PRIVACY INTERNATIONAL

May 2019

Privacy International's submission on digital technology, social protection and human rights

Privacy International welcomes the decision of the UN Special Rapporteur on extreme poverty and human rights, Philip Alston, to dedicate a thematic report on digital technology, social protection and human rights. This submission aims to outline case-studies from around the globe as they relate to key areas of concern observed by Privacy International.[1]

I. Introduction of digital technologies in national social protection systems

Social protection programmes which integrate technology have been in place for a while: with the beginning of e-health programmes in the late 1990s,[2] the deployment of biometric systems to access food,[3] national health insurance programmes, smart card for recipients of welfare,[4] and biometric national ID systems,[5] amongst other examples.[6] But what has changed over the last decade is the advancement in technology and data processing and exploitation capabilities which are providing ever increasing powers to collect, process and gather intelligence.

[1] Privacy International (PI) PI was established in 1990 as a non-profit, non-governmental organisation based in London, working with partners around the globe, at the intersection of modern technologies and rights. It envisions a world in which the right to privacy is protected, respected, and fulfilled. PI believes that privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. In order for individuals to fully participate in the modern world, developments in law and technologies must strengthen and not undermine the ability to freely enjoy this right. We are building the global movement because people must have access to privacy protection without regard to citizenship, race and ethnicity, economic status, gender, age, or education. https://privacyinternational.org/

[2] Vincenzo Della MEa, "What is e-Health (2): The death of telemedicine", J Med Internet Res (2001). Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1761900/.

[3] For example, in Venezuela, see: López, V., *Venezuela to introduce new biometric card in bid to target food smuggling*, The Guardian, 21 August 2014. Available at: https://www.theguardian.com/world/2014/aug/21/biometric-venezuela-food-shortages-smuggling-fingerprints, and Botswana, see: SmartSwitch, *The Electronic Food Coupon System – an African Success Story*. Available at: http://www.smartswitch.co.bw/fcSuccess

[4] Mastercard Press Release: *Ten Million SASSA MasterCard Cards Issued to South African Social Grant Beneficiaries*. Available at: http://newsroom.mastercard.com/press-releases/ten-million-sassa-mastercard-cards-issued-to-south-african-social-grant/.

[5] These are mandatory to access social protection programmes in India, Peru, Pakistan, for example.

[6] The types of "IT" or "ICT" uses in management and support of social protection policies have included "Management Information Systems, automated contribution collection and benefit administration, telephone claim filing, or intelligent job-matching systems." See: *Costs and Benefits of Information Technology in Social Protection*, Knut Leipold, HDNSP, The World Bank, 2000, p. 4. Available at: http://documents.worldbank.org/curated/en/548541468134394335/pdf/406420IT0CostsBenefits01PUBLIC1.pdf.

Newly established or reformed social protection programmes have gradually become founded and reliant on the collection and processing of vast amounts of personal data; often access and management is tied to the provision of unique identifier; and increasingly the models for decision-making include data exploitation and components of automated-decision making and profiling.

ID requirements

Digital identity systems raise some key questions in relation to the rights of individuals and the protection of their autonomy and dignity, as well as to the security and integrity of the data and the infrastructure put in place.[7]

This is why we are particularly concerned with the emerging practice to connect national identity with social protection programmes and in particular when making the former a requirement for the latter whether it is a requirement in law or in practice.

India: Aadhaar, India's national identity system established in 2010, is mandatory to access welfare system. Worryingly, the Supreme Court ruled that the system was constitutional.[8] Government subsidies are processed under the Direct Benefit Transfer scheme,[9] which requires citizens to have a bank account and to ensure that their Aadhaar number is linked to their bank account so they can receive subsidies. While not currently mandatory to access healthcare services, Aadhaar is increasingly used to manage access to health care services.[10] The National Aids Control Organisation has also been encouraging Indian states to collect the Aadhaar numbers of people accessing HIV treatments from antiretroviral therapy centres.[11]

USA: In the USA, people can have difficulties in accessing benefits because they lack certain forms of ID as some states require government-issued photo identification before recipients can collect public benefits. More than 21 million American adults, which is 11% of USA citizens, do not have non-expired government-issued photo identification, and it is disenfranchised Americans who are least likely to have such identification.[12]

---

[7] As demonstrated by Privacy International and its Network's work in this area. See: Privacy International, Identity, Topic Page. Available at: https://privacyinternational.org/topics/identity.

[8] 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.

[9] Jumar, S., *Want to Avail Government Subsidies? Provide Aadhaar and Get it Easily*, PaisaBazaar, 1 May 2018. Available at: https://www.paisabazaar.com/aadhar-card/want-to-avail-government-subsidies-provide-aadhaar-and-get-it-easily/.

[10] In 2018, the health ministry issued a statement to clarify that Aadhaar was "desirable" but mandatory to access a 5-rupee insurance cover for hospitalisation under the Ayushman Bharat scheme. See: Kaul, R., *Aadhaar desirable, not must for Rs 5 lakh healthcare scheme, says Centre*, Hindustantimes, 12 July 2018. Available at: https://www.hindustantimes.com/india-news/aadhaar-desirable-not-must-for-rs-5-lakh-healthcare-scheme-says-centre/story-mvQwqSKzDFYE0rhxqLFbLO.html

[11] Rao, M*., Why Aadhaar is prompting HIV positive people to drop out of treatment programmes across India*, Scroll, 17 November 2017, Scroll. Available at: https://scroll.in/pulse/857656/across-india-hiv-positive-people-drop-out-of-treatment-programmes-as-centres-insist-on-aadhaar

[12] Brennan Centre for Justice, *Citizens Without Proof: A Survey of Americans' Possession f Documentary Proof of Citizenship and Photo Identification,* November 2017. Available at: https://www.brennancenter.org/sites/default/files/legacy/d/download_file_39242.pdf

Chile: A 9-digit number is issued as part of the birth registration process – the RUN (Rol Único Nacional – Unique National Number in Chile. This is the number is featured on the Chilean ID cards. However, the exact same number is more commonly known as the "RUT" (Rol Único Tributario – Unique Tax Number) – a Chilean individual's RUT is identical to their RUN. Having a RUT number is necessary for various activities from opening a bank account to getting health insurance. It is also necessary for the signing of most legal contracts, including employment, housing, and marriage.[13]

Indonesia: The e-KPT (Kartu Tanda Penduduk which literally translates as 'Resident Identity Card'), in Indonesia, is needed in order to obtain a state health insurance card, that is required to gain access to free health insurance, as well as a wide range of public health services.[14]

Philippines: In August 2018, the Philippines adopted a new law introducing a new national ID system, the Philippine Identification System (PhilSys).[15] The system has been set-up to be used for various purposes including the application for eligibility, services and access to social welfare as well as benefits granted by the government, admission in schools and public hospitals.[16]

Biometrics

Increasingly biometric technology is integrated within social protection programmes.[17] As in other sectors such as the development and humanitarian sector, the given justifications vary but include preventing fraud, duplication, and even empowerment of individuals.

In addition to national ID systems which often require biometrics, there are also parallel biometric social protection programmes being deployed. For instance, in Ireland, benefits claimants are expected to register for a Public Services Card (PSC)[18] in order to access benefits. PSC users are expected to have their photographs taken in department offices,[19]

[13] 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.

[14] 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.

[15] Foundation for Media Alternatives, *The National ID Debate: Is the Philippines Ready?,* Available at: https://www.fma.ph/resources/resources-on-privacy/national-id-system/

[16] See: PhilSys, Philippine Statistics Authority. Republic of the Philippines. Available at: https://psa.gov.ph/philsys.

[17] Sepúlveda, M.C., *Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection*, ESS – Working Paper No. 59, Social Protection Department, International Labour Office, Geneva. Available at: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---soc_sec/documents/publication/wcms_631504.pdf.

[18] Farries, E., *Bartering your privacy for essential services: Ireland's Public Services Card*, 16 April 2018. Available at: https://digitalfreedomfund.org/bartering-your-privacy-for-essential-services-irelands-public-services-card/2/.

[19] Kane, C., Facial recognition tool used to expose 155 cases of welfare fraud, The Irish Times, 7 February 2017. Available at: https://www.irishtimes.com/news/crime-and-law/facial-recognition-tool-used-to-expose-155-cases-of-welfare-fraud-1.2967045.

which is then digitally captured along with their signature.[20] The National Board of Scholarships and School Aid (Junaeb) in Chile has deployed facial recognition programmes to deliver meals at thirty schools in three cities across the country.[21]

E-programmes

Across the world, e-government systems have been emerging from the last three decades to regulate government to citizen interaction and these are predicted to grow.[22] These have been deployed across the world including for the delivery of public services such as social protection such as the benefits.gov in the USA,[23] and e-health in Jordan[24] and the 'carpeta cuidadana' (citizen folder) in Colombia.[25]

Smart (debit) cards

Often the result of public-private partnerships, social protection programmes such as benefits systems have taken the form of smart (debit) cards. Such systems were deployed until recently in South Africa[26] in partnership with Mastercard, and in Bangladesh, as part of the USAID supported the Access to Information (a2i) programme[27]. The government of Bangladesh has built a system to allow citizens to receive their welfare payment on a pre-paid debit card given to them at the Bangladesh Post Office after having been registered with their biometric data.

Digital, AI and automation

In some countries such as the United Kingdom and the USA, governments are deploying digital welfare systems which are increasingly designed to integrate automated systems,

---

[20] Lillington, K., Wary of the Public Services Card? You have good reason to be, The Irish Times, 11 January 2018. Available at: https://www.irishtimes.com/business/technology/wary-of-the-public-services-card-you-have-good-reason-to-be-1.3351106.

[21] Bastarrica, D., *Junaeb se llena de críticas por aplicación de biometría facial para entregar alimentos*, 17 January 2019. Available at: https://www.fayerwayer.com/2019/01/junaeb-biometria-facial-alimentos/.

[22] Bhattarai, T.N., *Emerging trends in the use of technology as. Driver of the transition to formality: Experiences from Asia and the Pacific, ILO Asia-Pacific Working Paper Series, December 2018, pp. 3.* Available at: https://www.ilo.org/wcmsp5/groups/public/---asia/---ro-bangkok/---sro-bangkok/documents/publication/wcms_655243.pdf.

[23] See: Benefits.gov. Available at: https://www.benefits.gov/.

[24] See: Electronic Health Solution International. Available at: http://ehs-int.com/about-hakeem.

[25] See: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombi, MinTIC publica para comentarios el borrador de decreto sobre lineamientos generales del Sistema de Información Clínica y Laboral. Available at: https://www.mintic.gov.co/portal/604/w3-article-61798.html; Fundación Karisma , *Otras historias, el lanzamiento de Fundación Karisma en el marco del Día Internacional de internet*. Available at: https://karisma.org.co/otras-historias-el-lanzamiento-de-fundacion-karisma-en-el-marco-del-dia-internacional-de-internet/.

[26] Mastercard, *Ten Million SASSA MasterCard Cards Issued to South African Social Grant Beneficiaries, Press Release*. Available at: https://newsroom.mastercard.com/press-releases/ten-million-sassa-mastercard-cards-issued-to-south-african-social-grant/; Mastercard, *SASSA Social Benefits Card in South Africa*. Available at: https://www.mastercard.us/content/dam/mccom/en-us/documents/sassa-case-study.pdf; Burt, C., *South African biometric grant system suspended to end public sector workers' strike*, Mastercard, 12 October 2018. Available at: https://www.biometricupdate.com/201810/south-african-biometric-grant-system-suspended-to-end-public-sector-workers-strike.

[27] Chambers, J., and Rohaida, N., Seriously, *Bangladesh is the country to beat on e-payments*, GovInsider, 2 May 2017. Available at: https://govinsider.asia/smart-gov/bangladesh-a2i-mobile-payments/.

often in parallel to non-automated elements.[28] Automated components are primarily seen in the registration and eligibility decision-making process as seen with the Universal Credit and the Real Time Information (RTI) system of the UK Her Majesty's Revenue and Customs (HMRC) and fraud investigation, for example the UK Department of Work and Pension's 'Analysis & Intelligence Hub' and 'Risk Intelligent Service'.

Another area which has emerged is the use of artificial intelligence to identify children who may be at risk of harm before they are harmed. Automated programmes have been deployed aimed at identifying families needing attention from child services as seen in the UK[29], and to identify children at greatest risk for abuse and neglect in New Zealand.[30]

II. Human rights concerns in connection with digital technologies in social protection systems

The use of technology in social protection systems raises, among others, some key concerns in relation to the protection, respect and promotion of the right to privacy as provided for under Article 17 of the International Covenant on Civil and Political Rights and Article 12 of the Universal Declaration of Human Rights.[31] Beyond the failure to protect individuals and their data as they interact with social protection programmes,[32] these programmes have also implications for non-discrimination and equality.[33] There is no question that technology can help governments tackle some key challenges in the provision of social protection services, but safeguards and due process guarantees need to be taken into account from the onset in order to identify and mitigate risks. Otherwise, the same programmes that are intended to facilitate social protection will amplify pre-existing shortcomings and injustice.

Governments have a positive obligations to uphold economic, social and cultural rights, and these means that they must refrain from any violations, prevent third parties from violating,

---

[28] See: 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.

[29] McIntyre, N., and Pegg, D., *Councils use 377,000 people's data in efforts to predict child abuse*, The Guardian, 16 September 2018. Available at: https://www.theguardian.com/society/2018/sep/16/councils-use-377000-peoples-data-in-efforts-to-predict-child-abuse.

[30] Hurley, D., *Can an Algorithm Tell When Kids Are in Danger?*, 2 January 2019. Available at: https://www.nytimes.com/2018/01/02/magazine/can-an-algorithm-tell-when-kids-are-in-danger.html.

[31] See: International Covenant on Civil and Political Rights. Available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx; Sepúlveda, M.C., *Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection*, ESS – Working Paper No. 59Social Protection Department, International Labour Office, Geneva. Available at: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---soc_sec/documents/publication/wcms_631504.pdf; Statement on Visit to the USA, by Professor Philip Alston, United Nations Special Rapporteur on extreme poverty and human rights, 15 December 2017. Available at: and https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22533.

[32] Privacy International, The Keys to Data Protection: A guide for policy engagement on data protection. Available at: https://privacyinternational.org/data-protection-guide.

[33] OHCHR, Key concepts on ESCRs – What are the obligations of States on economic, social and cultural rights? Available at: https://www.ohchr.org/EN/Issues/ESCR/Pages/WhataretheobligationsofStatesonESCR.aspx.

and take necessary measures to progressively realise them.[34] What can be observed is that in practice the way social protection programmes are designed and implemented are raising some key questions around privacy and security but also the enjoyment of economic, social and cultural rights with observed risks of discrimination and exclusion.[35] Little or no measures are taken to ensure third-parties, such as companies that develop these programmes, often involved through public-private partnerships, are not undermining the rights of individuals. There are concerns with how private actors reconcile this sort of initiatives with their commercial interests.[36] The lack of integration of privacy, data protection and security within this sector means that individuals are currently having to accept a trade-off between accessing social protection programmes and their fundamental right to privacy but also non-discrimination, amongst others.

Risks and harms

Noting that as the application of these technologies to the accessibility and delivery of social services would inevitably impact on the enjoyment of economic, social and cultural rights, such impact needs to be assessed and periodically reviewed. Further, because these technologies rely on the processing of personal data, they interfere with individuals' privacy and therefore need to meet the three overarching principles of legality, necessity and proportionality.

Whilst this is not an exhaustive list, some of the reported and documented risks experienced by individuals and communities, include:

- stigmatisation, i.e. burden to prove they are continuously worthy and they do not intend to abuse the system, as seen with the increased data demanded from those seeking to access social protection programmes as seen when tied to national ID system (see above section on National ID system);

[34] *Ibid*., https://www.ohchr.org/EN/Issues/ESCR/Pages/WhataretheobligationsofStatesonESCR.aspx.

[35] For more details look at the section on "Risks and Harms" below.

[36] See: Hern, A., *Google 'betrays patient trust' with DeepMind Health move*, The Guardian, 14 November 2018. Available at: https://www.theguardian.com/technology/2018/nov/14/google-betrays-patient-trust-deepmind-healthcare-move; Thielman, S.,
This article is more than 2 years old
Your private medical data is for sale – and it's driving a business worth billions, The Guardian, 10 January 2017. Available at: https://www.theguardian.com/technology/2017/jan/10/medical-data-multibillion-dollar-business-report-warns; Deloitte., Connected health, How digital technology is transforming health and social care. Available at: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-connected-health.pdf.

- discrimination, i.e. criteria and/or decision-making for registration and eligibility as seen in multiple examples across the world including India[37], Chile[38] and the USA[39] , amongst others.
- exposure to state surveillance as part of profiling and monitoring practices - both physical as seen with the use of CCTV cameras to monitor benefits claimants in the United Kingdom[40] and Israel[41], and physical and digital surveillance as seen in Canada[42] and Switzerland.[43] Claiming benefits should not be exposed to increased surveillance. Everyone should be able to claims what they are entitled to without having to fear such state scrutiny.

Privacy, security and data protection safeguards must be considered from the onset, when deciding if a new social protection programme is necessary, through the whole decision-making process from design, implementation to maintenance. If they are not or if they come in too late into the process, then there is a high risk that not only would these programmes be unlawful but actually the benefits expected to result from them will be undermined and even outweighed by the risks which emerge.[44]

---

[37] For example, a 28-year old domestic worker, for instance, had to be hospitalised for a blood transfusion after she had an abortion with an unqualified local physician. She had been denied an abortion, to which she was legally entitled, from a reputable government hospital, as she did not have an Aadhaar card. See: *Activists Slam Mandatory Linking of Aadhaar to Health Services After Woman Denied Abortion*, The Wire, 1 November 2017. Available at: https://thewire.in/government/activists-slam-mandatory-linking-aadhaar-health-services-woman-denied-abortion Following this case, 52 public health organisations and individuals issued a statement demanding that "the linking of Aadhaar to health and other social services be revoked by the Centre and all states." See: Indian Journal of Medical Ethics, *Public Statement: Gross violation of human rights due to the mandatory linking of Aadhar to health and allied social security schemes*. Available at: Choudhury, A. D., Linking Aadhaar With PDS Has Left Some of India's Most Marginalised Hungry, The Wire, 27 November 2017. Available at: https://thewire.in/rights/aadhaar-welfare-scheme-jharkhand.

[38] 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.

[39] See: Eubanks, V. (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*

[40] Watts, J., *No wonder people on benefits live in fear. Supermarkets spy on them now*, The Guardian, Opinion, 31 May 2018. Available at: https://www.theguardian.com/commentisfree/2018/may/31/benefits-claimants-fear-supermarkets-spy-poor-disabled; Gentleman, A., *Benefit fraud: spies in the welfare war*, The Guardian, 1 February 2001. Available at: https://www.theguardian.com/society/2011/feb/01/benefits-fraud-investigators

[41] See: http://mynetnetanya.co.il/%D7%97%D7%93%D7%A9%D7%95%D7%AA/881.

[42] See: Heussner, K.M., *Woman Loses Benefits After Posting Facebook Pics*, ABC News, 23 November 2019. Available at: https://abcnews.go.com/Technology/AheadoftheCurve/woman-loses-insurance-benefits-facebook-pics/story?id=9154741. Other examples include the United Kingdom, see: Adams, J., *Mother, 50, who claimed £2.5million compensation from the NHS saying operation left her disabled is caught partying on her daughter's Ibiza hen do and jailed for five months*, Daily Mail, 8 April 2019. Available at: https://www.dailymail.co.uk/news/article-6898069/Jail-mother-2-5m-NHS-claim-op-said-left-severely-disabled-exposed.html.

[43] *Swiss vote on insurance company spies,* The Local, 23 November 2018. Available at: https://www.thelocal.ch/20181123/swiss-vote-referendum-on-insurance-company-spies-switzerland-insurance-detectives.

[44] See: Eubanks, V. (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*

It there are individuals and communities who are negatively impacted and whose experiences are further heightened because of existing power dynamics. The 'digitalisation' of social protection programmes may negatively impact individuals and communities who are already in a disadvantaged position. These include, but are not limited, to those who are: disadvantaged because of their economic, social, class, or legal status, amongst others; those who have to rely on the state to provide for themselves and their families and dependents; and those who were already marginalised and who have been and continue to be hit the hardest by austerity measures and cuts in benefits including women, ethnic minorities, LGTBIQ and gender fluid persons, and migrants (regular and irregular).

Systemic issues: threats and challenges

Digital technology has created what can be described as 'government-industry complex' that manages and regulates social protection programmes. Some of the concerning features of this 'government-industry complex' include:

- poor governance of social protection policies, including limited open, inclusive and transparent decision-making processes;
- limited transparency and accountability of the systems and infrastructure;
- access is tied to a rigid national identification system;
- excessive data collection processing;
- data exploitation by default; and
- multi-purpose and interoperability as the endgame.

Furthermore, the security concerns cannot be ignored. Technologically complex systems are inherently vulnerable to intrusions or data breaches. There are numerous high-profile example of 'secure' digital systems being breached.[45] If some of the most well-resourced governments in the world are unable to protect their most sensitive data sources, it is reasonable to assume that resource-constrained governments and humanitarian agencies will face significant challenges to appropriately securing databases, while making them 'honey pots' for attackers.

The aforementioned threats and risks are further heightened given some specific factors of this sector, which amongst others include:

- the vulnerable and challenging position of individuals and communities affected by decisions which impacts their lives in the short- and long-term,
- the limited knowledge and expertise within social protection policy-making of data protection and security resulting in the lack of prioritisation of resources and skills-development to make informed decisions, and
- the reliance on third-parties, in particular the private sector, which raises questions of control, transparency and accountability, as well as a threat of inappropriate influence from lobbying and the risk of facilitating corruption.

[45] Perhaps most notoriously is the breach of the US Office of Personnel Management containing sensitive personal data of millions of US government employees. See: Koener, B., *Inside the Cyberattack That Shocked the US Government,* Wired, 23 October 2016. Available at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/. For other examples from across the world, see: Privacy International, State of Privacy, 'Examples of data breaches'. Available at: https://privacyinternational.org/type-resource/state-privacy

This is why it is essential that certain measures be taken to ensure that governments implement safeguards by design into all social protection programmes – and if risks cannot be mitigated, then system must not be deployed. Data generated and processed in the delivery of social protection programmes must be firewalled from other government policies which may have other purposes including for law enforcement and immigration enforcement, amongst others.[46]

Industry not only provide solutions to governments but through the delivery of their own services they also feed the broader data exploitation ecosystem.[47] Not only should companies be transparent about how their business models operate in practice, i.e. the design of their systems, and the solutions they provide to governments, but these should also be firewalled from other areas of their business models and interests.[48]

III. Contextual circumstances

Contextual drivers include rising concerns around austerity, and transparency, efficiency and financial management. There are various dynamics and considerations at play including the balance of the legitimate interest of government to prevent defrauding the system used to justify disproportionate measures that result in disproportionate collection of personal data and other intrusions to privacy of those seeking accessing to social services, ultimately resulting to discrimination. Also, many of the technical, data intensive solutions, are put forward as cost savings solutions (in support, among others, to austerity measures)

Technology as a panacea

The use of technology and data in social protection programmes is yet another example whereby technology is seen as the panacea to a socio-economic and political issues which have various root causes for which there is not a single solution, and therefore one system, one technology cannot solve them.

The drivers vary from country and region but globally countries have reacted to legacies of waves of economic crisis and waves of political support for draconian austerity policies.[49]

---

[46] See: A Guide to the Hostile Environment: the border controls dividing our communities – and how we can bring them down. Available at: https://www.libertyhumanrights.org.uk/policy/policy-reports-briefings/guide-hostile-environment-border-controls-dividing-our-communities-%E2%80%93.

[47] The data exploitation system is so opaque and secretive that is very difficult to oversee. See: Privacy International, Why we've filed complaints against companies that most people have never heard of – and what needs to happen next, 8 November 2018. Available at: https://privacyinternational.org/advocacy-briefing/2434/why-weve-filed-complaints-against-companies-most-people-have-never-heard-and.

[48] Hern, A., "=Google 'betrays patient trust' with DeepMind Health move", The Guardian, 14 November 2018. Available at: https://www.theguardian.com/technology/2018/nov/14/google-betrays-patient-trust-deepmind-healthcare-move. Also similar concerns are raised in the humanitarian sector, see: Privacy International, Palantir and the UN's World Food Programme are partnering for a reported $45 million, 6 February 2019. Available at: https://privacyinternational.org/news/2684/palantir-and-uns-world-food-programme-are-partnering-reported-45-million.

[49] Booth, R., UN report compares Tory welfare policies to creation of workhouses, 22 May 2019. Available at: https://www.theguardian.com/politics/2019/may/22/un-report-compares-tory-welfare-reforms-to-creation-of-workhouses.

Social protection programmes have evolved not to provide access to social protection programmes but to find ways to minimise those eligible through various filtering mechanisms.

This context also requires us to consider some of the promoters of such developments. Whilst governments have increasingly pushed for a reform of social protection programmes, we have observed that the proponents have a lot of power in the form of financial resources, expertise, influence and the ability to mobilise. Proponents include the private sector (as detailed further in the next paragraph) but the power and role of actors with investment structures, such as the World Bank[50] and the Word Economic Forum[51], and leading development funders amongst others.

An ecosystem of government and corporate exploitation and surveillance

Just as in many sectors ranging from the use of digital technologies in the field of development and humanitarian[52] and migration[53] to name a few, these developments in the social protection sector have emerged in an ecosystem of government and corporate exploitation and surveillance as facilitated by ongoing improvement in data processing capabilities, the growing amounts of data and metadata that can be processed[54]. More of our actions and interactions now generate data and metadata, and (meta)data surveillance no longer concerns itself with the individual.[55]

Mission creep by default and design

There is also a narrative where the implementation of social protection programmes is used as an excuse to build databases, which are often interoperable, and then used secondary and tertiary purposes, be it immigration, law enforcement, counter terrorism, and broader surveillance - and sharing with the private sector who are increasingly providing these services.

IV. Recommendations

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 we hope that the mandate will take steps:

---

[50] See: https://www.worldbank.org/en/topic/socialprotection. Also see: World Bank, *World Bank Approves $75 Million to Strengthen Sri Lanka's Social Safety Net Program*, Press Release, 2 December 2016. Available at: http://www.worldbank.org/en/news/press-release/2016/12/02/strengthen-sri-lankas-social-safety-net-program.

[51] World Economic Forum, Global Risks Report 2017, Part 2 – Social and Political Challenges: 2.3 The Future of Social Protection Systems. Available at: http://reports.weforum.org/global-risks-2017/part-2-social-and-political-challenges/2-3-the-future-of-social-protection-systems/.

[52] See: Privacy International, Development and Humanitarian Sector, Topic Page. Available at: https://privacyinternational.org/topics/development-and-humanitarian-sector.

[53] See: Privacy International, Migration and Border, Topic Page. Available at: https://privacyinternational.org/topics/migration-and-borders.

[54] Reference to data brokers here as well as concerns regarding regime changes that may then have access to those data bases and repurpose the data to means of surveillance and oppression.

[55] International Committee of the Red Cross (ICRC) and Privacy International, *The humanitarian metadata problem: "Doing no harm" in the digital era*, October 2018, pp. 3-4. Available at: https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era.

- To promote a human rights approach for developing social protection programmes;
- To demand that the right to privacy and data protection are respected while implementing new and existing programmes, in order to ensure that those in most need do not have to trade their right to privacy for receiving social rights; among others, the data processed by social protection programmes should be adequate, relevant and limited to what is necessary in relation to the processing purpose (purpose limitation and data minimisation principles);
- To demand that appropriate measures are in place to ensure that the infrastructures supporting social protection programmes are secure by design and by default;
- To require appropriate safeguards to be put in place, including effective oversight, to ensure categories of beneficiaries are not disproportionately affected.

In addition:

- There is an opportunity for Special Rapporteur to develop collaboratively with national human rights institutions methodologies and strategies for integrating questions of technology, security and privacy within their work on monitoring and promoting socio-economic rights;
- As social protection programmes involve a wide array of actors, it is important for the Special Rapporteur to engage with international organisations, such as the World Bank, that fund those programmes, in order to exchange knowledge and expertise of technology, security and privacy, and to ensure they integrate human rights analysis, including privacy and data protection, in their approach to their mandates, priorities and funding decisions.