Follow up Written Evidence Submitted by the Information Commissioner's Office (ICO) (DDA0070)

Thank you for inviting me to appear in front of your committee on 08 June; and for the opportunity to outline in more detail the range of work my office is doing in this area.

I wanted to directly answer your question around how the ICO's powers apply to AI and the wider question around how we are regulating this space.

This is a challenging and complex area of regulation, but the ICO has a wide range of powers and regulatory tools and I believe these can be effectively applied to AI systems. I see enforcement action as a back stop and not a first step. With robust information governance and the opportunity for organisations to safely test modern technologies and ideas, I believe we can have an information rights space where privacy is protected, and the potential of AI and machine learning can bring great benefits to our economy and society.

Definition of AI

For clarity, I thought it would be helpful if I set out how we define AI in the context of our regulatory work. In our guide to the UK GDPR[1], we explain AI as an *umbrella term for a range of algorithm-based technologies that solve complex tasks by carrying out functions that previously required human thinking.* This can include solely automated decisions or those with some human involvement.

There are rules regarding the use of personal data for decisions which are solely automated and either produce a legal effect or affects an individual in a similarly significant way (set out in Article 22 of the UK GDPR). Individuals have the right to object to an automated decision unless (a) it is required or authorised by law, (b) is needed to enter into a contract or to carry out core contractual obligations, or (c) they have given their explicit consent. In addition to other safeguards, for the latter two, the individual must be able to give their view and ask for a human review of that decision.

The legal position – regulation of AI

The question was raised during the session as to whether my powers extended only to the collection and sharing of data in the context of an AI system. The short answer to this question is no. Our powers and indeed the scope of data protection law apply to more than just collection and/or sharing.

Data protection law applies to almost anything an organisation does with personal data, including collecting, recording, storing, using, analysing, combining, disclosing or deleting it. These activities fall within the scope of 'processing' as defined by Article 4(2) of the UK GDPR, which explicitly includes automatic processing, and is technology blind. The UK GDPR also contains several further explicit references to profiling and automated decision making and large-scale automated processing.

This means that UK GDPR applies to the use of personal data when building and

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-artificial-intelligence/

testing the AI system and when AI is used to make a decision, provide a prediction or recommendation about someone. The most relevant UK GDPR data protection principles to reference here are 'Lawful, Fair and Transparent,' 'Accuracy' and 'Accountability'.

Lawful, Fair and Transparent

To be compliant with this principle, the processing of personal data must come within one of 6 'lawful bases' for using data, must be fair to those individuals, who have (within reason) been told about the use. In practice, it means that if an AI system is used to infer data or make decisions about people, the system must be sufficiently statistically accurate and avoid discrimination.

Where there is more than a minimal risk that an AI system will produce an unfair outcome for an individual, there must be a reasonable right of review and/or that risk must have been clearly explained to the individual at the outset. The exception to this is where other circumstances make the outcome both fair and proportionate in any event.

Informing people about how their information will be used in an AI system is clearly central to the transparency requirements but is also a key factor for both fairness and lawfulness. It helps to ensure the use of personal data in the AI system is within their reasonable expectations. For example, you will need to explain to people the scope of your AI system, how it is used and that it provides a statistically informed guess and not a factual decision.

Accuracy

There are two key aspects to accuracy in AI. First, the accuracy of personal data used to train and test the AI system. Second, how often an AI system selects the correct answer about an individual, measured against correctly labelled test data. Accuracy in AI refers to how often an AI system selects the correct answer, measured against correctly labelled test data. To be accurate does not require a system to achieve 100% accuracy, but AI systems should be utilised to consider that its outputs are treated as at best a statistically informed guess. This links to

the previous principle: unless the AI system is used and explained to people in this way, it is unlikely to comply with the principle of lawfulness, fairness and transparency.

Accountability

The accountability principle is crucial in the context of the wider question of how we regulate AI. It encourages organisations to make considered and evidence-based decisions and places on them an expectation that they must be able to demonstrate compliance with UK GDPR. For AI, this means taking several steps before the deployment of the system. This will usually include conducting a Data Protection Impact Assessment ('DPIA') and potentially consulting with my office. All organisations using AI systems needs to be able to demonstrate its UK GDPR compliance proactively and when asked by my office.

The work of the ICO

In addition to the legal framework which governs use of personal data are the practical steps the ICO takes to regulate AI. The ICO has produced world-renowned guidance[2] on AI and data protection in partnership with the Alan Turing Institute. This guidance, which we will be updating as AI evolves, provided the foundations for our recently published AI and Data Protection Risk Toolkit[3]. The toolkit was developed after extensive consultation with data scientists, industry, venture capital firms and academics and is a practical tool to assist practitioners managing AI systems. Alongside these resources, we have also actively engaged stakeholders in this area.

The ICO's Regulatory Sandbox is a service developed to support organisations looking at innovative forms of processing, including AI. By way of example, we worked with Onfido[4] when exploring the training for its facial recognition technology ('FRT') based identity verification services. Onfido's research in this

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection

[3] https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit

[4] https://ico.org.uk/media/for-organisations/documents/2618551/onfido-sandbox-report.pdf

area was designed to mitigate any bias of the technologies it used. This engagement has helped develop ICO knowledge of complex AI supply chains and clarified how different organisations involved in this process operate. This clarity should provide a direct privacy benefit for individuals in the form of transparency and control[5].

The ICO actively cooperates with other regulators to tackle innovative technologies and issues as they emerge. We work with three other regulators (Ofcom, the Competition and Markets Authority, and the Financial Conduct Authority) at the Digital Regulation Cooperation Forum to ensure we can take a coordinated approach to AI policy, providing clarity for businesses and innovators. Our Forum recently published two discussion papers on the landscape for AI auditing and algorithmic harms and benefits[6]. The ICO holds the secretariat of the Regulators and AI Working Group that includes various members for UK regulatory landscape; and the ICO also participates in the AI Working Group of the Global Privacy Assembly, engaging in work in relation to AI risk management and AI in employment.

Enforcement

Working with organisations to promote compliance is my priority. However, where enforcement is required, I have a range of powers as set out in the ICO's Regulatory Action Policy[7] ('RAP'). Where an organisation is failing to process personal data in accordance with the data protection principles, including those set out in this response, and the criteria within our RAP is met then we can act. This includes the power to issue fines up to 4% of global turnover and to issue orders which require an organisation to cease unlawful processing of data.

---

[5] https://ico.org.uk/media/for-organisations/documents/2618551/onfido-sandbox-report.pdf

[6] https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022

[7] https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf

Gaining Public Trust

The final area to address is how to increase and retain public trust for data use in research. We all recognise the lessons that need to be learned following the initial launch of GDPR, and the committee has heard from a few witnesses on this point. Professor Ben Goldacre mentioned citizen juries and other witnesses have correctly emphasised the importance of civil society engagement. However, my main message is that there is a need to utilise multiple channels of engagement and that getting that engagement right is essential to the success of data sharing initiatives.

The ICO commissions an annual track survey[8] which focuses on several aspects of data use, and we are using this information along with other feedback to ensure our products and guidance reflect the needs of the public, including a successful experience working to improve our products in the AI space.

Artificial intelligence and algorithms rely on data sharing to function, but they are only a part of the wider data ecosystem. The question of building and maintaining public trust in data sharing is a crucial task in which the ICO has a vital role, however, it is bigger than just the ICO. It needs commitment and investment from government, civil society and the organisations that share people's data.

I am happy to provide any further information you need. I look forward to the report of your committee on this inquiry.

John Edwards
UK Information Commissioner

(21st June 2022)

[8] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/07/ico-publishes-annual-tracking-research/