Privacy International's submission in advance of the consideration of the United Kingdom at the 77th session of Committee on Economic, Social and Cultural Rights

January 2025

Introduction

This submission is ahead of the 77th Session of the Committee on Economic Social and Cultural Rights that will take place between 10 and 28 February 2025 in relation to the consideration of the the United Kingdom of Great Britain and Northern Ireland's compliance with the International Covenant on Economic, Social and Cultural Rights (ICESCR).

Privacy International (PI) is a global advocacy and campaigning group that works at the intersection of technology and human rights. PI campaigns against companies and governments who exploit our data and technologies. We expose harm and abuses, mobilise allies globally, campaign with the public for solutions, and pressure companies and governments to change.

Our submission will cover issues relating to Articles 2, 7, 9, 11, 12 and 13 of ICESCR.

1. **Surveillance of welfare fraud (Articles 2, 9, 11)**

PI has documented the increasing surveillance capabilities of the UK government's Department for Work and Pensions (DWP), including covert surveillance which threatens individual's access to social security, particularly those from marginalised and vulnerable populations.[1] The expansion includes the use of algorithms to scan millions of bank accounts and potentially granting access to individuals' financial information or allowing authorities to withdraw funds directly.[2] The UK government justifies the use of these powers to combat fraud, but PI believes that these measures are not proportionate and not in accordance with the UK's obligations under the Covenant.

The reliance on technology, especially artificial intelligence (AI), for exercising these new powers is particularly concerning, as it is prone to errors and biases, and no safeguards can fully eliminate the risk of mistakes.[3] The result of erroneous investigations could unjustly withhold access to society security, leaving individuals unable to afford necessities. Moreover, the lack of transparency in how

[1] Privacy International, 'Shedding light on the DWP Part 1 - We read the UK welfare agency's 995-page guide on conducting surveillance and here are the scariest bits', February 2021. https://privacyinternational.org/long-read/4395/shedding-light-dwp-part-1-we-read-uk-welfare-agencys-995-page-guide-conducting

[2] The Guardian, 'UK government failing to list use of AI on mandatory register', 28 November 2024. https://www.theguardian.com/technology/2024/nov/28/uk-government-failing-to-list-use-of-ai-on-mandatory-register

[3] The Guardian, 'AI use widened to assess universal credit applications and tackle fraud', 11 July 2023. https://www.theguardian.com/society/2023/jul/11/use-of-artificial-intelligence-widened-to-assess-universal-credit-applications-and-tackle

the DWP conducts fraud investigations, particularly regarding the triggers for investigations and the thresholds for action, compounds this issue further.[4]

Such powers also pose specific risks to marginalised populations such as persons with disabilities, due to the propensity of the computer algorithms used by the DWP to discriminate against them.[5] An internal assessment of the DWP machine-learning programme used to vet thousands of universal credit claims across England has revealed troubling evidence of algorithmic bias.[6] The assessment, disclosed through a Freedom of Information request, identified a "statistically significant outcome disparity" in how the automated system recommended fraud investigations. According to The Guardian, it disproportionately targeted individuals based on characteristics such as age, disability, marital status, and nationality.[7]

The DWP is facing legal action by a disability rights group, claiming that the algorithm used to flag individuals as 'fraud risks' is unfair and discriminatory.[8] According to their claim, by profiling individuals who interact with caseworkers and the DWP based on unknown data points, the DWP is creating derived, inferred, and predicted profiles which may be inaccurate or systematically biased. This type of profiling can lead to individuals being misidentified, misclassified, or misjudged, increasing their vulnerability to poverty and marginalisation, as recognised by the UN Special Rapporteur on the Rights of Persons with Disabilities.[9]

Fraud, Error, and Debt Bill

The UK government plans to introduce a new Fraud, Error, and Debt Bill aimed at "cracking down on fraud in the social security system".[10] While the bill has not yet been tabled, the government suggests that it will allow DWP to request data from banks and financial institutions to identify customers who may not meet eligibility rules for benefits and recover debts from those who can repay but have avoided doing so.[11] We are deeply concerned that the proposed approach on eradicating fraud which overlooks the essential framing of social security as a fundamental human right. Instead of punitive measures and policing social security, the government should prioritise equitable access to social protection, free from discrimination, while safeguarding recipients' dignity.[12] PI has documented these practices and developed a framework for examining social benefits through a human rights lens.[13]

---

[4] Privacy International, 'Shedding light on the DWP Part 2 - A Long Day's Journey Towards Transparency', 14 February 2021, https://privacyinternational.org/long-read/4397/shedding-light-dwp-part-2-long-days-journey-towards-transparency; Privacy International, 'Stage 3 - The policing of social benefits: punishing poverty', 7 August 2019, https://privacyinternational.org/node/3114.

[5] Privacy International, 'Submission to the OHCHR on the rights of persons with disabilities', 17 August 2023, https://privacyinternational.org/advocacy/5107/submission-ohchr-rights-persons-disabilities

[6] https://www.whatdotheyknow.com/request/ai_strategy_information/response/2748592/attach/6/Advances%20Fairness%20Analysis%20February%2024%20redacted%201.pdf?cookie_passthrough=1

[7] The Guardian, 'Revealed: bias found in AI system used to detect UK benefits fraud', 6 December 2024, https://www.theguardian.com/society/2024/dec/06/revealed-bias-found-in-ai-system-used-to-detect-uk-benefits.

[8] See GMCDP & Foxglove Legal Challenge to the Department for Work and Pensions DWP Fraud Algorithm https://gmcdp.com/gmcdp-foxglove-legal-challenge-department-work-and-pensions-dwp-fraud-algorithm.

[9] A/HRC/49/52 UN Human Rights Council, Report of the Special Rapporteur on the rights of persons with Disabilities, 28 December 2021. https://www.undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F49%2F52&Language=E&DeviceType=Desktop&LangRequested=False

[10] Department for Work and Pensions, 'Press release: New laws to be introduced to crack down on fraud', 24 September 2024, https://www.gov.uk/government/news/new-laws-to-be-introduced-to-crack-down-on-fraud.

[11] Ibid.

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

[13] Privacy International, 'Researching social benefits systems', https://privacyinternational.org/researching-social-benefits

2. Intrusive surveillance technologies impact mental and physical health of migrants and restrict access to social security and healthcare (Articles 2, 9, 11, 12)

The UK Home Office Electronic Monitoring Programme deploys a range of highly invasive surveillance tools on migrants including fitted GPS ankle tags, non-fitted GPS fingerprint scanners (non-fitted devices), and algorithmically powered immigration decision-making systems like Identify and Prioritise Immigration Cases' (IPIC).[14] This places migrants and asylum seekers under constant surveillance which have reported detrimental impacts to their mental and physical health.[15]

With respect to the use of GPS ankle tags, civil society organisations carried out research that demonstrated that the imposition of ankle tags as a condition of immigration bail has consistently caused anxiety, stress, discomfort, and pain in wearers.[16] The research involved numerous interviews with tag wearers.[17] In several case studies tag wearers described the impacts as akin to "torture".[18] Wearers highlighted its stigmatising impact given the association between tagging and criminal offending, which in turn was said to have caused them to feel increasingly isolated.[19] Others noted the bulky size of the device, the physical presence of which reminded wearers of the constant risk of adverse immigration enforcement action including detention and/or deportation.[20] Finally, several wearers reported difficulties in sleeping due to onerous charging times – in some cases the devices were said to take up to 4 hours to fully charge. When the devices are low in battery they start vibrating, which wearers interviewed for the report said often meant that they could not sleep for long periods at a time.

In its Equality Impact Assessment (EIA) conducted prior to the introduction of the non-fitted devices, the Home Office suggested that this technology may be more suitable than ankle tags for individuals suffering from particular health conditions - including mental health conditions exacerbated by social stigma associated with fitted devices.[21] Further research by civil society organisations has however exposed significant harms stemming from technology that the EIA suggests is at least in part

---

[14] Privacy International, 'Life under 24/7 GPS surveillance - A GPS ankle tag experiment', 5th May 2023, https://privacyinternational.org/long-read/5064/life-under-247-gps-surveillance-gps-ankle-tag-experiment; Privacy International, 'Two court judgments, one regulatory decision - Bricks fall around UK's GPS tagging of migrants', 16 May 2024, https://privacyinternational.org/news-analysis/5323/two-court-judgments-one-regulatory-decision-bricks-fall-around-uks-gps-tagging; Privacy International, 'Non-fitted devices in the Home Office's surveillance arsenal: Investigating the technology behind GPS fingerprint scanners', 29 October 2024, https://privacyinternational.org/long-read/5457/non-fitted-devices-home-offices-surveillance-arsenal-investigating-technology-behind; Privacy International, 'Automating the hostile environment: uncovering a secretive Home Office algorithm at the heart of immigration decision-making', 17 October 2024, https://privacyinternational.org/news-analysis/5452/automating-hostile-environment-uncovering-secretive-home-office-algorithm-heart.

[15] Medical Justice, Bid for Immigration Detainees & Public Law Project, 'Constantly on edge: The expansion of GPS tagging and the rollout of non-fitted devices. Annual review of GPS tagging in the immigration system', December 2023, https://medicaljustice.org.uk/wp-content/uploads/2023/12/2023_Constantly-On-Edge_Final.pdf

[16] Bail for Immigration Detainees (BID), Research reveals "inhumane" effects of GPS tagging on migrants, 31 October 2022, https://www.biduk.org/articles/research-reveals-inhumane-effects-of-gps-tagging-on-migrants.

[17] BID, Medical Justice, and Public Law Project, Every Move You Make: The Human Cost of GPS Tagging in the Immigration System, October 2022, https://hubble-live-assets.s3.amazonaws.com/biduk/file_asset/file/682/GPS_Tagging_Report_Final.pdf.

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] UK Home Office, Equality Impact Assessment: GPS non-fitted devices (accessible), Updated 23 October 2024, https://www.gov.uk/government/publications/offender-management/equality-impact-assessment-gps-non-fitted-devices-accessible.

deployed in order to mitigate the detriment suffered by ankle tag wearers.[22] In particular, the research points to the fact that the randomness of daily prompts to provide one's fingerprints contributes to individuals subjected to the monitoring feeling as though they are "in a constant state of alertness and in a heightened sense of being under constant surveillance".[23] The research shows through the anonymised interviews that this in turn impacts the enjoyment of basic everyday activities - such as being able to sleep properly. Subjects also reported that having too little time (e.g., 1 minute) to provide their fingerprints contributed to the feelings of anxiety and stress they felt.[24]

The IPIC system processes migrants' personal data collected through immigration enforcement activities, from information about their health to their GPS tracking and bail conditions, all without their knowing.[25] The algorithm that processes this data, among a multiple of other categories of personal information, makes recommendations about whether to subject an individual to a particular immigration enforcement action. The Home Office has refused to disclose the nature of the recommendations and the enforcement actions in relation to which they are used. It is clear from several training materials disclosed from the Home Office in response to a PI complaint, that the IPIC's algorithmic outputs can include recommendations for referrals by the Home Office to other government departments for the cessation or limitation of certain public services and welfare benefits where a migrant is suspected of not having immigration status. The relevant Home Office policy includes referrals relating to the charging of National Health Service (NHS) treatment in cases where individuals do not have immigration status.[26]

There is therefore an urgent need for greater transparency as regards how sensitive health data is being used in algorithmic decision-making for the purposes of immigration enforcement decisions and regarding access to social security and healthcare.

3. The right of everyone to the enjoyment of the highest attainable standard of physical and mental health (Article 12)

General Comment 14 of the CESCR outlines the that the realisation of the right to health is dependent on other rights including the right to privacy and healthcare should respect confidentiality and privacy.[27] Increasingly healthcare in the UK is being digitalised and we are seeing new technologies being used in healthcare, as well as the increasing involvement of private sector actors in healthcare, which are all presenting new threats to the realisation of the right to health and wider rights.

---

[22] Public Law Project, 'Constantly on Edge': The expansion of GPS tagging and the rollout of non-fitted devices, 20 December 2023, https://publiclawproject.org.uk/resources/constantly-on-edge-annual-review-of-gps-tagging-in-the-immigration-system-2023/.

[23] Ibid.

[24] Ibid.

[25] Privacy International, 'Automating the hostile environment: uncovering a secretive Home Office algorithm at the heart of immigration decision-making', 17 October 2024, https://privacyinternational.org/news-analysis/5452/automating-hostile-environment-uncovering-secretive-home-office-algorithm-heart; See freedom of information request: https://www.whatdotheyknow.com/request/identify_and_prioritise_immigrat_3/response/2780331/attach/5/04608%20Privacy%20International%20Annex%20C.pdf?cookie_passthrough=1

[26] UK Home Office, 'Immigration Removals, Enforcement and Detention General Instructions. Sanctions: refer case to Interventions and Sanctions Directorate (ISD)', 17 January 2018, https://assets.publishing.service.gov.uk/media/5a82ccb3e5274a2e87dc30aa/ISD-referrals-and-sanctions-v3.0ext.pdf; See freedom of information request: https://www.whatdotheyknow.com/request/identify_and_prioritise_immigrat_3#outgoing-1735546

[27] CESCR General Comment No. 14: The Right to the Highest Attainable Standard of Health (Art. 12) https://www.ohchr.org/sites/default/files/Documents/Issues/Women/WRGS/Health/GC14.pdf

The UK government is currently consulting on the development of their 10 Year Health Plan which will transform the NHS from analogue to digital.[28] The government has suggested that this will include plans to introduce 'patient passports' containing health data that can be accessed across health services.[29] These single patient records will combine a range of different data (including health information and test results) in one place, which could be potentially accessed by up to 1.5 million NHS staff without appropriate safeguards to uphold rights and ensure protections against abuse.[30] The Data Use and Access Bill, currently making its way through Parliament, supports this initiative by containing new legal provisions to facilitate the transfer of patient data across the NHS.[31] England's Women's Health Strategy also included within its 10-year plan to make greater use of technologies such as period tracking and menopause apps and femtech more generally.[32]

PI is also concerned about reports that UK healthcare data records could be combined with other forms of public sector data, for example social housing data and employment and earnings data, which may result in re-identification, discrimination, or restricting access to health services.[33]

New technologies in healthcare

UK healthcare professionals are increasingly reported to be using social media and AI tools without adequate safeguards for patient confidentiality and privacy.[34] Further still some AI tools can also lead to discriminatory outcomes if trained on biased data sets and may lead to discrimination and exclusion of marginalised groups including on grounds of race, gender, class, migration status, disability, sexual orientation and gender identity. The issue was raised by the UN Special Rapporteur on contemporary forms of racism in her thematic report on AI and racism to which PI provided input during the call for evidence.[35] The rapporteur specifically drew out health as an important sector and specifically highlighted an example of skin cancer detection technology showing poorer performance

---

[28] See: https://change.nhs.uk/en-GB/.

[29] The Guardian, 'Wes Streeting unveils plans for 'patient passports' to hold all medical records', 21 October 2024, https://www.theguardian.com/society/2024/oct/21/wes-streeting-unveils-plans-for-patient-passports-to-hold-all-medical-records.

[30] Department for Health and Social Care, 'Press release: Government issues rallying cry to the nation to help fix NHS', 21 October 2024, https://www.gov.uk/government/news/government-issues-rallying-cry-to-the-nation-to-help-fix-nhs; See: https://x.com/BBCr4today/status/1848286462900326893; The Guardian, 'Warnings over NHS data privacy after 'stalker' doctor shares woman's records', 14 May 2023, https://www.theguardian.com/society/2023/may/14/nhs-england-data-privacy-confidentiality-records-addenbrookes-hospital.

[31] See: https://bills.parliament.uk/bills/3825; Digital Health, 'New data laws will allow patient data to be shared across the NHS', 24 October 2024, https://www.digitalhealth.net/2024/10/new-data-laws-will-allow-patient-data-to-be-shared-across-the-nhs/.

[32] Department for Health and Social Care, 'Policy paper: Women's Health Strategy for England', 30 August 2022, https://www.gov.uk/government/publications/womens-health-strategy-for-england/womens-health-strategy-for-england.

[33] Public Technology, 'Liverpool NHS trust to combine social housing and health data', 1 November 2024, https://www.publictechnology.net/2024/11/01/health-and-social-care/liverpool-nhs-trust-to-combine-social-housing-and-health-data/; NHS England, 'News: World leading NHS trial to boost health and support people in work', 5 December 2024, https://www.england.nhs.uk/2024/12/world-leading-nhs-trial-to-boost-health-and-support-people-in-work/; Office for National Statistics, 'Press Release: The impact of bariatric surgery on monthly employee pay and employee status, England', 23 October 2024, https://www.ons.gov.uk/peoplepopulationandcommunity/healthandsocialcare/healthandwellbeing/articles/theimpactofbariatricsurgeryonmonthlyemployeepayandemployeestatusengland/april2014todecember2022.

[34] Financial Times, 'NHS Staff use WhatsApp 'Constantly' to Share Private Patient Data', https://www.ft.com/content/c19fe8bf-0fd3-42bf-8e07-8f4e5d26ec25; The Guardian, 'One in five GPs use AI such as ChatGPT for daily tasks, survey finds', 17 September 2024, https://www.theguardian.com/society/2024/sep/17/one-in-five-gps-use-ai-such-as-chatgpt-for-daily-tasks-survey-finds.

[35] Privacy International, 'PI seeks to inform report on AI and racial discrimination of the UN Special Rapporteur on racism', 9 April 2024, https://privacyinternational.org/advocacy/5295/pi-seeks-inform-report-ai-and-racial-discrimination-un-special-rapporteur-racism

for individuals with darker skin tones, because many of the publicly available image data sets used to train them are biased, with a lack of diversity in skin tones and ethnic backgrounds.[36]

Private actors' involvement in healthcare

The involvement of private actors also poses risks to the right to privacy and health, as the proliferation of personal health data gives rise to the risk of security systems being breached through malware and hackers, as well as the risk that personal data will be sold to third parties for uses not originally consented to.[37]

Throughout the Covid-19 Pandemic the UK government awarded at least £1.7 billion in contracts to private companies, most of them without a competitive tender.[38] Most notably, the UK Government granted Palantir a £1 contract allowing them to access reportedly unprecedented quantities of NHS patient data during the pandemic.[39] Palantir is a US based data analytics firm who have numerous contracts with intelligence agencies, military forces, or law enforcement and immigration authorities that have raised human rights concerns.[40] Yet despite this track record the UK government awarded Palantir a £330m contract to create a new Federated Data Platform (FDP) in November 2023.[41] Palantir's CEO has already suggested that its FDP may also help sell NHS data and reports emerged that data collected across the FDP could be used to train AI models.[42] The government have already faced legal action regarding access to their contract with Palantir over significant redactions and lack of transparency around the intentions of the partnership.[43]

A contract has also been awarded to biotech company, IQVIA, which has also raised concerns about a lack of a legal basis for the data processing by the privacy-enhancing technology as part of the (FDP).[44] I

As noted above, plans to create single patient records will also facilitate greater access to primary data for private companies and researchers.[45]

---

[36] A/HRC/56/68 Human Rights Council, 'Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Ashwini K.P.', 3 June 2024, https://documents.un.org/doc/undoc/gen/g24/084/20/pdf/g2408420.pdf

[37] A/HRC/53/65 Human Rights Council, 'Report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health', 21 April 2023, 'https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F53%2F65&Language=E&DeviceType=Desktop&LangRequested=False

[38] Privacy International, 'UK awards £1.7 billion in coronavirus-related contracts', 4 June 2020, https://privacyinternational.org/examples/4032/uk-awards-ps17-billion-coronavirus-related-contracts

[39] Digital Health, 'Palantir's road to the Federated Data Platform contract: a timeline', 21 November 2023, https://www.digitalhealth.net/2023/11/palantirs-road-to-the-federated-data-platform-contract-a-timeline/

[40] See: https://www.palantir.com/uk/; Amnesty International, 'Failing to do Rights: The Urgent Need for Palantir to Respect Human Rights', September 2020, https://www.amnestyusa.org/wp-content/uploads/2020/09/Amnest-International-Palantir-Briefing-Report-092520_Final.pdf.

[41] See: https://privacyinternational.org/examples/5299/controversial-data-analytics-firm-palantir-run-uks-health-data-platform & https://www.theguardian.com/society/2023/nov/21/patient-privacy-fears-us-spy-tech-firm-palantir-wins-nhs-contract

[42] Digital Health, 'Palantir CEO acknowledges FDP could aid NHS data being sold in future', 30 October 2023, https://www.digitalhealth.net/2023/10/palantir-ceo-acknowledges-fdp-could-aid-nhs-data-being-sold-in-future/; HSJ, 'Exclusive: AI models to be trained on Federated Data Platform', 10 December 2024, https://www.hsj.co.uk/technology-and-innovation/exclusive-ai-models-to-be-trained-on-federated-data-platform/7038320.article.

[43] Good Law Project, 'Case: We're taking legal action to uncover Palantir's blanked-out contract', https://goodlawproject.org/case/were-taking-legal-action-to-uncover-palantirs-blanked-out-contract/.

[44] The Register, 'Key aspects of Palantir's Federated Data Platform lack legal basis, lawyers tell NHS England', 5 September 2024, https://www.theregister.com/2024/09/05/fdp_lacks_legal_basis/

[45] See: https://www.iqvia.com/locations/united-kingdom ; See: https://www.progress.org.uk/uk-biobank-will-be-able-to-access-participants-gp-data/.

PI is concerned about the commoditisation of health data undermining people's ability to access quality and affordable healthcare. We are also concerned about the number of examples of poor practice of health data security within the private sector, for example:

- UK Biobank sharing data with insurance companies despite promising not to;[46]
- UK Biobank being accused of allowing a racist "race science" network to access their data;[47]
- Data of 6.9million users of 23andme being accessed by hackers;[48]
- DNA testing company Atlas Biomed disappeared without warning, leaving uncertainty about the status of highly sensitive user data and;[49]
- A workplace mental health service letting corporate clients listen in to confidential calls.[50]

All these above issues have been raised by the UN Special Rapporteur on the right to health in her report on 'Digital innovation, technologies and the right to health'.[51] The rapporteur recommended human rights impact assessments must be embedded in the design, development and implementation of new technologies, including the meaningful engagement of stakeholders.

4. New technologies in education: accessing education means a trade-off of wider rights (Article 13)

Education in the UK was rapidly driven online by during the Covid-19 pandemic. This, combined with the UK's broader uptake of education technologies in schools, has created significant risks for those accessing education, particularly those most disadvantaged.

Examples include the uptake of facial recognition technologies in schools and use of online proctoring services to prevent cheating in exams.[52] Many proctoring systems employed facial recognition technology that had difficulty recognising black student's faces, making it harder for black students to undertake their exams than their white peers.[53] Moreover, the systems are designed to flag certain behaviours for cheating such as when a person leaves the camera frame or looks away from the camera. This led to unpleasant circumstances for some students who felt the need to go to the toilet in buckets or in bottles to avoid leaving the frame.[54] Moreover, some students were flagged for cheating due to having people in the background of the camera, which could be due to not having access to a private room to take the exam.[55] It also led to students with disabilities being flagged for so called 'suspicious' behaviours.[56]

---

[46] See: https://www.theguardian.com/technology/2023/nov/12/private-uk-health-data-donated-medical-research-shared-insurance-companies
[47] See: https://www.theguardian.com/world/2024/oct/17/race-science-group-say-they-accessed-sensitive-uk-health-data
[48] See: https://www.bbc.co.uk/news/technology-67624182
[49] See: https://www.bbc.co.uk/news/articles/cz7wl7rpndjo
[50] See: https://www.bbc.co.uk/news/articles/cxee3glz2pyo
[51] A/HRC/53/65 Human Rights Council, 'Report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health', 21 April 2023, https://www.ohchr.org/en/documents/thematic-reports/ahrc5365-digital-innovation-technologies-and-right-health
[52] Open Knowledge, 'Open Knowledge Justice Programme challenges the use of algorithmic proctoring apps', 26 February 2021, https://blog.okfn.org/2021/02/26/open-knowledge-justice-programme-challenges-the-use-of-algorithmic-proctoring-apps/.
[53] Frontiers in Education, 'Racial, skin tone, and sex disparities in automated proctoring software', 20 September 2022, https://www.frontiersin.org/journals/education/articles/10.3389/feduc.2022.881449/full.
[54] Open Knowledge, 'Open Knowledge Justice Programme challenges the use of algorithmic proctoring apps', 26 February 2021, https://blog.okfn.org/2021/02/26/open-knowledge-justice-programme-challenges-the-use-of-algorithmic-proctoring-apps/.
[55] The New York Times, 'How It Feels When Software Watches You Take Tests', https://www.nytimes.com/2020/09/29/style/testing-schools-proctorio.html
[56] Hybrid Pedagogy, 'Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education', 2 April 2020, https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-

These concerns do not seem to have slowed down the UK's adoption of facial recognition without necessary safeguards in the UK. Schools in Essex and Scotland have been reprimanded by the Information Commissioner's Office (ICO) for inadequate processes in their deployment of this disturbing and invasive technology - which would seem to fail to meet the necessity and proportionality requirements for the use of this kind of technology.[57] Some schools have even installed sensors in the toilets which 'listen' to pupils and send alerts if keywords are triggered - as part of a vape sensor. Disturbingly, one headteacher whose school had installed the sensors was reportedly not aware that the sensors were listening at all.[58]

These technologies are being implemented in a context of a huge amount of data collection in UK schools- often with inadequate protections.[59] The ICO conducted an audit of the Department of Education following complaints about the department's data processes. It found significant issues in the Department's Compliance with existing law that governs data protection.[60] This failure cannot be surprising given its history, which included granting access to a database of student learning records to gambling companies.[61]

As is often inevitable after data is collected, the potential for scope creep in the re-use of such data is significant, and ministers at the Department of Education were reported to be asking questions including what the extensive data they hold might be worth.[62]

The increasing volume and sensitivity of personal data being collected in schools by the state and by private companies is hugely problematic, not only is this highly sensitive data vulnerable to unauthorised access is ways that threaten children's education and privacy rights but can also lead to adverse outcomes for children.[63] For example, one system used by schools in Bristol - which gathered data on pupils including broader data from students and their families' interactions with other part of the UK state like the police or child protection services - has been criticised for increasing the risks of discrimination for students from a minority ethnic or working-class background.[64]

5. Recommendations

education/#:~:text=Algorithmic%20test%20proctoring%20encodes%20ideal,exclusion%20from%20the%20educational%20community

[57] Information Commissioner's Office, 'Facial recognition technology in schools', https://ico.org.uk/for-the-public/ico-40/facial-recognition-technology-in-schools/; See: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/dpia-tools/online-retail/step-4-assess-necessity-and-proportionality/; Privacy International, 'Legality, Necessity and Proportionality', https://privacyinternational.org/our-demands/legality-necessity-and-proportionality.

[58] Schools Week, 'Schools install toilet sensors that 'actively listen' to pupils', 4 February 2024, https://schoolsweek.co.uk/schools-install-toilet-sensors-that-actively-listen-to-pupils/

[59] Defend Digital Me, 'The State of Data 2020', October 2020, https://defenddigitalme.org/wp-content/uploads/2020/11/The-state-of-data-2020-v2.2-1.pdf

[60] Information Commissioner's Office, 'Department for Education (DfE) Data protection audit report', February 2020, https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf.

[61] The Guardian, ''Woeful' DfE blamed as betting firms gain access to children's data', 6 November 2022, https://www.theguardian.com/education/2022/nov/06/woeful-dfe-blamed-as-betting-firms-gain-access-to-childrens-data.

[62] Schools Week, 'Minister wants schools to benefit from AI revolution', 19 June 2023, https://schoolsweek.co.uk/minister-wants-schools-to-benefit-from-ai-revolution/.

[63] The Record, 'Ransomware attack forces high school in London to close and send students home', 9 September 2024, https://therecord.media/ransomware-attack-forces-london-high-school-to-close.

[64] The Guardian, 'Call to shut down Bristol schools' use of app to 'monitor' pupils and families', 21 September 2023, https://www.theguardian.com/education/2023/sep/21/calls-to-shut-down-bristol-schools-use-of-think-family-education-app-pupils-and-families.

Based on these observations, Privacy International suggests the Committee on Economic, Social and Cultural Rights considers the following recommendations for the UK government in their concluding observations:

1. Address longstanding concerns regarding the use of surveillance mechanisms by the Department for Work and Pensions, including covert practices, by ensuring transparency, accountability, and the protection of individuals' rights within its fraud prevention initiatives.
2. Recognise and address the risks that the use of AI technologies poses to access to social benefits, including the dangers that the use of such technology lead to exclusionary and discriminatory impacts.
3. Cease the imposition of GPS tagging on migrants and adopt measures that are respectful of human rights, instead of surveillance-based technologies.
4. Ensure that the digitalisation of healthcare services does not come at cost to human rights to health and the right to privacy, including by protecting people's sensitive health data and by ensuring that the use digital innovation and technologies in healthcare do not lead to discriminatory outcomes and impacts;
5. Carry out regular human rights due diligence and impact assessments to ensure that the involvement of the private sector in the UK's provision of healthcare is compliant with the UK's obligations under the Covenant.
6. Prohibit the use of facial recognition technology (FRT) in educational settings due to its disproportionate impact, security risks, inaccuracies, and discriminatory biases that pose threats to the right to education.
7. Regulate the use of education technologies and implement regulations governing the use of EdTech in educational settings (including private institutions), ensuring alignment with robust data protection standards and to guarantee educational institutions create an environment fulfils the right to education.