**Response of the Government of the United Kingdom of Great Britain and Northern Ireland to the call for inputs from the Office of the United Nations High Commissioner for Human Rights on Artificial Intelligence and the Right to Privacy**

**Introduction**

The United Kingdom (UK) is fully and actively committed to upholding the right to privacy as set out in Article 17 of the International Convention on Civil and Political Rights, and that the same rights that people have offline must be protected online. We believe that artificial intelligence (AI) can and should be a force for good. At the same time, we recognise the challenges posed by the use of AI for the effective exercise of the right to privacy and other human rights. We welcome the work of the UN Special Rapporteur on the Right to Privacy in looking at these and other related issues.

The UK seeks to work alongside likeminded countries to ensure the ethical, human-centred, and responsible development and deployment of AI, and on creating an enabling environment for AI policy. This environment should also encourage diversity in the development of these technologies.

The UK has a proud history of innovation and championing a free and open internet. We believe that an agile approach to regulation will provide a framework that encourages innovators, provides confidence to investors, and builds public trust. We are keen to work with businesses across a range of industries and subsectors to consider how and where regulation can keep pace with new technologies and support innovation. We are determined that the UK should lead the world in innovation-friendly regulation that encourages the tech sector and provides stability for businesses.

1. **The specific impacts on the enjoyment of the right to privacy caused by the use of artificial intelligence, including profiling, automated decision-making and machine-learning technologies (hereinafter referred to in short as “AI”) by governments, business enterprises, international organizations and others. Of particular interest is information concerning:**
	1. **relevant technological developments, the driving economic, political and social factors promoting the use of AI and the main actors in and beneficiaries of deploying and operating AI (developers, marketers, users);**

Harnessed properly, with the right drivers to deliver responsible adoption across sectors, AI has the potential to yield huge economic benefits by accelerating productivity, improving efficiency and delivering reliable insights in many fields. There are enormous opportunities for the UK to capitalise on AI to improve lives through better public services and consumer choice.

In 2021, the UK will launch a new National AI Strategy[[1]](#footnote-1). This Strategy will focus on Growth of the economy through widespread use of AI technologies; ethical, safe and trustworthy development of responsible AI; and resilience in the face of change through an emphasis on skills, talent and research, and development.

* 1. **ways, in which AI can help promote and protect the right to privacy;**

If AI and complementary digital and data technologies are developed in the right way, they have the potential to enable major advances in tackling global challenges, and reinforce the enjoyment of human rights. The full range of stakeholders – governments, industry, civil society and academia – should engage in continuous dialogue about the principles and ethics according to which new technologies are developed, deployed and regulated, and governments should regularly consult these stakeholders.

Developing and deploying responsible AI is dependent upon access to high quality datasets that reflect society’s diversity and the right of individuals in a fair manner. The UK’s vision is to work bilaterally with like-minded countries to enhance and protect global data flows and ensure data sharing is safe, secure, fair, legal and ethical. We want to promote genuine global cooperation in the development of AI. Governments have a responsibility to ensure that the development and deployment of digital technologies within their borders is consistent with their human rights obligations and wider international law.

* 1. **challenges posed by the use of AI for the effective exercise of the right to privacy and other human rights, including features and capabilities of AI that present existing or emerging problems;**

Whilst AI technologies have driven dramatic improvements to our economy and society, we must ensure the responsible, ethical and human-centric development and deployment of technologies, in a manner that respects individuals’ human rights. For example, technologies such as AI and the Internet of Things collect vast amounts of personal data, such as an individual's location. There is a need to ensure that this data is not used inappropriately or is not used in a way that breaches people's right to privacy. We must take an inclusive and ethical approach to AI; protecting / respecting rights, protecting data privacy, and avoiding harms resulting from automated decision-making.

While governments have legitimate security reasons for accessing personal data in certain circumstances, governments must make sure that the access is proportionate and that there are mechanisms in place to ensure that human rights are not violated

* 1. **discriminatory impacts of the use of AI;**

We know that individuals pioneering this technology are shaped by their own personal experiences and backgrounds. Acknowledging this is only the first step – we must go further and draw on a diverse mix of minds to develop, apply and govern our use of AI. Left unmanaged, our use of AI risks incorporating and reflecting the beliefs and assumptions of its creators – AI systems are no better or no worse than the human beings that create them. This is why governments and industry need to consider and take concrete steps to ensure the datasets used to train algorithms are not unfairly discriminatory or risk reinforcing existing structural inequalities, for example, by adopting or even enhancing unfair bias created by historic racism.

1. **legislative and regulatory frameworks, including:**
	1. **information on relevant existing or proposed national and regional legislative and regulatory frameworks and oversight mechanisms;**

The UK Data Protection Act is a complete data protection system, governing the processing of personal data covered by the EU’s General Data Protection Regulation (GDPR), as well as all other processing of personal data for UK law enforcement and national security.

The UK is developing a comprehensive governance system to manage AI and data ethics, drawing on best practice and consultation with a wide range of external stakeholders. This governance system will set out the standards developers will be expected to meet and practical guidance to help them achieve these The UK believes in innovation-friendly regulation and that there is not a one-size-fits-all approach to regulation. Governance should be risk-based in nature, and suitably flexible to capture differences across sectors, especially where risks can vary by context rather than by technology. The UK believes that empowering sectoral regulators to review how AI technologies affect their sector is the right approach, allowing for more flexibility, an evidence-based approach, and the creation of innovation-friendly regulator practices.

The UK has established several public bodies to support this work. The Office for AI[[2]](#footnote-2) is a joint Department for Business, Energy and Industrial Strategy (BEIS)-Department for Digital, Culture, Media and Sport (DCMS) unit aimed at driving responsible and innovative uptake of AI technologies for the benefit of everyone in the UK.

The UK Centre for Data Ethics and Innovation (CDEI)[[3]](#footnote-3) is dedicated to considering the implications of digital technologies for democracies. It provides independent advice to both government and regulators on the measures needed to enable and ensure safe, ethical and innovative uses of AI and data-driven technologies. The UK’s AI Council[[4]](#footnote-4) is an expert committee of independent members from industry, public sector and academia, providing high-level expertise and priorities.

In February 2021, the UK published a pioneering ethical framework to guide the responsible use of AI by Government Communications Headquarters (GCHQ) across its missions – from tackling serious and organised crime, to disrupting state-based disinformation campaigns.[[5]](#footnote-5)

The UK fully revised and updated our investigatory powers framework in the [Investigatory Powers Act (IPA) 2016](https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted), which includes important new privacy safeguards, in particular the double lock whereby use of the most intrusive capabilities are subject to ex ante judicial authorisation. The UN Special Rapporteur on the Right to Privacy praised the UK’s policy on surveillance.[[6]](#footnote-6) While the Act does not legislate for AI per se, UK Intelligence Community (UKIC) use of bulk data sets is subject to regulation under Part 7.

In addition, UKIC is subject to regulation of its data processing more generally by a special dedicated regime under Part 4 of the [Data Protection Act (DPA) 2018](https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/#:~:text=Part%204%20of%20the%20DPA,schedules%209%2D11.), which is based on the modernised [Council of Europe Convention](https://www.coe.int/en/web/data-protection/convention108-and-protocol). The DPA also contains the general prohibition on automated decision making (i.e. with no meaningful human input) that has significant effects on individuals, regulates UK intelligence service processing of special category data including biometric data and imposes an obligation that UKIC processing integrate privacy by design. UKIC processing of data is also subject to robust oversight arrangements, through the Investigatory Powers Commissioner’s Office (IPCO), and is regulated by the Information Commissioner’s Office in important areas, including compliance with data subject rights of access to information regarding the processing of their data. Data subjects also have full access to the Investigatory Powers Tribunal, which has a wide remit to investigate complaints against the UK intelligence services concerning surveillance.

* 1. **analysis of related human rights protection gaps, ways to bridge those gaps and barriers to advancing effective, human-rights based regulation of AI;**

To ensure the impact on privacy is properly considered in every circumstance, the UK Government Communications Headquarters undertakes an assessment to determine the necessity and proportionality of any intrusion into privacy. This is undertaken both when considering the use of operational data to train and test AI software, and when applying the software to the analysis of operational datasets. These assessments are made available for audit by the [Investigatory Powers Commissioner’s Office (IPCO)](https://www.ipco.org.uk/publications/).

1. **other safeguards and measures to prevent violations of privacy when using AI, and address and remedy them, where they occur, including:**
	1. **self-governance approaches by business enterprises to regulate AI applications, which meet the companies' responsibilities to respect the right to privacy;**

The UK believes that major changes affecting public safety or other standards, including in respect of AI, should not be made unilaterally by tech firms, but in partnership with governments. Tech companies who deliver services that are not designed with public safety in mind enable and exacerbate other harms, online and offline. It is our strong view that the tech industry should work with governments to embed the safety of the public in their system designs.

The UK supports the call to businesses to meet their responsibility to respect human rights in accordance with the UN Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, including the right to privacy in the digital age. Businesses have to ensure user safety and protection when enabling technical solutions to secure and protect the confidentiality of digital communications, including in the context of child sexual exploitation and abuse, and wider public security. We also believe that such solutions should not preclude legal access to content where an authorisation is lawfully issued and is subject to strong safeguards and independent oversight.

* 1. **human rights due diligence in the context of the use of AI by governments, business enterprises and international organisations;**

As AI technologies like facial recognition technology continue to develop in sophistication, we need to ensure that governments do not use these technologies as a tool to curb human rights, including freedom of expression, the right to liberty of movement, and the right to privacy.

* 1. **data governance models, such as data trusts, that provide effective protection to the right to privacy in data-intensive environments;**

The UK is developing data governance models, such as data trusts, that provide effective protection to the right to privacy in data-intensive environments. For example,novel forms of data governance such as data cooperatives, data collectives and data trusts could enable sharing of sensitive data, whilst allowing valuable computation and analysis of that data to solve very difficult public policy problems. The [OpenSAFELY](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fopensafely.org%2F&data=04%7C01%7Cn-oldham%40dfid.gov.uk%7C70ca671f3ce74ab2d6dc08d916f4f7d9%7Ccdf709af1a184c74bd936d14a64d73b3%7C0%7C0%7C637566063659652967%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=Rl5tkRoVX9ijBIJiErVXOAySastlKaayrIuPxOFdUF0%3D&reserved=0) secure analytics platform developed as a data collaborative in response to the COVID-19 pandemic enabled independent researchers to run large scale analysis without transferring the highly sensitive patient data out of the secure data centre in which it resided. This allowed researchers to quickly and accurately identify risk factors associated with the disease

Following a series of workshops on the ways in which data intermediaries can enable new forms of safe and efficient data sharing, we are considering the role of data intermediaries in supporting responsible data sharing, and how government can intervene to support their adoption. This approach builds on the Ada Lovelace Institute and AI Council [joint report on Legal Mechanisms for Data Stewardship](https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship/). As part of this, we will support the Open Data Institute’s work on data institutions – organisations whose purpose involves stewarding data on behalf of others – to create an environment that supports existing data institutions in the public, private and third sectors and is conducive to innovation around new forms of data intermediaries such as data trusts and data cooperatives.

* 1. **Technological applications that could help adequately protect the right to privacy when applying AI and their limits.**

One innovation to protect privacy is through Privacy-Enhancing Technologies (PETs). The technological applications could help protect the right to privacy when applying AI and their limits. Emerging privacy enhancing technologies such as homomorphic encryption, secure multi-party computation, differential privacy, and federated analytics are increasingly being applied to protect the privacy of individuals when training or using AI systems. Example applications have been collated in CDEI’s [PETs use case repository](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fcdeiuk.github.io%2Fpets&data=04%7C01%7Cn-oldham%40dfid.gov.uk%7C70ca671f3ce74ab2d6dc08d916f4f7d9%7Ccdf709af1a184c74bd936d14a64d73b3%7C0%7C0%7C637566063659652967%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=iAFDX6xfIy81mY4h4z0SCXYMkcV4fYehETt0BHWRCyk%3D&reserved=0).

PETs are not a complete solution to privacy problems, but a technical option that can drastically reduce privacy harms when applied appropriately and in the right contexts. One of the key limitations in the use of PETs is around [accountability and transparency](https://eur02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.adalovelaceinstitute.org%2Fblog%2Fprivacy-enhancing-technologies-not-always-our-friends%2F&data=04%7C01%7Cn-oldham%40dfid.gov.uk%7C70ca671f3ce74ab2d6dc08d916f4f7d9%7Ccdf709af1a184c74bd936d14a64d73b3%7C0%7C0%7C637566063659662922%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=G48NteX%2B2GTbcv%2FgaOMxRgJ9oEmKtYHrCeqpr8ER49c%3D&reserved=0). Whilst preserving the privacy of data subjects, they risk obscuring the processing or analytical activity being carried out on personal data.

1. https://www.gov.uk/government/news/new-strategy-to-unleash-the-transformational-power-of-artificial-intelligence#:~:text=The%20National%20AI%20Strategy%20will,cent%20of%20GDP%20by%202027. [↑](#footnote-ref-1)
2. https://www.gov.uk/government/organisations/office-for-artificial-intelligence [↑](#footnote-ref-2)
3. https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation [↑](#footnote-ref-3)
4. https://www.gov.uk/government/groups/ai-council [↑](#footnote-ref-4)
5. <https://www.gchq.gov.uk/artificial-intelligence/index.html> [↑](#footnote-ref-5)
6. <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E> [↑](#footnote-ref-6)