Privacy International's Submission to the UN Special Rapporteur on extreme poverty and human rights:

Input for the thematic report titled "Social protection: a reality check"[1]

17 December 2021

I. Background

Privacy International ("PI") is a London-based non-profit, non-governmental organization (Charity Number: 1147471) that works internationally to protect people's privacy, dignity, and freedoms. Through our work we aim to build a world where technology will empower and enable us, not exploit our data for profit and control. [2] PI works globally with partners[3] to challenge overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

PI previously engaged with the UN Special Rapporteur on extreme poverty and human rights when the 2019 annual thematic report related to digital welfare states was being developed. PI contributed a submission, participated in further consultation meetings, and supported the launch of the 2019 annual thematic report.[4]

It is against this background that PI welcomes the opportunity to engage once again with the mandate by submitting comments, evidence, and recommendations to the UN Special Rapporteur on extreme poverty and human rights, Mr. Olivier de Schutter. We hope that our input will contribute to the forthcoming report, "Social protection: a reality check."

This submission builds on PI's and our global partners' research and reporting around the use of data and technology in the design, delivery and management of social protection programmes. In this submission, we aim to outline developments from around the world as they relate to key areas of concern that are being explored by the mandate for its report to the 50th session of the Human Rights Council.

---

[1] UN OHCHR, "Call for submissions: Thematic report to the UN Human Rights Council, 'Social protection: a reality check,' 2021, accessed online: https://www.ohchr.org/EN/Issues/Poverty/Pages/SocialProtection-RealityCheck.aspx

[2] For more information about PI, please visit our website at www.privacyinternational.org and in particular: https://privacyinternational.org/strategic-areas

[3] For more information about our global network of partners, please see: https://privacyinternational.org/where-we-work

[4] See: Privacy International, Submission on digital technology, social protection and human rights, May 2019, available online at: https://privacyinternational.org/advocacy/2996/privacy-internationals-submission-digital-technology-social-protection-and-human, and Privacy International, "UN Special Rapporteur warns that beneficiaries are forced to give up their right to privacy and data protection to receive their right to social security", Press release, 17 October 2019, available online at: https://privacyinternational.org/press-release/3261/un-special-rapporteur-warns-beneficiaries-are-forced-give-their-right-privacy

II. Introduction

In order to understand the full range of obstacles that individuals and households face when seeking to access social protection, policymakers and other actors with a decision-making mandate in this sector must consider and assess the systemic problems emerging from the increased digitalisation, automation and intrusive data collection in the "digital welfare state". The fact that the 2019 thematic report of the UNSR was dedicated to this issue illustrates the importance of our concerns with these developments.[5]

These developments have been observed across the world, including in Colombia, Paraguay, Brazil,[6] the United Kingdom, Uganda and India to name a few.[7] The Covid-19 pandemic has acted as a catalyst for the deployment of digital social protection programmes. As a result, the concerns and issues presented in this submission are timely and it is increasingly urgent for them to be addressed.[8]

In our submission, we have sought to answer two key questions from the Special Rapporteur's call for submissions: firstly, "what obstacles prevent eligible individuals and households from accessing benefits they are entitled to?" Second, "to what extent do conditionalities attached to the granting of social protection benefits undermine social protection systems? What is the impact of such conditionalities on people who experience poverty?"

With the aim of answering these questions, our submission focuses on how the implementation of the "digital welfare state" has negatively impacted access to social protection in three fundamental ways:

i. first, systems that are "digital-by-default" and rely on automated decision-making and profiling have led to discrimination and exclusion and as a result, individuals and households from marginalised communities face significant obstacles when seeking to access benefits;
ii. second, intrusive conditionalities are creating legal and technical barriers for people, preventing them from accessing social protection programmes;
iii. third, surveillance and a lack of guaranteed data protection have led to serious and unjustified interferences with affected individual's fundamental right to privacy and dignity, therefore undermining public trust in social protection systems.

At the end of our submission, we provide some detailed recommendations, but we would like to highlight that our key recommendation to the Special Rapporteur is to develop strategies that will integrate critical questions about the human rights

[5] UN General Assembly, "Report of the Special Rapporteur on extreme poverty and human rights," A/74/493, 11 October 2019
[6] InternetLab, "Brazil's Bolsa Familia Program: the impact on privacy rights", 13 May 2020, published on PI's website and available online at: https://privacyinternational.org/long-read/3758/brazils-bolsa-familia-program-impact-privacy-rights
[7] See: Privacy International's submission on digital technology, social protection and human rights, May 2019, https://privacyinternational.org/advocacy/2996/privacy-internationals-submission-digital-technology-social-protection-and-human; Joints submission to the Special Rapporteurship on Economic, Social, Cultural and Environmental Rights of the Inter-American Commission on Human Rights (IACHR) regarding the situation of Economic, Social, Cultural and Environmental Rights (ESCR) in the region, November 2019, available online at: https://privacyinternational.org/node/3361
[8] Privacy International, "
A year into the pandemic, welfare "innovation" continues to penalise the poor", 22 June 2021, available online at: https://privacyinternational.org/long-read/4582/year-pandemic-welfare-innovation-continues-penalise-poor

implications associated with digital social protection programmes. Specifically, to ensure that certain categories of individuals and households, especially those who rely on social protection programmes for their survival, are not disproportionately excluded or disadvantaged from accessing social protection benefits as a result of invasive conditions, operational failures in tech-based solutions and automated decision-making, and that they are not subject to arbitrary monitoring and surveillance. This would include recommending that the development and implementation of digital social protection programmes be informed by comprehensive human rights due diligence mechanisms, and builds in, at every stage, human oversight, support, and appeal mechanisms.

III. Discrimination and Exclusion by default

The risks of discrimination and exclusion triggered by the digitalisation, automation and intrusive data processing of social protection programmes have been well-documented.[9] We have outlined some of these in this section.

Digital divide: Social protection systems which are "digital-by-default" exclude individuals who are not digitally literate, as well as households that do not have access to mobile phones and computers, a stable internet connection and electricity. This is exacerbated when systems are poorly designed and do not account for case-by-case variations in digital literacy and familiarity with online data sharing. This has an obvious exclusionary effect: if social protection systems are difficult to use, people who are in vulnerable or precarious situations may not be able to access benefits they are entitled to. Additionally, poorly designed systems can lead to accidental non-compliance and system failures which further exclude people from accessing life-saving benefits. This kind of exclusion has been widely documented under India's Aadhaar system.[10]

Automation: At every stage of the decision-making process in the provision of social services, automation is being built into the system. From automated digital identity verification,[11] to eligibility assessments and so-called 'fraud' detection mechanisms.[12] Automating these processes while failing to build in sufficient safeguards which require human intervention and review has led to discrimination and unjust sanctions against people who are eligible for support. For example, in the UK, the public body responsible for overseeing access to welfare and social protection (the Department for Welfare and Pensions, "DWP") is facing legal action from a rights group represented disabled people after "mounting testimony from disabled people [was received] that they were being disproportionately targeted for benefit fraud investigations."[13] In Colombia, Fundación Karisma revealed the role that Experian, an Irish-domiciled multinational consumer credit reporting company, is playing in assessing the income of people registering for benefits, and in cross-

[9] UN General Assembly, "Report of the Special Rapporteur on extreme poverty and human rights," A/74/493, 11 October 2019

[10] Shiv Sahay Singh, "Death by digital exclusion?: on faulty public distribution system in Jharkhand", 13 July 2019, accessed online: https://www.thehindu.com/news/national/other-states/death-by-digital-exclusion/article28414768.ece; See also: Access Now, "Busting the Dangerous Myths of Big ID Programs: Cautionary Lessons from India", October 2021, accessed online: https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf.

[11] Privacy International, "Exclusion by design: how national ID systems make social protection inaccessible to vulnerable populations" 29 March 2021, accessed online: https://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessible.

[12] Privacy International, "Stage 3: The policing of social benefits: punishing poverty," 7 August 2019, accessed online: https://privacyinternational.org/node/3114

[13] Michael Savage, "DWP urged to reveal algorithm that 'targets' disabled for benefit fraud."

checking the information that is being provided by individuals at the point of enrolment. This raised two key concerns: firstly, that a private company was involved in processing this kind of personal information, and second, that there was limited scrutiny, due diligence and transparency around how the information provided by Experion was being used to make life-changing decisions.[14]

Companies are developing increasingly advanced was of implementing algorithmic data analysis in order to profile individuals and make predictions about their trustworthiness or their risk profile when it comes to committing fraud.[15] '

It has been widely recognised that these practices have had discriminatory effects.[16] Using personal data points about individuals who are seeking to access social protection, such as their sex, age, place of residence, immigration status, ethnicity, history of employment, marriage status etc., to 'profile' them increases the risk of discrimination and exclusion against specific communities. This was recently recognised by a Dutch court after assessing the impact of a risk profiling method known as "System Risk Indicator" ("SyRI") which was being used by the Dutch government to detect individual risks of welfare fraud.[17] This profiling method "was primarily deployed in poor neighbourhoods" where "many residents are more likely to be immigrants and/or from racial and ethnic minority backgrounds."[18]

Further, the risk models that were being relied on were secretive, and made it "impossible for citizens to 'defend themselves against the fact that a risk report had been submitted against them."[19] Using software which analyses data to profile welfare recipients without building-in safeguards that correct for system errors or unlawful discrimination can unfairly exclude entire groups of people from accessing social protection by making incorrect determinations about eligibility,[20] miscalculating welfare benefits, and incorrectly flagging individuals for "fraud".[21]

IV. Intrusive Conditionalities: barriers to access

While it may be necessary for governments and international development organisations implementing social support programmes to set conditions for access and eligibility, we are concerned by the overly invasive and onerous conditionalities imposed on those seeking to enrol in such programmes. These not only amount to interferences with potential beneficiaries' inherent right to privacy but may also unduly limit the right to access social security and the right to the

[14] See: https://privacyinternational.org/long-read/4144/benefitting-whom-overview-companies-profiting-digital-welfare
[15] See for example Singapore-based start-up LenddoEFL using behavioural traits and smartphone habits for credit scoring: https://privacyinternational.org/examples/3145/startups-use-behavioural-data-and-smartphone-habits-credit-scoring.
[16] See: UN General Assembly, "Report of the Special Rapporteur on extreme poverty and human rights," A/74/493, 11 October 2019, and United Nations High Commissioner for Human Rights, "The right to privacy in the digital age", A/HRC/48/31, September 2021
[17] Privacy International, "The SyRI case: a landmark ruling for benefits claimants around the world", 20 February 2020, available online at: https://privacyinternational.org/news-analysis/3363/syri-case-landmark-ruling-benefits-claimants-around-world; and Tijmen Wisman, "The SyRI Victory: Holding Profiling Practices to Account", 23 April 2020, accessed online: https://digitalfreedomfund.org/the-syri-victory-holding-government-profiling-to-account/7/
[18] Digital Freedom Fund, "NJCM, Platform Bescherming Burgerrechten and others v the Netherlands (the SyRI case): Case facts at a glance," accessed online: https://digitalfreedomfund.org/case-analyses/njcm-platform-bescherming-burgerrechten-and-others-v-the-netherlands/.
[19] Ibid, n11.
[20] Ibid, n3 at paras. 21 and 22, page 9.
[21] Privacy International, "Stage 3 – The policing of social benefits: punishing poverty", 7 August 2019, accessed online: https://privacyinternational.org/node/3114.

protection of other human rights. This is because invasive and onerous conditionalities may deter people who are vulnerable to persecution or deportation, such as refugee and migrant populations or people from marginalised groups, from accessing life-saving social services. [22]

ID as a pre-requisite for accessing social protection: In collaboration with our global partners, we have undertaken extensive research and analysis on the exclusionary effects of making access to social protection conditional on producing forms of identification. A key problem with making ID a conditionality of access to social protection is that often people who are already in precarious economic conditions, such as women, the elderly, asylum seekers, refugees or stateless persons, are excluded from accessing ID.[23]

Such instances of exclusion have been well-documented in countries such as Uganda[24] and India. In India, for example, it was deemed unconstitutional to require people to provide Aadhaar ID cards to access the welfare system[25]. In the USA, where than 21 million American adults (which is 11% of USA citizens) do not have non-expired government-issued photo identification, a requirement to produce any form of identification would clearly exclude a substantial number of people. Other examples include Chile,[26] Indonesia,[27] Venezuela, Bolivia,[28] and the Philippines[29]. The exclusionary effects of such ID requirements can also be seen in the UK, where people who were legitimately claiming universal credit saw their "awards summarily terminated and [were] told they must repay all of the money- in some cases as much as GBP 13,000" simply because they failed to respond to an online notice to supply proof of identification.[30]

V. Surveillance of beneficiaries: policing whether they "deserve" support

[22] Ibid n 3, at para. 7, page 5.
[23] Privacy International, "Exclusion by design: how national ID systems make social protection inaccessible to vulnerable populations", 29 March 2021, accessed online: https://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessible
[24] Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness, "Chased Away and Left to Die", June 2021, available online at: https://www.unwantedwitness.org/chased-away-and-left-to-die-new-human-rights-report-finds-that-ugandas-national-digital-id-system-leads-to-mass-exclusion/
[25] Privacy International, *Initial analysis of Indian Supreme Court decision on Aadhaar,* 26 September 2019. Available at: https://privacyinternational.org/feature/2299/initial-analysis-indian-supreme-court-decision-aadhaar.
[26] See: Campaign "#NodoymiRUT" by Fundadción Datos Protegidos. Available at: https://datosprotegidos.org/no-doy-mi-rut/; Privacy International, *Exclusion and identity: life without ID*, 18 December 2019. Available at: https://privacyinternational.org/feature/2544/exclusion-and-identity-life-without-id; and Privacy International, *Exclusion and identity: life without ID*, 18 December 2019. Available at: https://privacyinternational.org/feature/2544/exclusion-and-identity-life-without-id; Privacy International, Liliana: "If you don't have RUT, you can't do it.". Available at: https://privacyinternational.org/case-studies/2545/liliana-if-you-dont-have-rut-you-cant-do-it; Privacy International, Carolina: "You are legal, but on the other hand you're not." Available at: https://www.privacyinternational.org/case-studies/2546/carolina-you-are-legal-other-hand-youre-not.
[27] Jakarta Global, *Home Affairs Minister Urges People to Apply for e-KTP Immediately*, 23 August 2016. Available at: https://jakartaglobe.id/context/home-affairs-minister-urges-people-apply-e-ktp-immediately.
[28] Jamila Venturini, "Derechos Digitales publish a report on ID systems and social protection in Venezuela and Bolivia", 13 April 2021, available online at: https://privacyinternational.org/news-analysis/4478/derechos-digitales-publish-report-id-systems-and-social-protection-venezuela-and
[29] PhilSys, Philippine Statistics Authority. Republic of the Philippines. Available at: https://psa.gov.ph/philsys.
[30] Patrick Butler, "Universal Credit claimants were sent unlawful demands to repay, says charity," 13 November 2021, accessed online: https://www.theguardian.com/society/2021/nov/13/universal-credit-claimants-were-sent-unlawful-demands-to-repay-says-charity.

"Welfare surveillance" is closely linked to intrusive data collection by authorities that are responsible for providing social protection. One way to define "welfare surveillance" is as an aggregation of a variety of covert and overt intelligence gathering by caseworkers about any individual who applies for, or receives, social protection entitlements.[31] This has a chilling effect and may deter individuals from even applying to benefit from social protection programmes because they are concerned about being placed under increased levels of scrutiny by the government. Welfare surveillance is a well-documented form of social policing, which is commonplace across the United States,[32] the UK[33] and other countries in Europe.[34] It is also part of the policy recommendations that the World Bank includes when providing low-interest loans to governments for social protection provisions.[35]

In the UK, for example, asylum seekers with ongoing applications are entitled to debit cards known as 'Aspen Cards' to pay for basic subsistence such as food and transport. However, the UK's Home Office uses these cards to monitor the expenses of the cardholders and track their location. Through research and interviews with asylum seekers, PI documented how "monitoring and surveillance of people's Aspen Card usage (alongside other Home Office reporting obligations, check-ins with housing officers and other forms of immigration enforcement) put extreme psychological pressure on people seeking asylum in the UK."[36]

In countries such as Jordan, for example, many informal workers are also migrants without settled status or asylum seekers without the legal right to undertake certain kinds of work.[37] Their fear of government surveillance and ultimately, deportation, could amount to a significant deterrent to update social protection that they are eligible for. For example, when the World Bank implemented its "Emergency Cash Transfer" response project in Jordan, the programme deployed software which enabled data sharing about beneficiaries between numerous government bodies.[38] If social protection programmes fail to guarantee that informal workers' information will *not* be shared and used by government agencies - such as law

[31] See: https://privacyinternational.org/news-analysis/3113/stage-2-maintaining-social-benefits-under-surveillance-and-control and https://privacyinternational.org/node/3114

[32] See for example, Michele. E. Gilman, "Welfare, Privacy and Feminism" (2008) University of Baltimore Law Forum, accessed online: https://scholarworks.law.ubalt.edu/lf/vol39/iss1/4/; See also, Virginia E. Eubanks, "Technologies of Citizenship: Surveillance and Political Learning in the Welfare System" (2006).

[33] Privacy International, "Shedding light on the DWP", 14 February 2021, accessed online: https://privacyinternational.org/long-read/4395/shedding-light-dwp-part-1-we-read-uk-welfare-agencys-995-page-guide-conducting; See also, Privacy International, "Is Your Local Authority Looking at Your Facebook Likes?, May 2020, accessed online: https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020_0.pdf; Statement on Visit to the United Kingdom, by Professor Philip Alston, United Nations Special Rapporteur on extreme poverty and human rights, 16 November 2018. Available at: https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23881&LangID=E.

[34] Catrine S. Byrne & Julia Sommer, "Is the Scandinavian Digitalisation Breeding Ground For Social Welfare Surveillance?" 27 May 2019, accessed online: https://dataethics.eu/is-scandinavian-digitalisation-breeding-ground-for-social-welfare-surveillance/.

[35] See for example, World Bank, "Lebanon Emergency Crisis and Covid-19 Response Social Safety Net Project (ESSN)", 12 January 2021, accessed online: https://www.worldbank.org/en/country/lebanon/brief/lebanon-emergency-crisis-and-covid-19-response-social-safety-net-project-essn

[36] Privacy International, "What is an Aspen Card and why does it need reform?" 23 February 2021, accessed online: https://privacyinternational.org/explainer/4425/what-aspen-card-and-why-does-it-need-reform

[37] Shaddin Almasri, "Daily-wage workers and government COVID-19 responses in Jordan", 8 July 2020, accessed online: https://www.compas.ox.ac.uk/2020/daily-wage-migrant-workers-and-government-covid-19-responses-in-jordan/.

[38] World Bank, "Project Information Document – Jordan Emergency Cash Transfer COVID-19 Response", 23 May 2020, accessed online: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/328901590211842779/project-information-document-jordan-emergency-cash-transfer-covid-19-response-project-p173974.

enforcement or immigration enforcement, their fear of deportation action may act as a barrier to accessing social welfare.

VI. Conclusion and recommendations

The Special Rapporteur's thematic report is an important opportunity to highlight the policy implications of over-reliance on unchecked data collection, analysis and automation in relation to social welfare. In order to identify existing and emerging obstacles that individuals and households face in seeking to access social protection, it is essential to address issues related to digitalisation and to build on, as well as update, the findings from the mandate's 2019 report. This will further assist stakeholders to propose recommendations and solutions to overcome these issues.

We hope the UNSR will take the opportunity to integrate critical questions about the use of digital technologies in the design and delivery of social protection into policymaking. These issues are becoming more pressing as socio-economic crises unfold globally alongside the Covid-19 pandemic. Further, we believe that this report may reflect upon ongoing efforts in the European Union and elsewhere to regulate artificial intelligence in order to ensure that the right to social security is effectively protected.[39]

We hope that the UN Special Rapporteur on extreme poverty and human rights will further explore the areas we have highlighted in our submission, and that the report develops recommendations to governments, companies and international organisations involved in the funding and/or delivery of social services.

Finally, we recommend that the report include recommendations aimed at:

- Promoting a comprehensive human rights approach in the design and deployment of digital social protection programmes, as well as describing the necessary measures to achieve this, including, for example 'human rights by design' and human rights impact assessments,
- Demanding that any conditions to accessing social protection programmes are necessary and proportionate and do not create onerous and invasive barriers for eligible individuals. Conditions should not disproportionally disadvantage marginalised groups and people who are most in need of welfare assistance,
- Establishing the need for a human rights-based approach to all AI applications in social protection programmes and giving careful consideration to the risks and the circumstances in which such automated decision-making should not be permitted,
- Requiring appropriate safeguards to be put in place by governments, companies, and other actors such as funders of digital social protection programmes. This includes effective and clear articulation of each actor's role and responsibilities, including, due diligence and oversight to ensure specific categories of beneficiaries are not disproportionately affected,
- Ensuring that effective accountability mechanisms are in place to guarantee meaningful access to redress and appeal mechanisms,

[39] Human Rights Watch, How the EU's Flawed Artificial Intelligence Regulation Endangers the Social Safety Net: Questions and Answers, 10 November 2021, accessed online: https://www.hrw.org/news/2021/11/10/how-eus-flawed-artificial-intelligence-regulation-endangers-social-safety-net?utm_source=POLITICO.EU&utm_campaign=25c6120bdd-EMAIL_CAMPAIGN_2021_11_17_09_59&utm_medium=email&utm_term=0_10959edeb5-25c6120bdd-190000757#_Part_I_:_Algorithmic

- Encouraging national human rights institutions to integrate questions of technology, security and privacy within their work on monitoring and promoting socio-economic rights in their methodologies and strategies,
- Presenting an effective public policy around social protection which engenders trust and does not lead to a chilling effect on access, by preventing intrusive surveillance and monitoring practices.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471