Privacy International's submission for the High Commissioner for Human Rights' report on privacy in the digital age and discrimination

May 2025

1. Introduction

Privacy International (PI)[1] welcomes the opportunity to provide input to the forthcoming report the High Commissioner for Human Rights to the 60th session of Human Rights Council on the challenges and risks with regard to discrimination and unequal enjoyment of the right to privacy associated with the collection and processing of data.[2]

The following submission seeks to follow the structure and to address some of the questions posed in the call for submission.

2. Scenarios and concrete examples of instances of discrimination and unequal enjoyment of the right to privacy

2.1 Discrimination in the context of migration management and border security

Technologies relying on processing of personal data (including AI and automated decision making) have been deployed in border management and immigration enforcement. These have included mobile phone extractors,[3] lie detectors at the border,[4] tracking of social media accounts,[5] language

[1] PI is an international non-governmental organisation, which campaigns against companies and governments who exploit individuals' data and technologies. PI employs specialists in their fields, including technologists and lawyers, to understand the impact of existing and emerging technology upon data exploitation and our right to privacy. For more information: https://privacyinternational.org/

[2] Call for input available at: https://www.ohchr.org/en/calls-for-input/2025/right-privacy-digital-age

[3] See PI intervenes in judicial review to support asylum seekers against the UK Home Secretary's seizure and extraction of their mobile phones, https://privacyinternational.org/news-analysis/4782/pi-intervenes-judicial-review-support-asylum-seekers-against-uk-home-secretarys

[4] See: iborderCtrl website, https://www.iborderctrl.eu/The-project.

[5] PI, '#PrivacyWins: EU Border Guards Cancel Plans to Spy on Social Media (for now)', 19 November 2019, https://privacyinternational.org/advocacy/3289/privacywins-eu-border-guards-cancel-plans-spy-social-media-now

analysis[6], automated decision making about visitor visa applications,[7] to the identification refugees,[8] or as part of digital border monitoring systems.[9]

These technologies affect the right to privacy in unique ways and because they are justified for purposes such as migration control, they disproportionately affect migrants and other non-nationals, as they cross international borders. Further, the experimental nature of some of these technologies and the fact that they are often first tested on migrants before being deployed elsewhere is already a form of discrimination.

In Europe, this includes the use of technology which supposedly identifies if a person is lying based on their 'micro-gestures', a person's origin based on their voice, and their age based on their bones.[10] The European Union's Horizon 2020 research and innovation programme has been funding a project called iBorderCtrl, defined as "an innovative project that aims to enable faster and thorough border control for third country nationals crossing the land borders of EU Member States".[11] In addition to other features, the system undertakes automated deception detection.[12] The system was tested at the border in Hungary, Latvia and Greece.[13] In July 2019, The Intercept used the system at the Serbian-Hungarian border: reportedly, the system failed, and the results were not disclosed.[14]

In this context, it is concerning that the EU AI Act falls short in addressing the potential harms of AI when used for border and immigration.[15] The EU AI Act aims to regulate the use of AI within the European Union, setting prohibitions and accountability requirements for 'high-risk' AI applications. However, prohibitions on AI systems do not extend to the migration context, allowing discriminatory risk assessments, emotion recognition or predictive analytics to persist.

In addition, the EU AI Act fails to recognise the potential harms of many AI systems used in migration control, such as biometric identification systems (Annex III, point 1(a)) that have been shown to discriminate, exclude and serve as means of oppression if deployed without safeguards.[16] Such systems have been excluded from the list of "high-risk" systems that attract higher transparency and accountability requirements, and AI used in large-scale interoperable EU databases is exempted from regulation until 2030. Transparency requirements are limited for AI systems used in migration control, such that details of these systems (as opposed to systems deployed in the general population) don't have to be published (Article 49(4)). And high-risk AI systems deployed for migration control purposes

---

[6] PI, 'The UK's Privatised Migration Surveillance Regime: A rough guide for civil society', 2021, https://privacyinternational.org/sites/default/files/2021-01/PI-UK_Migration_Surveillance_Regime.pdf

[7] Foxglove, "Legal action to challenge Home Office use of secret algorithm to assess visa applications", https://www.foxglove.org.uk/news/legal-challenge-home-office-secret-algorithm-visas.

[8] Patrick Tucker, "Refugee or Terrorist? IBM thinks its software has the answer", *Defense One*, 27 January 2016, http://www.defenseone.com/technology/2016/01/refugee-or-terrorist-ibm-thinks-its-software-has-answer/125484/.

[9] Olivia Solon, "'Surveillance society': has technology at the US-Mexico border gone too far?", *The Guardian*, 13 July 2018, https://www.theguardian.com/technology/2018/jun/13/mexico-us-border-wall-surveillance-artificial-intelligence-technology.

[10] Melanie Ehrenkranz, "An AI Lie Detector Is Going to Start Questioning Travelers in the EU", Gizmodo, 31 October 2018, https://gizmodo.com/an-ai-lie-detector-is-going-to-start-questioning-travel-1830126881

[11] See: iborderCtrl website, https://www.iborderctrl.eu/The-project]

[12] See: iborderCtrl Participants, https://www.iborderctrl.eu/#Project-Participants

[13] See: iborderCtrl Pilot Results, https://www.iborderctrl.eu/Pilot-Results

[14] Ryan Gallagher and Ludovica Jona, "We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive", *The Intercept*, 26 July 2019, https://theintercept.com/2019/07/26/europe-border-control-ai-lie-detector

[15] PI, "Joint statement – A dangerous precedent: how the EU AI Act fails migrants and people on the move", 13th March 2024, https://privacyinternational.org/advocacy/5264/joint-statement-dangerous-precedent-how-eu-ai-act-fails-migrants-and-people-move; For more details: https://protectnotsurveil.eu/

[16] Ben Hayes, Migration and displacement. Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and "big data", International Review of the Red Cross (2017), 99 (1), 179–209.A Available at: https://international-review.icrc.org/sites/default/files/irrc_99_12.pdf

are exempted from a key human oversight safeguard of requiring independent human verification of any identification performed by an AI system (Article 14(5)).

In the UK, the Home Office uses a range of automated decision-making systems which directly affect migrants. Firstly, an automated triage system to assess whether a prospective marriage warrants investigation as a 'sham,' aiming to circumvent immigration laws rather than reflecting a bona fide relationship. Public Law Project (PLP) highlighted their concerns over its implementation[17] and filed a legal challenge the Home Office's use of this algorithm on the grounds that the triage tool's outcomes potentially discriminate based on nationality, that the Home Office may not have fulfilled its duty to prevent discrimination and promote equality, especially when using innovative digital systems, that the Home Office's secrecy about the system violates transparency regulations under the GDPR and that the failure to ensure human/manual review of 'fail' cases contradicts government policy and could constitute a breach of the Immigration Act 2014 by delegating decision-making to a machine-learning algorithm.[18] Second, the "Identify and Prioritise Immigration Cases ("IPIC") Business Rules" is another triage tool used by the Home Office to prioritise and recommend "interventions" to authorities regarding migrants, assessing "the removability and level of harm posed by immigration offenders".[19] Despite PI's attempt to seek information under the Freedom of Information Act (FOIA) regarding this tool, there is a pervasive lack of transparency around it.[20]

As recognised by the UN Special Rapporteur report on "Racial and Xenophobic discrimination and the use of digital technologies in border and immigration enforcement",[21] there is often no or inadequate legal framework regulating the deployment of these technologies by public authorities and private security companies, and in most cases, there are not effective safeguards to protect refugee and migrants against undue interferences with their privacy. Further because of the heightened vulnerability of the situation they are in, refugees and migrants are very unlikely to be able to object to the application of these technologies or to seek remedy against abuses.

2.2 Discrimination on grounds of economic status in access to social welfare

Current and emerging technologies, including AI, to access social welfare are designed and managed in a way that interfere with the privacy of individuals seeking access to benefits and thereby impact disproportionately those economically marginalised. From the stage of eligibility and registration to access benefits, recipients need to turn over vast amounts of personal data – about their employment, their health conditions, their relationship status – which is processed by AI applications to make (or support the making of) decision related to access to social welfare benefits.[22]

Social protection systems around the world are increasingly 'conditional', meaning that aspects of state support, usually financial or practical, are dependent on claimants complying with a set of rules or conditions. These processes are increasingly tied to rigid digital identification systems and

[17] Public Law Project, "Public Law Project (PLP) — Written evidence (NTL0046)", 29 September 2021, https://committees.parliament.uk/writtenevidence/39761/pdf/

[18] Public Law Project, 'Legal action launched over sham marriage screening algorithm', https://publiclawproject.org.uk/latest/legal-action-launched-over-sham-marriage-screening-algorithm/

[19] See The Home Office response to the Independent Chief Inspector of Borders and Immigration's report: A re-inspection of the Home Office's Reporting and Offender Management processes and of its management of non-detained Foreign National Offenders, October 2018 - January 2019, available at: https://assets.publishing.service.gov.uk/media/5cd3e056e5274a3fd5871f36/Formal_response_ICIBI_FNO_ROM.PDF

[20] See Identify and Prioritise Immigration Cases ("IPIC") Business Rules used by the Home Office, available at: https://www.whatdotheyknow.com/request/identify_and_prioritise_immigrat_3

[21] Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance: "Racial and Xenophobic discrimination and the use of digital technologies in border and immigration enforcement", 22 September 2021, UN doc. A/HRC/48/76

[22] PI, "When Big Brother Pays Your Benefits", available at: https://privacyinternational.org/taxonomy/term/675

determined by algorithmic and automated decision making processes.[23] Those who fail to comply with the rules can find themselves automatically cut-off from welfare programs, have their assistance reduced or are subject to sanctions and fines. In some cases, the most vulnerable groups of the population are subject to particularly intrusive level of control and surveillance via digital technologies.[24]

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,[25] to eligibility assessments and so-called 'fraud' detection mechanisms[26]. It has been widely recognised that 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.[27] 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.

Concerns about the negative, discriminatory impact of the use of technologies processing personal data in the welfare context have already been expressed by UN human rights experts[28] and national courts are beginning to rule against these systems on the grounds that they fail to comply with human rights law.[29] For example, a Dutch court assessed 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.[30] 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."[31] 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."[32] 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

[23] See: PI, "Stage 1 - Applying for social benefits: facing exclusion", https://privacyinternational.org/news-analysis/3112/stage-1-applying-social-benefits-facing-exclusion
[24] See: PI, "What is an Aspen Card and why does it need reform?", 23 February 2021, https://privacyinternational.org/explainer/4425/what-aspen-card-and-why-does-it-need-reform
[25] PI, "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.
[26] PI, "Stage 3: The policing of social benefits: punishing poverty", 7 August 2019, https://privacyinternational.org/node/3114
[27] 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, 13 September 2021, UN Doc. A/HRC/48/31
[28] Report of the UN Special rapporteur on extreme poverty and human rights, 11 October 2019, UN doc. A/74/48037
[29] PI, "The SyRI case: a landmark ruling for benefits claimants around the world", 20 February 2020, 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, available at: https://digitalfreedomfund.org/the-syri-victory-holding-government-profiling-to-account/7/; https://gmcdp.com/gmcdp-foxglove-legal-challenge-department-work-and-pensions-dwp-fraud-algorithm
[30] PI, "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/
[31] 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/.
[32] Ibid, n11.

of people from accessing social protection by making incorrect determinations about eligibility,[33] miscalculating welfare benefits, and incorrectly flagging individuals for "fraud".[34]

2.3 Discrimination in digital healthcare, including sexual and reproductive services

The processing of personal data by digital technologies, including AI, within healthcare has been expanding rapidly in recent years. While these technologies may offer new and efficient means to assist with medical diagnosis and to streamline services, the adoption of these technologies in the delivery of healthcare have led to abuses of the right to privacy including discriminatory outcomes, based on processing of personal data,[35] as noted also by the UN Special rapporteur on the right to health.[36]

Digital health technologies may ingrain discriminatory, including racial bias. For example, the UK government commissioned an independent review into the equity of medical devices and the role they play in perpetuating discrimination of minority ethnic people, women and people from deprived communities and the risks of poorer healthcare outcomes.[37] The report evidenced biases at every stage of the lifecycle of medical tools and devices which are then magnified in algorithm development and machine learning. In particular, the report confirmed a link between pulse oximetry devices, racial bias and Covid-19. These were widely used devices during the Covid-19 pandemic to measure low oxygen levels in the blood, which were found to be overestimating the amount of oxygen in the blood of people with dark skin and Black and minority ethnic people.[38] Other AI enabled devices, such as dermoscopes used in dermatology, which are used to capture and help interpret images of skin lesions have been attributed to the under-diagnosis of skin cancer, as they do not cater as well for non-white skin. The consequences could include increased false negative error rates for skin cancer detection and delayed treatment for patients from some ethnic groups.[39]

As access to reproductive healthcare becomes increasingly digitalised, accessing reproductive healthcare oftentimes requires interacting with a digitalised system that collects vast amounts of personal information. For example, digital initiatives such as SMS appointment scheduling, remote access to care and counselling, health workers using a mobile phone to track an individual pregnant mother over the cycle of pregnancy, or a child over his/her cycle of immunization, and the use of mobile applications, sensors, wearable devices and others, all collect personal information.[40]

A key dimension of non-discriminatory, safe access is being able to access sexual and reproductive rights without negative repercussions. However, in many cases, women are prevented access to safe abortion services on account of being unnecessarily subjected to data exploitation and surveillance by

[33] Ibid, n3 at paras. 21 and 22, page 9
[34] See: PI, "Stage 3 – The policing of social benefits: punishing poverty", 7 August 2019, https://privacyinternational.org/node/3114
[35] See: PI, "Digital Health: what does it mean for your rights and freedoms", https://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms
[36] Report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health on Digital innovation, technologies and the right to health, UN doc. A/HRC/53/65, 21 April 2023.
[37] Nicola Davis, "UK report reveals bias within medical tools and devices", *The Guardian*, 11 March 2024, https://www.theguardian.com/society/2024/mar/11/medical-tools-devices-healthcare-bias-uk
[38] See: https://assets.publishing.service.gov.uk/media/65e89e9e62ff48001a87b2d8/equity-in-medical-devices-independent-review-report-web-accessible.pdf
[39] Ibid
[40] PI, Protecting Privacy In The Digitalisation Of Reproductive Healthcare, https://privacyinternational.org/campaigns/protecting-privacy-digitalisation-reproductive-healthcare

governments or/and opposition groups.[41] Privacy often becomes a hidden cost to the access of abortion care or other sexual and reproductive health services.[42]

In India, research by the Center for Internet and Society found that many public hospitals are demanding Aadhaar cards – the national ID – before allowing women to access reproductive health procedures. This has resulted in a denial of essential services to people who have not been able to register to the Aadhaar database. For those people who are able to access reproductive health care services, their data is collected, centralised and accessible to parties who have their individual's Aadhaar number. Those parties include most government bodies, banks and telecommunications companies. Moreover, the Aadhaar system is susceptible to data leaks; for instance, the data breach of a government agency in April 2019 made health records of 12.5 million pregnant women available online.[43]

More broadly, Privacy International[44] and its partners in Argentina, Brazil, Chile, India, Indonesia, Kenya and Peru[45] have documented a range of data exploitation practices used by anti-abortion groups to limit women's access to reproductive healthcare. These include targeting advertising using geo-fencing, as well as data-collection tactics deployed by crisis pregnancy centres using online chat services.

3. Main factors that cause or contribute to discriminatory outcomes - Technological factors

3.1 Discriminatory challenges posed by AI technologies

Modern data protection principles offer some useful protection against discrimination. In particular, it is common for certain categories of personal data to be distinguished on the grounds that they are 'sensitive', or a special category, which, when processed, requires additional levels of protection. While there is no exhaustive list of what constitutes sensitive personal data, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; biometric data; health-related data; and data concerning a person's sex life or sexual orientation are widely regarded as constituting sensitive personal data. This category of data attracts higher safeguards, including limitations on the permitted grounds for processing it.[46]

However, AI technologies pose specific challenges to these data protection safeguards.

Firstly, existing data protection laws tend to provide safeguards only in relation to the processing of personal data, i.e. data from which an individual can be identified either directly or indirectly. AI technologies often blur this distinction between personal and non-personal data. Machine learning and big data analytics, for example, are fundamentally based around the idea of extracting

[41] PI, International Safe Abortion Day 2023, available at: https://privacyinternational.org/long-read/5145/international-safe-abortion-day-2023
[42] PI, "Privacy matters because…it protects our bodily autonomy", available at: https://privacyinternational.org/case-study/3388/it-protects-our-bodily-autonomy
[43] PI, Country case-study: sexual and reproductive rights in India, available at: https://privacyinternational.org/long-read/3863/country-case-study-sexual-and-reproductive-rights-india
[44] PI, A Documentation of Data Exploitation in Sexual and Reproductive Rights, available at: https://privacyinternational.org/sites/default/files/2020-04/PI-Sexual-Repruductive-Rights-report.pdf
[45] PI, Country case studies, reproductive rights, available at: https://privacyinternational.org/learning-resources/country-case-studies-reproductive-rights
[46] For references to definition, see PI, Data Protection Guide available at: https://privacyinternational.org/data-protection-guide

information from data, and these technologies develop ways to identify individuals from data that would historically be considered non-personal data, and therefore outside the purview of data protection law.

Secondly, AI applications may also blur the distinction between sensitive and non-sensitive personal data. Certain categories of personal data, similar to protected characteristics, are usually considered more sensitive, and are thus subject to higher protections. Through advanced data analytics, highly sensitive details revealing or predicting an individual's sexual life, health status, religious or political views, can be gained from seemingly mundane data. For example, location data or browser searches can reveal individuals' religion or their sexual orientation.

When sensitive personal data, such as information about race, ethnicity, or political beliefs can be predicted from seemingly unrelated data, there are risks of exacerbating discriminatory practices, particularly if AI interpret data to predict future behaviours. These discriminatory concerns of AI have been raised by UN human rights mechanisms, as well as resolutions by the Human Rights Council and the General Assembly. For example, the 2024 report of the UN Special rapporteur on contemporary forms of racism noted how AI systems supporting facial recognition technologies and predictive policing tools carry an inherent risk of perpetuating or even enhancing discrimination, reflecting embedded historic racial and ethnic bias in the data sets used, such as a disproportionate focus of policing of certain groups.[47]

Further, AI applications may rely on non-personal data to make or inform decisions that still negatively impact the human rights of individuals and groups affected. In these circumstances, data protection law offers little in ways of protection.

In assessing the adequacy of the national legal framework to respect and protect privacy against discriminatory outcomes of AI technologies, it is therefore necessary to consider the wider range of laws relevant to AI technologies, including equality and anti-discrimination, consumer protection, electronic safety, product liability, competition, redress and administrative law, to name a few, together with sectoral legislation governing the deployment of AI applications in specific sectors, such as health care, criminal justice, immigration control, financial and insurance sector, etc.

3.2 Discrimination resulting from the deployment of Facial Recognition Technology (FRT)

[47] Report of the Special Rapporteur on contemporary forms of racim, racial discrimination, xenophobia and related intolerance, UN doc. A/HRC/56/68, 3 June 2024.

The human rights risks associated with the use of FRT[48] has been well-documented by the High Commissioner for Human Rights' previous reports.[49] PI has highlighted how the deployment of FRT is not only happening in a regulatory void but it is not subject to public and democratic scrutiny.[50]

In particular FRT for identification and categorisation purposes could lead to discrimination. Among the specific concerns around discrimination resulting from the use of FRT are: non-representative training data with data sets used to train AI models and algorithms do not necessarily represent the communities on which the final system will be used,[51] and there are reported concerns of lower accuracy of facial recognition technologies with certain groups with skin colour being a key factor in the bias and lack of accuracy and profiling on the basis of race, ethnicity, national origin.[52]

In his 2019 Report, the UN Special Rapporteur on the right to freedom expression noted that FRT "seeks to capture and detect the facial characteristics of a person, potentially profiling individuals based on their ethnicity, race, national origin, gender and other characteristics, which are often the basis for unlawful discrimination".[53]

Across the world we have seen government deploy FRT in public spaces for law enforcement purposes.[54] In Brazil, civil society organisations have warned of risks of discrimination and face positives posed by FRT in public spaces,[55] including São Paulo where a network of some 25,000

[48] FRT may involve the use of cameras, which can capture individuals' facial images and process them in real time ("live FRT") or at a later point ("Static" or "Retrospective FRT"). The collection of facial images results in the creation of "digital signatures of identified faces", which are analysed against one or more databases ("Watchlists"), usually containing facial images obtained from other sources to determine if there is a match.

[48] See, for example, the report of the High Commissioner for Human Rights on the "Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests", 24 June 2020, UN doc. A/HRC/44/24. The UN Special Rapporteur on freedom of opinion and expression has called for a moratorium of the sale and use of live facial recognition (LFR) technology (Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 28 May 2019. A/HRC/41/35, para 66 (f).

[49] Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, 13 September 2021, UN Doc. A/HRC/48/31; UNGA Resolution on the right to privacy in the digital age, 15 December 2022, UN Doc. A/RES/77/211, page 3

[50] PI, "UK MPs Asleep at the Wheel as Facial Recognition Technology Spells The End of Privacy in Public", 7 November 2023, https://privacyinternational.org/long-read/5155/uk-mps-asleep-wheel-facial-recognition-technology-spells-end-privacy-public

[51] Joy Buolamwini, Unmasking the bias in facial recognition algorithms, 13 December 2023, Excerpted from the book "Unmasking AI: My Mission to Protect What Is Human in a World of Machines," by Joy Buolamwini (2023), Published by Random House, an imprint and division of Penguin Random House LLC, available at: https://mitsloan.mit.edu/ideas-made-to-matter/unmasking-bias-facial-recognition-algorithms

[52] Larry Hardesty, Study finds gender and skin-type bias in commercial artificial-intelligence systems, MIT News, 11 February 2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 and https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0

[53] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 28 May 2019, UN Doc. A/HRC/41/35, para 12

[54] PI, The End of Privacy In Public, https://privacyinternational.org/campaigns/end-privacy-public; World Economic Forum, UNICRI, INTERPOL and Netherlands Police, A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations, Insight Report, Revised November 2022, Available at: https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf; Rohit Talbot, Automating occupation: International humanitarian and human rights law implications of the deployment of facial recognition technologies in the occupied Palestinian territory, International Review of the Red Cross (2020), 102 (914), 823–849, Emerging Voice, available at: https://international-review.icrc.org/articles/ihl-hr-facial-recognition-technology-occupied-palestinian-territory-914; ADC, Tecnologías de Vigilancia en Argentina, December 2021, available at: https://adc.org.ar/wp-content/uploads/2021/12/ADC-Tecnologias-de-Vigilancia-en-Argentina.pdf; INCLO, In Focus: Facial Recognition Tech Stories and Rights Harms from Around the World, January 2021, available at: https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf; Maria Badillo, Navigating the complexities of facial recognition for public security in Latin America, *International Bar Association*, 9 May 2023.

[55] See https://tiremeurostodasuamira.org.br/

cameras with FTC technology known as Smart Sampa has been deployed for purposes of fighting criminality.[56]

In the UK in 2020, in the case of *Ed Bridges v South Wales Police*, the Court of Appeal found that the police's use of FRT breached privacy rights, data protection laws and equality laws. The case was supported by Liberty[57] and brought by campaigner Ed Bridges, who had his biometric facial data scanned by the FRT on a Cardiff high street in December 2017, and again when he was at a protest in March 2018. The UK Court of Appeal ruled that these deployments were unlawful and noted that the force did not take reasonable steps to find out if the software had a racial or gender bias.[58]

In the UK, FRT is also reportedly being deployed by private companies in cooperation with the police.[59] PI together with anti-poverty, homelessness, human rights, criminal justice, data, tech and privacy experts have repeatedly expressed concerns about the collaboration between retailers and the police that involves the use of facial recognition technology in response to a rise in shoplifting.[60] In our communications to the CEOs of shops involved in the scheme, we flagged concerns about such a system amplifying existing inequalities within the criminal justice system given that FRT has shown to misidentify people of colour, women and LGBTQ+ people, meaning that already marginalised groups are more likely to be subject to an invasive stop by police, or may be at increased risk of physical surveillance, monitoring and harassment by workers in those retail spaces.[61]

FRT is also increasingly being used to mediate children's access to education. This is despite the persistent evidence of discrimination within facial recognition systems, including systems being deployed by schools.[62] Some data protection authorities have taken steps to prevent the technology from being used in classrooms,[63] and some other authorities - such as New York State - have banned the use of the technology in schools because of the "potentially higher rates of false positives for

[56] El Pais, In São Paulo, 'Big Brother' is watching, with 25,000 cameras and facial recognition technology, 10 May 2025, available at https://english.elpais.com/international/2025-05-10/in-sao-paulo-big-brother-is-watching-with-25000-cameras-and-facial-recognition-technology.html

[57] Liberty, "Liberty Wins Ground-Breaking Victory Against Facial Recognition Tech", 11 August 2020, Available at: https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/; Liberty, Legal Challenge: Ed Bridges v South Wales Police, Available at: https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/

[58] R (on the application of Edward Bridges) v the Chief Constable of South Wales Police [2020] EWCA Civ 1058, para 201, available at: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf; Also see: Evani Radiya-Dixit, A Sociotechnical Audit: Assessing Police Use Of Facial Recognition, October 2022, Minderoo Centre for Technology and Democracy, Available at: https://www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf

[59] Alex Hern, "MPs condemn Frasers Group's use of facial recognition cameras in stores", *The Guardian*, 23 April 2023, https://www.theguardian.com/business/2023/apr/23/mps-condemn-frasers-groups-use-of-facial-recognition-cameras-in-stores; PI, "Cooperating With Who?! Answers Needed as UK Retailer Southern Co-Op Tests Facewatch", 9 December 2020, https://privacyinternational.org/advocacy/4342/cooperating-who-answers-needed-uk-retailer-southern-co-op-tests-facewatch; BBW, "BBC – Big Brother Watch files legal challenge with the ICO against Southern Co-op's use of facial recognition systems", 26 July 2022, https://bigbrotherwatch.org.uk/2022/07/bbc-big-brother-watch-files-legal-challenge-with-the-ico-against-southern-co-ops-use-of-facial-recognition-systems/

[60] Liberty, "Rights Groups Urge Shops To Reject Facial Recognition", 29 October 2023, https://www.libertyhumanrights.org.uk/rights-groups-urge-shops-to-reject-facial-recognition/

[61] Letter available at: https://www.libertyhumanrights.org.uk/wp-content/uploads/2023/10/Liberty-Joint-letter-to-retail-CEOS-regarding-Project-Pegasus-October-2023.pdf and joint letter to UK retailers regarding the potential use of facial recognition technology (FRT) within their stores, available at: https://privacyinternational.org/advocacy/5351/joint-letter-uk-retailers-regarding-potential-use-facial-recognition-technology-frt

[62] Yoder-Himes DR, Asif A, Kinney K, Brandt TJ, Cecil RE, Himes PR, Cashon C, Hopp RMP and Ross E (2022) Racial, skin tone, and sex disparities in automated proctoring software. Frontier Education, 7:881449, Available at: https://www.frontiersin.org/articles/10.3389/feduc.2022.881449/full

[63] Sofia Edvardsen, How to interpret Sweden's first GDPR fine on facial recognition in school, IAPP, 27 August 2019, https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/

people of color".[64] However, many children live in countries either without an appropriate legal framework,[65] or where schools have been allowed to go ahead despite a seemingly protective legal framework.[66]

Further systems, intertwined with the FRT technology, intended to monitor children's emotions are also being deployed in schools.[67] These systems are fundamentally unsound, these technologies have been found to interpret the facial expressions of white and black people differently - attributing negative feelings, such as contempt and anger, more frequently to black people.[68] Facial recognition in schools is no more sophisticated and no less likely to discriminate than facial recognition deployed elsewhere.

4. Main factors that cause or contribute to discriminatory outcomes - Legal, policy and institutional factors

4.1 Discrimination in surveillance laws

It has long been noted with concerns, including in the High Commissioner for Human Rights' first thematic report on the right to privacy in the digital age,[69] that surveillance legislation often provides differing levels of protections for internal versus external communications, or those relating to nationals versus non-nationals. It is both irrational and contrary to international human rights norms to suppose that the privacy of a person's communications could be accorded different legal weight according to their nationality or residence. These laws were consistently held by international human rights mechanisms, including the UN Human Rights Committee,[70] as being discriminatory and thereby infringing upon the rights of all individuals within the respective States' jurisdiction to enjoy human rights protections equally and without discrimination. However, surveillance legislation in many countries continue to apply a differential treatment of nationals and non-nationals, and of those within or outside a state's territory. In 2023, the European Court of Human Rights held that the "interference with the privacy of communications clearly takes place where those communications are intercepted, searched, examined and used and the resulting injury to the privacy rights of the sender and/or recipient will also take place there" (para 93) and given the UK intercepted, searched, examined or used the applicants' communications within the United Kingdom's territory, the interference with their right to privacy fell within the territorial jurisdiction of the United Kingdom.[71]

[64] See: https://www.nysed.gov/sites/default/files/programs/data-privacy-security/biometric-determination-9-27-23.pdf
[65] PI, Stakeholder Report Universal Periodic Review 41st Session – India, April 2022, https://privacyinternational.org/advocacy/4981/right-privacy-indian-schools-universal-periodic-review
[66] Carolina Batista Israel, Rodrigo Firmino, coordenadores; [autores] Carolina Batista Israel ... [et al.]; capa, Manoela M. Jazar - Curitiba (2023) Reconhecimento facial nas escolas públicas do Paran. Page 20-31, available at: https://jararacalab.org/cms/wp-content/uploads/2023/12/RF_PR_2023.pdf
[67] Ibid, page 37
[68] Lauren Rhue, Racial Influence on Automated Perceptions of Emotions, SSRN, 9 November 2018, available at: https://ssrn.com/abstract=3281765 or http://dx.doi.org/10.2139/ssrn.3281765
[69] Report of the High Commissioner for Human Rights on right to privacy in the digital age, A/HRC/27/37, paragraph 35-36, 30 June 2014.
[70] For references to relevant concluding observations of the UN Human Rights Committee and relevant extracts of reports of UN special procedures, see Privacy International's Guide to International Law and Surveillance, March 2024, page 276, available at: https://privacyinternational.org/sites/default/files/2024-09/2024%20GILS%20version%204.0.pdf
[71] For references on this case, see PI, (Still) Challenging mass interception from outside the UK: Wieder and Guarnieri v the UK, available at: https://privacyinternational.org/legal-action/still-challenging-mass-interception-outside-uk-wieder-and-guarnieri-v-uk

4.2 Discrimination resulting from the imposition of digital ID systems

Digital identity systems are predicated upon the processing of personal data, including often biometric data. One of the concerns of national digital identity systems is that they lead to discrimination and exclusion, particularly when digital ID requirements are imposed in order to access goods and public services. The UN Secretary-General has drawn attention in particular to the risks of exclusion in his report on the role of new technologies for the realisation of economic, social and cultural rights.[72]

PI conducted research in Chile, where a single identity number is used for a very broad range of purposes in the public and private spheres. It is required to access state health care, to sign some contracts, and is used as a 'loyalty card' in some shops. This research found that migrants were entitled to but not able to get a card, often – as they
saw it – because of the pressure that the bureaucracy was under. The research found that as a result these individuals experienced difficulties in accessing state healthcare, change jobs, move house, or even getting married.[73] In 2021, PI conducted research on trans people, i.e. people who do not identify with the gender marker they were assigned at birth. As this research on trans people in the Philippines, Argentina and France reveals, this is a group that faces particular issues because their ID documents do not reflect how they present their gender identity. As a result of this, they face difficulties accessing social services, in particular healthcare.[74]

In Pakistan, the national ID – the Computerised National Identity Card (CNIC) – was held, in 2017, by 96 million out of a population of 210 million citizens. Holding a CNIC is a requirement to access Pakistan's largest social security scheme, the Benazir Income Support Programme (BISP), which provides cash transfers to around 4.7 million households in Pakistan.[75] As noted in research conducted for the UK's Department for International Development, "possession of a CNIC is required to verify IDs and is essential. It is, however, also an access barrier to the most vulnerable who are more likely not to have a CNIC". Particularly when considering the use of BISP in the case of responses to shock or disaster relief, the research found: "CNIC possession is likely to remain a core eligibility criterion to access any type of disaster relief but, at least at the moment, this criterion is likely to exclude those who need support the most…The biggest hurdle to rapidly accessing relief is the CNIC."[76]

5. Recommendations

Privacy International is very concerned by the tendency of States and other actors to present AI applications and other technologies relying on processing of vast amout of personal data as solutions to structural and systemic societal issues. States have an obligation to ensure the equal enjoyment of human rights by all people and should refrain from introducing technologies that risk perpetuating or even amplifying existing inequalities.

---

[72] UN Secretary-General, 2020, *Report on the role of new technologies for the realization of economic, social and cultural rights*, https://www.ohchr.org/en/documents/reports/ahrc4329-report-role-new-technologies-realization-economic-social-and-cultural , para 33.

[73] PI, 2018, *Exclusion and identity: Life without* ID, https://privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id

[74] PI, 2021, *My ID, My Identity? The impact of ID systems on transgender people in Argentina, France and the Philippines*, https://privacyinternational.org/long-read/4372/my-id-my-identity-impact-id-systems-transgender-people-argentina-france-and

[75] Seyfert and Ahmad, 2020, *Options for making Pakistan's flagship national cash transfer programme shock-responsive,* https://www.opml.co.uk/files/Publications/A2241-maintains/making-bisp-shock-responsive-14062021.pdf?noredirect=1

[76] *ibid.*

In light of the above analysis, PI suggests that the report of the High Commissioner for Human Rights makes the following recommendations:

- States to refrain from using AI and other technologies that may have discriminatory impacts or risk amplifying existing structural and systemic inequalities;

- States to ban the deployment of technologies, such as facial recognition in public spaces and in schools, where the risks of discriminatory outcomes are high and undermine the enjoyment of fundamental human rights such as freedom of assembly and association and right to access to education;

- States to adopt or review existing discrimination laws and modern data protection legislation to address the risks of discrimination. Additionally, States should reform the surveillance legislation to provide enjoyment of the right to privacy without discrimination, including equal human rights safeguards;

- States to adopt robust anti-discrimination policies that address biases in digital technologies, including ensuring that AI systems do not perpetuate or exacerbate existing inequalities;

- States to refrain from making access to public services, including social benefits and healthcare, conditional upon digital identification and to ensure that any involvement of AI in the decision-making process of the provision of public services, undergo thorough human rights analysis to prevent discriminatory outcomes;

- States to encourage the development of digital tools and platforms that are designed inclusively, taking into account the diverse needs of different populations to prevent discrimination;

- States to implement regular audits and bias detection mechanisms in AI systems to identify and mitigate discriminatory outcomes, in particular in the provision of public services;

- States to ensure that all public servants have appropriate training in the use of AI technologies and the probabilistic nature of their outcomes;

- States to refrain from deploying experimental untested technologies in the provision of public services, particularly against groups found in precarious situations, such as in the context of migration management and border security;

- States and businesses to explicitly include in their human rights due diligence policies, an assessment of the potential discriminatory impacts of the processing of personal data throughout the lifecycle of any technology deployment.