Privacy International response to the inquiry of the UK Joint Committee on Human Rights to examine how human rights can be protected in the age of Artificial Intelligence (AI)

August 2025

Executive Summary

AI tools consist of intriguing technologies in an exciting phase of development. They may achieve considerable positive gains for society.

In our 30+ years of experience navigating technology and regulation, however, we've never seen a technology deployed in the UK with this level of abandon. For nearly a decade the UK Government has missed numerous opportunities to develop legal bases for the use of AI tools, and yet it keeps pushing deployment despite considerable prior government IT project failures.

We therefore recommend that the committee treat AI:

1. like any other form of technology, and expect compliance with human rights and other frameworks;
2. as a form of infrastructure that will introduce new dependencies, where accountability and independence must be maintained; and
3. as a highly adaptable form of technology deployed in specific circumstances, and protect people who will be affected in a diversity of ways.

We draw particular attention to a core aspect of AI tools and AI policy: it motivates the processing of vast amounts of personal data.

We argue that Parliament, and this Committee in particular, can play a crucial role in plugging a gap that continuously arises in UK technology policy, rather than wait until the next IT failure and crisis.

About Privacy International

Privacy International ("PI") is a registered charity (no 1147471), that works globally at the intersection of modern technologies and rights.[1] Established in 1990, PI undertakes research, litigation and advocacy to build a better future where technologies, laws and policies contain modern safeguards to protect people and their data from exploitation. PI has long documented how a diverse range of 'AI' applications and technologies are impacting people and their rights.[2]

PI welcomes the Committee's inquiry. It is timely given that many of these AI applications and technologies are already being rolled out in the UK, and their adverse effects must be urgently addressed to prevent further risks to human rights.

Full submission

Human rights issues

1. How can Artificial Intelligence (AI) affect individual human rights for good or ill, in particular in the areas of:

Data is an essential component for the development and use of AI. Often these systems process personal data and make decisions that affect people's dignity and autonomy. As governments choose to invest directly, de-regulate, and promote deployment of these tools, they're fuelling a new infrastructure that will have ramifications on the fabric of power in our societies.

AI is a periodically fascinating part of computer science with a myriad of compelling applications. 'AI' is also a domain full of speculation, ambition, and science fiction. Given the broad usage of the term of AI,[3] at PI we always focus on a given domain of use (e.g. health, police, conflict) and specific types of AI applications (e.g. analysis, prediction) and the context into which they are deployed (e.g. workplace, public events), the purpose, and who is affected (e.g. general public, children, health communities, migrants) as they impact of a variety of rights, and raise specific regulatory issues.[4]

Whilst at the core it starts with data and how it is used, exploited, and manipulated, triggering the right to privacy in an array of manners, AI applications and technologies can affect the whole range of human rights depending on how they are being used, by who and for what purpose.[5] There is evidence that they are disproportionally affecting particular communities

---

[1] https://privacyinternational.org/

[2] PI, Artificial Intelligence, Explainer, https://privacyinternational.org/learn/artificial-intelligence

[3] It can encompass machine learning (which makes inferences, predictions and decision and other actions), 'traditional' Large Language Models and 'visual' models including computer vision, domain-specific AI applications, fully autonomous and connected objects, and the poorly defined Artificial General Intelligence or even the futuristic idea of an AI 'singularity'.

[4] On definitions of different AI applications and techniques, see PI and ARTICLE 19, Privacy and Freedom of Expression In the Age of Artificial Intelligence, April 2018, pp. 6-7, https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf,

[5] As noted by the UN General Assembly resolution on the right to privacy in the digital age, "*artificial intelligence or machine-learning technologies […] may lead to decisions that have the potential to affect the enjoyment of human*

from benefit claimants, people on the move, children, persons with disabilities, and those already marginalised and subject to discrimination on the basis of gender, race or ethnicity, to name a few. [6]

With great care and assurance, technology can be used to help and empower people; too often however we see governments and industry prioritise exploitative development and applications.

Without aiming to be comprehensive, here are some instances:

- Despite **Facial Recognition Technology (FRT)** use being documented in the UK in 2017, no existing legal or regulatory frameworks have been applied nor restrictions or safeguards for its use, the use of including live/real-time. FRT is being used for policing including live monitoring in public spaces,[7] in retails spaces[8], on public transport,[9] and at sport venues.[10] We've also tracked how some specific FRT tools are developed using problematic sources of data including scraping images from social media[11], using systems from conflict zones[12], or using government databases[13].

---

rights, including economic, social and cultural rights, and affect non-discrimination", See: The right to privacy in the digital age, GA Res 75/176, 16 December 2020, https://undocs.org/A/RES/75/176.) See also PI, Artificial Intelligence, Explainer, https://privacyinternational.org/learn/artificial-intelligence

[6] These include rights protected by the Human Rights Act from rights to freedom of expression, freedom of peaceful assembly, education, freedom of movement, to seek asylum, to social security, health, fair working conditions, non-discrimination.

[7] Sky News, Police to expand use of live facial recognition technology - amid concern from campaigners, 31 July 2025, https://news.sky.com/story/police-to-expand-use-of-live-facial-recognition-technology-amid-concern-from-campaigners-13404404; Callum Cuddeford, Anti-knife activist brings legal challenge to Met after he's detained in facial recognition failure, MyLondon, 4 June 2024, https://www.mylondon.news/news/south-london-news/anti-knife-activist-brings-legal-29285138; Daniel Boffey and Mark Wilding, Live facial recognition cameras may become 'commonplace' as police use soars, The Guardian, 24 May 2025, https://www.theguardian.com/technology/2025/may/24/police-live-facial-recognition-cameras-england-and-wales

[8] TechInformed, Asda launches facial recognition tech trial, 3 April 2025, https://techinformed.com/asda-launches-facial-recognition-tech-trial/; See also: On 25 July 2024, PI co-signed a letter alongside UK civil society organisations campaigning against the use of facial recognition, to retailers across the UK calling on them to not use live FRT within their stores,.https://privacyinternational.org/advocacy/5351/joint-letter-uk-retailers-regarding-potential-use-facial-recognition-technology-frt

[9] Ross Lydall, Tube fare dodging: live facial recognition cameras could be used to catch most prolific evaders, The Standard, 9 July 2025, https://www.standard.co.uk/news/transport/facial-recognition-cameras-fare-dodging-tube-london-underground-tfl-b1237049.html

[10] Wired, Soccer Fans, You're Being Watched, 3 November 2022, https://www.wired.com/story/soccer-world-cup-biometric-surveillance

[11] PI, Challenge against Clearview AI in Europe, https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe

[12] PI, Biometrics and counter-terrorism: Case study of Israel/Palestine, 28 May 2021, https://privacyinternational.org/report/4527/biometrics-and-counter-terrorism-case-study-israelpalestine includes reporting on AnyVision that was used at checkpoints in the occupied territories, that was then used by Waltham Forest Council according to this report https://walthamforestecho.co.uk/2020/08/17/councils-facial-recognition-trial-should-concern-us-all/

[13] PI, Revealed: "Skyrocketing" scale of UK police's Secret Facial Recognition Searches of Passport and Immigration Databases, 7 August 2025, https://privacyinternational.org/news-analysis/5635/revealed-skyrocketing-scale-uk-polices-secret-facial-recognition-searches

- In the **context of education and in schools**[14] in the UK, including the use of LLMs[15] and teacherless AI classrooms[16], and facial recognition in educational spaces[17] including to manage 'cashless catering'.[18]

- Adding to existing concerns with the use of **social media monitoring**[19] by law enforcement and other public bodies[20] in the UK without appropriate legal frameworks or remedies, this data can potentially feed AI applications used in a variety of contexts, from predictive policing[21], to monitoring migration routes[22], to investigating fraud of welfare services and other minor offences[23], and to target people in war.

- In the context of **welfare and social security**, the UK Department for Work and Pensions (DWP) has used algorithms for fraud prevention. In 2019, we uncovered that DWP used an algorithm to identify and investigate individuals as part of its fraud investigation, but in opaque manner,[24] and in 2024 the DWP announced it would explore 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.[25]

- **Gig economy** workers are subject to opaque algorithmic decisions being made about them that determines, without their knowledge, their likelihood to get work and get

---

[14] Privacy International's response to the call for contributions on artificial intelligence in education and its human rights-based use at the service of the advancement of the right to education, May 2024, https://privacyinternational.org/examples/5222/uk-government-seeks-ensure-schools-benefit-llm-use-pupils-data
[15] Freddie Whittaker, Minister wants schools to benefit from AI revolution, Schools Week, 19 June 2023, https://schoolsweek.co.uk/minister-wants-schools-to-benefit-from-ai-revolution/
[16] Mickey Caroll, UK's first 'teacherless' AI classroom set to open in London, Sky news, 31 August 2024, https://privacyinternational.org/examples/5650/uks-first-teacherless-ai-classroom-set-open-london
[17] PI, Why you should be worried about facial recognition in educational spaces, October 2024, https://privacyinternational.org/advocacy/5469/pis-briefing-critical-examination-facial-recognition-implementation-educational
[18] ICO, North Ayrshire Council's use of Facial Recognition Technology in its schools, https://ico.org.uk/media2/migrated/4023847/ico-letter-to-nac-appendix.pdf; ICO, Statement: Using FRT in schools – letter to North Ayrshire Council, 31 January 2023, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/01/using-frt-in-schools/
[19] PI, Social Media Intelligence, Explainer, https://privacyinternational.org/explainer/55/social-media-intelligence
[20] See: PI, When Local Authorities aren't your Friends, 24 May 2020, https://privacyinternational.org/report/3584/when-local-authorities-arent-your-friends
[21] PI, How predictive policing technology can lead to discrimination and profiling", 18 March 2019, https://privacyinternational.org/node/2720.
[22] PI, Who supplies the data, analysis, and tech infrastructure to US immigration authorities?, 9 August 2018, https://privacyinternational.org/long-read/2216/who-supplies-data-analysis-and-tech-infrastructure-us-immigration-authorities
[23] 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; PI, 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
[24] ; PI, 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
[25] Robert Booth, UK government failing to list use of AI on mandatory register, The Guardian, 28 November 2024, https://www.theguardian.com/technology/2024/nov/28/uk-government-failing-to-list-use-of-ai-on-mandatory-register

paid for that work.[26] We are calling on food delivery platforms in the UK (and the EU) to respect their workforce and improve transparency and explainability. [27]

- Regarding the **employment and recruitment sector,** PI responded to the ICO's consultation on its draft guidance for employers and recruiters on deploying AI in recruitment. Our response focuses on candidates' employment rights that may be undermined by algorithmic decision-making (ADM).[28]

- Employers monitoring employees' productivity as part of a wider trend of **workplace surveillance** raises concerns regarding workers' rights to privacy and data protection.[29]

- There are growing concerns with how **intelligence and security agencies** in the UK may be using AI to collect and analyse large amounts of data about individuals. This would likely entail data from multiples sources - including bulk datasets of sensitive personal data such as financial records, medical information and intercepted communications.[30] We've tracked instances of governments using AI tools to create LLMs of targeted populations languages, contexts, and biometrics.

Privacy and data usage

Some of the key concerns regarding AI and privacy are:

- **Vast and mass processing of personal data:** AI systems rely on large data sets, often including personal data. The push for AI development and deployment therefore incentivizes widespread collection, storage and processing of vast amount of data.
- **Automated decision making:** Some AI applications can be opaque to individuals, regulators, or even the designers of the system themselves, making it difficult to challenge or interrogate outcomes. There are also concerns with the probabilistic nature of the predictions too.[31] Sometimes the outcome has significant impacts on people's lives with AI tools being used to decided and/or inform decisions about whether someone is deserving of welfare and access to other public services, whether an asylum seeker should be subject to deportation or electronic monitoring.

---

[26] PI, Managed by Bots: surveillance of gig economy workers, 13 December 2021, https://privacyinternational.org/long-read/4709/managed-bots-surveillance-gig-economy-workers; See also: https://gigeconomy.privacyinternational.org/

[27] PI, Time to deliver answers: An open letter to Just Eat Takeaway, Uber and Deliveroo, 13 January 2025, https://privacyinternational.org/advocacy/5509/time-deliver-answers-open-letter-just-eat-takeaway-uber-and-deliveroo

[28] PI, AI-powered employment practices: PI's response to the ICO's draft recruitment and selection guidance, 22 March 2024, https://privacyinternational.org/advocacy/5287/ai-powered-employment-practices-pis-response-icos-draft-recruitment-and-selection

[29] PI, WFH - Watched from Home: Office 365 and workplace surveillance creep, 15 June 2022, https://privacyinternational.org/long-read/4909/wfh-watched-home-office-365-and-workplace-surveillance-creep

[30] Bill Goodwin, Investigatory powers: Guidelines for police and spies could also help businesses with AI, Computer Weekly, 4 June 2025, https://www.computerweekly.com/news/366625073/Investigatory-powers-Guidelines-for-police-and-spies-could-also-help-businesses-with-AI

[31] Report of the United Nations High Commissioner for Human Rights, right to privacy in the digital age, U.N. doc: A/HRC/48/31, para 24, https://docs.un.org/en/A/HRC/48/31

- **Inference of personal data, profiling and prediction:** AI applications make inferences about individuals' characteristic and behaviours based on data. As such AI technologies challenge the distinction between categories of data, including personal data and sensitive personal data. Highly sensitive information can be inferred or predicted from non-sensitive types of data. When sensitive personal data, such as data about race, ethnicity, or political beliefs can be inferred or predicted from unrelated data this poses significant challenges to the right to privacy and right to non-discrimination amongst others.[32]
- **Super-powers surveillance:** AI technologies challenge the capacity to remain anonymous online and off-line, with serious implications for the rights to privacy, freedom of expression and peaceful assembly. The systematic collection of personal data even from public spaces is widely recognised as an inference with right to privacy. Yet this has been a long- standing practice without transparency, regulation or oversight.[33] AI systems are supporting intelligence agencies and law enforcement authorities to collect and analyse the personal data of individuals. This includes activities in physical spaces (e.g. FRT) and in digital spaces (e.g. social media intelligence).

Discrimination and bias

There are risks of exacerbating discriminatory practices, particularly when AI technologies and applications are used to interpret data to predict future behaviours or infer characteristics on the basis of race, ethnicity, religion, amongst others.[34]

The use of AI by the UK in various sectors has raised serious concerns about discrimination such as persons with disabilities in the context of a DWP machine-learning system used to vet thousands of universal credit claims across England has revealed troubling evidence of algorithmic bias and the DWP had faced legal action by a disability group as a result,[35] and in the use of FRT that may misidentify individuals more often if they are women, people of colour

---

[32] See: PI's submission for the UNSR on racism's thematic report on artificial intelligence (AI) and racial discrimination, March 2024, https://privacyinternational.org/advocacy/5295/pi-seeks-inform-report-ai-and-racial-discrimination-un-special-rapporteur-racism

[33] Report of the United Nations High Commissioner for Human Rights, The Right to Privacy in the digital age, U.N. doc: A/HRC/48/31, https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high; See also jurisprudence of the European Court of Human Rights, such as Case of Perry v. the United Kingdom, (Application no. 63737/00), 17 October 2003, https://hudoc.echr.coe.int/eng?i=001-61228

[34] Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, U.N. doc. A/HRC/56/68, https://docs.un.org/en/A/HRC/56/68; Privacy International's submission for the UNSR on racism's thematic report on artificial intelligence (AI) and racial discrimination, https://privacyinternational.org/sites/default/files/2024-05/PI submission on AI and racial discrimination to UNSR on racism on AI_March 2024.pdf

[35] This legal action has now concluded, see: Foxglove, We forced the DWP to explain its benefits fraud algorithm: here's what we found, 2 May 2025, https://www.foxglove.org.uk/2025/05/06/dwp-explain-benefits-fraud-algorithm/. For background 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; https://www.whatdotheyknow.com/request/ai_strategy_information/response/2748592/attach/6/Advances%20Fairness%20Analysis%20February%2024%20redacted%201.pdf?cookie_passthrough=1; Robert Booth, Revealed: bias found in AI system used to detect UK benefits fraud, The Guardian , 6 December 2024, https://www.theguardian.com/society/2024/dec/06/revealed-bias-found-in-ai-system-used-to-detect-uk-benefits;

and people from minority and ethnic backgrounds, revealing underlying racial and gender biases in the system and subjecting particular communities to greater scrutiny.[36]

Existing legal and regulatory framework

2. To what extent does the UK's existing legal framework provide sufficient protections for human rights in relation to AI?

Currently, there is no general statutory regulation of AI in the UK. Some efforts have been made by the UK to consider the use and regulation of AI through the AI Opportunities Action Plan (2025) and the AI Regulation White Paper (2023), but these don't constitute a robust legal framework as they are not legally binding instruments.

The UK has existing legal obligations to protect people and their rights in relations to AI as under:

- national and international human rights law, including the HRA 1998, and the ICCPR, and
- data protection legislation.[37]

However, we find a lack of effective enforcement of these legal obligations as illustrated by the concerning decisions of the UK government to deploy new technologies in a variety of sectors without due respect to them, as we have documented in the sectors of immigration enforcement[38] and in relations to encryption[39], for example, and there are concerns that a similar approach is being taken for the deployment of AI as illustrated by the concerned outline above.

Furthermore, data protection law alone may not be sufficient to protect human rights in relation to AI. First, this is first due to exemptions awarded to processing by law enforcement or for

---

[36] See: INCLO, Eyes on the Watchers: Challenging the Rise of Police Facial Recognition, https://inclo.net/wp-content/uploads/2024/03/INCLO-FRT-Principles-Final.pdf; Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, U.N. doc. A/HRC/56/68, https://docs.un.org/en/A/HRC/56/68; PI's submission for the UNSR on racism's thematic report on artificial intelligence (AI) and racial discrimination, March 2024, https://privacyinternational.org/advocacy/5295/pi-seeks-inform-report-ai-and-racial-discrimination-un-special-rapporteur-racism

[37] In particular the General Data Protection Regulation ((EU) 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (UK GDPR) and the Data Protection Act 2018 (DPA 2018)

[38] See: PI, PI alerts regulator about the use of algorithms by the UK Government and their impact on migrants, 15 August 2025, https://privacyinternational.org/long-read/5639/pi-alerts-regulator-about-use-algorithms-uk-government-and-their-impact-migrants; PI, 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; PI, GPS tagging of migrants unlawful, UK authority finds after PI complaint, 29 February 2024, https://privacyinternational.org/news-analysis/5261/gps-tagging-migrants-unlawful-uk-authority-finds-after-pi-complaint

[39] PI, Update: Our case against UK Government's secret surveillance orders to be heard in 2026, 24 July 2025, https://privacyinternational.org/news-analysis/5624/update-our-case-against-uk-governments-secret-surveillance-orders-be-heard-2026

national security purposes. Second, AI technologies raise specific challenges to data protection law. These include:

- 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 based around the idea of extracting information from data and these technologies develop ways to identify individuals from data that would historically be considered non-personal data.
- 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.
- Finally, 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.

It is essential that we consider the wider range of laws relevant to AI technologies, including equality, 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. To what extent is the Government's policy approach to deploying AI, expressed in its "AI Opportunities Action Plan", sufficiently robust in respect of safeguarding human rights?

The Action Plan makes no direct reference to human rights, and the only reference to privacy and data protection is in section relating to making available public datasets to AI researchers and innovators. The action plan does however acknowledge the need to protect the security of AI infrastructure.

Whilst we welcome that government's recognition that it "*must protect UK citizens from the most significant risks presented by AI and foster public trust in the technology, particularly considering the interests of marginalised groups*", we are concerned that:

- This is directly followed by a statement that limits the extent of this obligation to protect people that reads: "*That said, we must do this without blocking the path towards AI's transformative potential.*" This approach betrays a belief that there's a choice to be made between protecting people and embracing innovation.
- We are concerned by the reference to "UK citizens" limits who will be protected, when under international human rights law and domestic laws, including the Human Rights Act, the UK has an obligation to protect everyone within their territory and jurisdiction.
- Data from people across the world may be exploited to develop and deploy AI. This can be in the form of a company or government agency seeking to build datasets to train AI that include data exfiltrated from platforms, data brokers, or more exploitative routes such as hacked datasets and data from conflicts.

Possible changes to legal and regulatory framework

4. What would be needed in any future UK legislation to protect human rights?

It is necessary to consider the wider range of laws relevant to AI.

As a general point, any future legislation should include meaningful recognition that the use of AI impacts human rights, and it should refer to the UK's existing human rights obligations under national and international law. Furthermore, recognising that the use of AI is underpinned by the processing of personal data, it is essential that any future legislation uphold and strengthen the enforcement of data protection frameworks.

In terms of the scope of the future legislation, it must ensure that:

- All actors, both private bodies and public actors, are accountable and can be held to account for their use of these types of technologies, and any exemptions must be narrowly construed so as not to provide loopholes, and to ensure clarity on when and how the rules dictated may not be applied.
- Everyone, not just *citizens*, within the UK's territory and jurisdiction, regardless of distinctions like nationality, race, sex, religion, or social origin, must be protected by the law; while the Government should also seek to protect data of all people from unlawful and unethical use.

Furthermore, there are certain specific safeguards that are key to protecting human rights when designing and deploying AI technologies, including:

- **Ensuring protection for human rights by design**

Decisions made in the design stage of AI application have a significant impact on whether the technology is human rights compliant. Relevant factors that would affect the design of an AI application include: deciding the governance of the data around the system (e.g. data the system learns, processes, alters, retains, shares); deciding which processes will be automated; setting the values the AI application is designed to optimise; deciding in which circumstances the AI application shall be used.

By design, AI applications must limit data collection, restrict further data processing, prevent unnecessary and unauthorised access, amongst others.

Furthermore, testing and evaluation of AI application should consider the specific contexts in which they are intended to be deployed; the data to be used in testing should mitigate risks of bias and discriminatory outcomes. These requirements and safeguards should be built in laws that regulate AI technologies in the relevant sectors.

- **Ensuring adequate data security of AI technologies**

The security of the data, stored (at rest) and in transit, as well as the infrastructure relied upon for processing, should be protected by security safeguards against risks such as unlawful or unauthorised access, use and disclosure, as well as loss, destruction, or damage of data. When assessing the level of security for AI applications, organizations should consider central processing and data storage sites, as well as the security of remote devices where data also may be collected or received. Security measures should include appropriate mechanisms for addressing actual and suspected security breaches.

- **Preventing discrimination and bias**

It is also essential to establish safeguards that prevent discrimination and algorithmic bias caused using AI in counter-terrorism efforts. This includes conducting regular human rights impact assessments, implementing fairness-aware machine learning practices, and ensuring transparency in data selection and model design. Particular attention must be paid to the risk of disproportionate impacts on marginalised or vulnerable communities, in line with the principles of equality and non-discrimination under international human rights law.

- **Adopting robust due diligences processes, including:**

  - **Human Rights Impact Assessment:** Human rights impact assessments of AI applications should be conducted at all stages of the tech lifecycle: prior to the design, during the development, the testing, the deployment and regularly thereafter in order to identify the emerging human rights risks. They should at minimum include privacy and data protection impact assessments and wider assessments on other human rights. They must be conducted within an existing context and the cumulative effects of interacting measures already in place around government surveillance and corporate exploitation, and not in isolation. The assessments should be conducted with the participation of affected individuals and groups, civil society actors and independent experts. The outcome of the assessment should be made public and should detail the mitigation and oversight measures envisaged.[40]

  - **Independent oversight:** Any deployment of AI technology should be subject to independent, effective, adequately resourced and impartial oversight. Oversight should cover all parts of the design, use and throughout the deployment of an AI application. Because of the human rights risk associated with the use of AI technologies for counter-terrorism, oversight should include judicial as well as parliamentary domestic oversight mechanisms capable of verifying the legality of the use of AI, ensuring transparency and accountability. Oversight mechanisms must have the power and capacity to conduct regular auditing of AI applications to ensure their compliance with human rights and other standards. Protection of intellectual property and trade secrets cannot justify refusal of such oversight, particularly when the AI application is used by the public sector.

  - **Transparency and explainability requirements**: The opacity of complex AI applications poses significant challenges to accountability and ultimately to access to effective remedies. However, not all sources of opacity are of a technical nature, and many can be addressed by adopting a human rights-centred approach. This is particularly the case when opacity is due to proprietary software and trade secrets; deliberate opacity by design; or lack of technical expertise that is required to properly understand advanced processing using AI.[41] Information shall include the category, purpose and sources of the data

[40] As noted by the Committee of Ministers of the Council of Europe "confidentiality considerations or trade secrets should not inhibit the implementation of effective human rights impact assessments."

[41] As noted in the Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems: "the legislative frameworks for intellectual property or trade secrets should not preclude such transparency, nor should States or private parties seek to exploit them for this purpose.

processed; the existence of profiling, of automated-decision making; and the logic involved and the significance and envisaged consequences of the processing.[42] Such an obligation should apply even where the task is burdensome.[43]

- **Safeguards against dependencies and over-reliance on the private sector**: Increasingly as Governments becoming reliant on Big Tech and other firms to provide public services,[44] it is essential that safeguards are put in place to require public bodies to consider any conflicts of interests, to prevent and minimise the risks of dependencies and over-reliance on the private sector, and to ensue that the involvement of the private sector does not replace domestic infrastructure and civil service expertise including by adopting principles of human rights and good governance for both governments and companies to

---

Transparency levels should be as high as possible and proportionate to the severity of adverse human rights impacts, including ethics labels or seals for algorithmic systems to enable users to navigate between systems. The use of algorithmic systems in decision-making processes that carry high risks to human rights should be subject to particularly high standards as regards the explainability of processes and outputs." See: Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies), CM/Rec(2020)1, https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

[42] This may be elaborated further to include for example "factors taken into account for the decision-making process, and their respective 'weight' on an aggregate level" and how a profile was built "including any statistics used in the analysis". See: Article 29 Data Protection Working Party, Guidelines on Automated Decision-Making and Profiling for the Purposes of Regulation 2016/679, 17/EN. WP 251rev.01, 6 February 2018, p 27, https://ec.europa.eu/newsroom/article29/items/612053/en

[43] The Article 29 Working Party Guidance on Transparency (adopted by the European Data Protection Board) has underlined that "[...] the mere fact that a database comprising the personal data of multiple data subjects has been compiled by a data controller using more than one source is not enough to lift this requirement if it is possible (although time consuming or burdensome) to identify the source from which the personal data of individual data subjects derived. Given the requirements of data protection by design and by default, transparency mechanisms should be built into processing systems from the ground up so that all sources of personal data received into an organisation can be tracked and traced back to their source at any point in the data processing life cycle." See: Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[44] If firms the government is contracting with were discovered to be abusing their power, e.g. anti-competitive conduct, exploiting data, unethical behaviours, these deep relationships and dependencies may create a challenging environment for addressing these harms. Decisions are being made about the use of various firms that will shape the medium-term future for all parties, replacing domestic infrastructure and civil service expertise. For instance, the UK Government's spy agencies use Amazon's AWS; see: Helen Warrell and Nic Fildes, Amazon strikes deal with UK spy agencies to host top-secret material, Financial Times, 25 October 2021, https://www.ft.com/content/74782def-1046-4ea5-b796-0802cfb90260; the NHS uses Palantir, see: Lindsey Clarck, Some English hospitals doubt Palantir's utility: We'd 'lose functionality rather than gain it', The Register, 16 May 2025, https://www.theregister.com/2025/05/16/nhs_hospitals_palantir/; the DSTI's announcement of a partnership with Google Cloud, see: Lindsey Clarck, Some English hospitals doubt Palantir's utility: We'd 'lose functionality rather than gain it', The Register, 16 May 2025, https://www.theregister.com/2025/05/16/nhs_hospitals_palantir/. Furthermore HMRC recently justified their continued use of Fujitsu, even after the Post Office Horizon IT system scandal, on the grounds that using a different contractor would be too challenging, see: Lindsay Clark, Fujitsu sorry for Post Office horror – but still cashing big UK govt checks, The Register, July 17 2025, https://www.theregister.com/2025/07/17/fujitsu_govt_contracts/

apply with: transparency, legality, necessity and proportionality, accountability, oversight, redress and proper procurement standards and procedures.[45]

To what extent should the same human rights standards apply to private actors as public bodies when they use AI?

All actors should be held to account and their use of AI regulated and overseen by a set of clear standards and obligations as well as accountability and mechanisms.

Any exemptions provided by law to comply with these standards and obligations must be narrowly construed, and to ensure clarity on when and how the rules dictated may not be applied. Too often governments enjoy blanket exemptions for national security, for example, and the private sector benefits from exemptions based on copyright or trade secrets.

Under international law, the UK government has the obligation to ensure that third parties, including private actors, protect human rights. This means that it must ensure that the private sector is held accountable and comply with human rights obligations, and that oversight mechanisms are in place to hold them to account.

As public bodies and private actors are working increasingly together hand in hand, there are overlapping, ill-defined and opaque roles and responsibilities. There is a need to effectively regulate and oversee public-private partnerships (PPPs)[46] to address the increasingly co-dependency between the parties, whereby the state may be developing new systems or processes entirely reliant on the services of one company, and the company may be receiving access to data or other information for use in developing its own services.

Widely recognised principles of human rights and good governance applicable to both governments and companies (notably via the UN Guiding Principles on Business and Human Rights) should apply, such as transparency, legality, necessity and proportionality, accountability, oversight, redress and proper procurement standards and procedures.

To what extent might different kinds of AI technology require different regulatory approaches?

As we noted elsewhere, because of the diversity of what AI can encompass and the uses they may have, different applications of AI will require careful consideration of the context of application, and who may be adversely impacted.

This does not mean that different regulatory approaches for every kind of AI technology are required as national and international human rights obligations should always apply regardless

[45] See: UN Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights and PI, PI, Public-Private Partnerships, https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships

[46] See: PI, Public-Private Partnerships, https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships

of the kind of AI technology or application, and similarly if personal data is processed then data protection law will apply.

However as noted above, there may be limits to how much the latter constitutes sufficient safeguards as some kind of AI technologies may rely on non-personal data to make or inform decisions that still negatively impact the human rights of individuals and groups affected, and that would need to be acknowledged and may require the adoption of specific safeguards for those AI technologies.

Finally, it is important to recognise that some kinds of AI technology or AI applications may never be deployed in a manner which protects human rights as we have argued in the case of generative AI models developed to date[47] and live/real-time facial recognition (FRT).[48]

5. Who should be held accountable for breaches of human rights resulting from uses of AI, and on what basis?

Any actor, whether private or public, who designs, develops, deploys and uses AI must be held accountable for breaches of human rights resulting from uses of AI.

They must be subject to clear standards and obligations, and oversight and accountability mechanisms as provide for in legally binding instruments.

Where in the process of developing, deploying and using AI technologies should liability arise?

Due to the challenges that AI technologies pose, there needs to be enhanced privacy safeguards throughout the AI lifecycle.

At every stage, there is an element of liability that must be considered:

- **Prior and during development:** When developing a new AI technology and application, there is a liability for those implicated in the design and development. Some of the issues they must consider include: the necessity and the impact they will have on people and the rights, and that assessment should inform their design as well as the measures that need to be taken to mitigate any risks identified including adopting security by design and by default and involve those who will be affected into the process.

- **Prior to deployment:** Prior to deciding to deploy, those deciding to use a particular AI technology or application must undertake a human rights assessment to identify the risks and impact to decide whether a system should be deployed for this particular purpose, namely is it necessary and proportionate in the first place, and then if its

[47] See: PI response to ICO consultation on data subject rights and generative AI, 2 July 2024, https://privacyinternational.org/advocacy/5338/pi-response-ico-consultation-data-subject-rights-and-generative-ai
[48] See: PI submission to the Scottish Parliament's Justice Sub-Committee on Policing inquiry into facial recognition policing, 11 November 2019, https://privacyinternational.org/advocacy/3274/submission-scottish-parliaments-justice-sub-committee-policing-inquiry-facial

deployment is justified its design and application must consider any risks identified and corresponding mitigation measures.

- **During and after deployment:** Throughout deployment, there must be regular audits and evaluations as to how AI is used, is it working as intended, are new risks emerging, can they mitigated, and the design and deployment must be amended accordingly, or it must be stopped. These audits and evaluations must be done regularly, including at the end once a project or programme has ended, they must be inclusive and open, and they must be then made public and accessible.

We would like to remind the Committee that the government has already deployed systems and developed deep relationships with industry that verge of dependencies. We question whether it would be possible to stop using these technologies. For instance, the UK Government's spy agencies use Amazon's AWS (who provides AI tools), and the NHS uses Palantir (a data analytics firm).[49] If it is discovered that these firms are problematic or the tools cross a line, can the government actually cease using these firms' services? Not only will the civil service have lost expertise, but it is also possible that the dependence will be too great. We remind the Committee that HMRC in May 2025 justified its continued use of Fujitsu, the provider of the Post Office Horizon IT system, on the grounds that "*A change to a different contractor cannot be made for these services because the HMRC applications concerned are hosted and/or operated by [Fujitsu on its] infrastructure in [its] datacenters with connectivity provided by Fujitsu. It would not be possible for another contractor to take over or provide these services using [Fujitsu's] infrastructure and hosting before they are migrated to HMRC's new replacement infrastructure.*"[50]

What additional measures, if any, are needed to ensure that individuals have sufficient redress where they have suffered harm because of the use of AI?

Individuals should have access to an effective remedy against applications of AI technologies that affect them. As access to a remedy is dependent on the ability to know if and how one has been affected by AI applications, transparency and explainability noted above are necessary preconditions to exercise the right to seek remedy.

Individuals should have access to accessible, affordable, independent and effective judicial and non-judicial authorities with the power to receive complaints from individuals, investigate them, and take enforcement action - or refer the case to a court.[51]

---

[49] See: Helen Warrell and Nic Fildes, Amazon strikes deal with UK spy agencies to host top-secret material, Financial Times, 25 October 2021, https://www.ft.com/content/74782def-1046-4ea5-b796-0802cfb90260; the NHS uses Palantir, see: Lindsey Clarck, Some English hospitals doubt Palantir's utility: We'd 'lose functionality rather than gain it', The Register, 16 May 2025, https://www.theregister.com/2025/05/16/nhs_hospitals_palantir/

[50] See: Lindsay Clark, Fujitsu sorry for Post Office horror – but still cashing big UK govt checks, The Register, July 17 2025, https://www.theregister.com/2025/07/17/fujitsu_govt_contracts/

[51] As noted by the UN Special Rapporteur on freedom of expression, there are concerns whether AI applications, such as automatic response processes, to respond to complaints constitute an effective remedy, "given the lack of discretion, contextual analysis and independent determination built into such processes." See: UN doc. A/73/348, para 41, https://docs.un.org/en/A/73/348

Mechanisms of collective redress are an important and effective tool for accountability of AI applications. As noted above, challenges in transparency and explainability and the fact that AI systems often affect groups and communities, as well as the society more broadly, make collective complaints an appropriate procedure to complement individual redress.

6. How might regulation match the pace of AI technology development, such as the emergence of agentic AI, to ensure that human rights are preserved as technology continues to develop?

We have worked at the forefront of technology and law for over thirty years. We have explored AI Assistants[52] and emerging agents.[53] Despite enthusiasm, the security and privacy challenges are quite clear. We can wait for them to arise in the wild and panic to respond, or we can inform development now.

There's a popular myth that technology policy is hard because the law moves slowly and technology moves quickly. When it comes to technology regulation, inaction and delay are deliberate choices. There are many lawyers in the firms building these tools and government agencies processing vast amounts of data.

The law is almost always clear as it is mostly technology-neutral. When it is not, it is possible for regulators to rectify this quite quickly, as we saw with the ICO[54] and the European Data Protection Board [55] respond to LLMs in 2024, or the UN General Assembly exploring autonomous weapon systems.[56]

Governments are also quick to act to regulate technology when it serves their interests, such as when the Home Office issued a secret Technical Capabilities Notice to Apple to undermine the security of their technology.[57]

The creation of a new technology does not change the law. The UK already has existing national and international obligations to protect, respect and promote human rights which must be complied with as new technologies continue to be developed. They provide the foundation for the UK government to consider if and how to use certain technologies.

Furthermore, many rights people have result in concrete obligations that must be met and therefore the argument that something is technically hard or novel provides no defence against non-compliance. This may be especially important where the new technology is widespread and the subject of considerable societal and economic upheaval. We are concerned that so far

---

[52] PI, Your future AI Assistant still needs to earn your trust, 10 April 2025, https://privacyinternational.org/long-read/5555/your-future-ai-assistant-still-needs-earn-your-trust

[53] PI, Do early steps into agentic AI respect our needs for privacy and security?, 18 July 2025, https://privacyinternational.org/news-analysis/5623/do-early-steps-agentic-ai-respect-our-needs-privacy-and-security

[54] PI, Response to ICO consultation on data subject rights and generative AI, 2 July 2024, https://privacyinternational.org/advocacy/5338/pi-response-ico-consultation-data-subject-rights-and-generative-ai

[55] PI, Submission to EDPB on AI models, 13 July 2024, https://privacyinternational.org/advocacy/5495/pi-submission-edpb-ai-models

[56] PI, Statement during informal consultations on autonomous weapons systems in New York, 22 May 2025, https://privacyinternational.org/legal-action/pi-apple-tcn-challenge

[57] Joseph Menn, U.K. orders Apple to let it spy on users' encrypted accounts, The Washington Post, 7 February 2025, https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/

the situation with AI and HM Government is that it has chosen to avoid creating clear rules when it has prioritised deployment of technology (e.g. FRT continues to lack a lawful basis), turned the regulation discourse away from 'AI safety'[58] to 'security'[59], engages with industry continually about developing new technology for government use,[60] undermines regulators in favour of growth,[61] while only releasing simplistic and non-legally binding statements about the necessary rights protections.

We believe that Parliament, and JCHR in particular, can play a crucial role in plugging a gap that continuously arises in UK technology policy, rather than wait until the next crisis.

[58] Department for Science, Innovation & Technology, Announcement of the 'AI Safety Institute', November 2023, https://www.gov.uk/government/publications/ai-safety-institute-overview/introducing-the-ai-safety-institute

[59] See: AI Security Institute, https://www.aisi.gov.uk/

[60] Ministry of Justice, The Rt Hon Shabana Mahmood MP and Lord Timpson OBE, Tech companies urged to join drive to cut crime, May 8 2025, https://www.gov.uk/government/news/tech-companies-urged-to-join-drive-to-cut-crime

[61] Suzi Ring and Jim Packard, How the UK's competition regulator lost the trust of ministers, Financial Times, February 16 2025, https://www.ft.com/content/0cc18c6e-bab5-43de-ae10-d72bbe129294