject to ongoing monitoring and evaluation to assess whether the desired outcomes are being achieved.[39]

**RETROGRESSIVE MEASURES**

27. GC19 provides that there is a strong presumption that retrogressive measures to the right to social security are prohibited under the ICESCR. The state party has the burden of proving that the measures were introduced after careful consideration of all alternatives and duly justified by the totality of rights in the ICESCR.[40]

28. The use of digital technologies without appropriate safeguards, assessments and education raise serious concerns of denying access to NSPS and the right to social security. In the event that a state implements such technologies, regard must be had to whether this constitutes retrogressive measures – including the availability of alternatives and the genuine participation of affected groups – to ensure compliance with the ICESCR and other international obligations.

---

[37] Information Commissioner's Office, 'What is valid consent?', undated, accessible at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/.

[38] Guiding Principles, above n 17 at p 20.

[39] In Kenya, for example, it has been observed that the implementation of the NIS "has created new levels of bureaucracy and overlapping functions that delay service delivery". See Liz Orembo, above n 11. For example, after applying for a passport, one still has to present themselves with the application documents and queue to register biometric information.

[40] GC19 at para 42. This requires, among other things, a careful inquiry at whether (i) there was reasonable justification for the action; (ii) alternatives were comprehensively examined; (iii) there was genuine participation of affected groups in examining the proposed measures and alternatives; (iv) the measures were directly or indirectly discriminatory; (v) the measures will have a sustained impact on the realization of the right to social security, an unreasonable impact on acquired social security rights or whether an individual or group is deprived of access to the minimum essential level of social security; and (vi) whether there was an independent review of the measures at the national level.

29. These concerns are exacerbated through there being disproportionate exclusion of already marginalised groups, such as persons living in poverty, rural dwellers, women, children, migrants and transgender persons. For such persons – whose lived experiences may include cultural and social relegation in mainstream settings, economic exclusion and digital illiteracy – being required to use digital technologies in NSPS risks being a bridge too far for them to access the benefits to which they are entitled. Further, the mandatory requirements of linking biometric identification systems to accessing NSPS means that economically-vulnerable persons most frequently populate the databases owing to their need to access NSPS, and in some instances an unwillingness to be seen as challenging the status quo for fear of exclusion from NSPS.

30. Furthermore, given the inextricable link between privacy, status and social identity – and the different social identities that one chooses to present in different public settings – the practical reality for persons required to provide their personal data to access NSPS means that lower-income persons are less able to enjoy their privacy and choice of social identity than those with the economic means not to require access to NSPS. This creates an untenable outcome of economically-vulnerable persons being rendered more vulnerable through the forced disclosure of tranches of personal data.

**CONCLUSION**

31. The upcoming report is an important contribution as there appears to be a need for further research and multi-stakeholder engagement on this issue which implicates a wide range of rights, the extent of which has not yet been fully considered. Please feel free to contact us should you seek further information.[41] Kindly note that we have no objection to this submission being made accessible to the public.

[Ends.]

[41] For any further enquiries, please contact Deborah Brown at deborah@apc.org.