More Speed, Less Haste: Finding an Approach to AI Regulation that Works for the UK

Simon McDougall
Future of Privacy Forum

Abstract

Artificial intelligence (AI) regulation is in vogue, with proposals around the world to regulate AI as an activity separate to other types of data processing. This article argues that this approach is problematic, given the difficulties in defining AI. It notes that the more *laissez-faire* approach of the United Kingdom (UK) risks subsequent hasty legislation being introduced when innovative applications of AI cause moral panic.

The article proposes a way forward, utilizing the UK's existing data protection framework to accelerate the shift to meaningful regulation. This approach leverages the substantial overlap between data protection regulation and the risks of AI and enables greater regulatory certainty and effectiveness by expanding the scope and powers of an existing regulator—the Information Commissioner's Office—rather than creating something from scratch. Doing so mitigates the challenges of defining AI by focusing instead on the risks presented to individuals, organizations and society by all automated decision-making.

Finally, the article notes that the speed of change in this area will require ongoing agility from all the bodies involved in digital regulation in the UK and outlines the potential for the Digital Regulation Cooperation Forum to support its member regulators.

Keywords: artificial intelligence; data protection; innovation; technology.

[A] AI: SOMETHING MUST BE DONE?

Every now and then, society encounters an issue about which "something must be done". Often this notion includes a dose of moral panic, and a sense that the current order is not equipped to address the new perceived threat. In my world of privacy and data protection, Warren and Brandeis developed the notion of the "right to be left alone" as a response to concerns in the United States (US) around the consumerization

of photography (Samuel & Brandeis 1890). More recently in the United Kingdom (UK), we can recall furore around "video nasties" (British Board of Film Classification nd; Video Recordings Act 1984), dangerous dogs (Bennett 2016; Dangerous Dogs Act 1991) and genetically modified foods (Burke 2004; Harvey 2023), all examples of when media and societal concerns have driven a hasty legal and regulatory response.

AI inspires similar emotions, but this time (with all due respect to dog lovers) the stakes are higher. AI already has an impact across our daily economic and social lives; it is proving to be disruptive and destructive, as well as fun, transformative and productive. Use of AI has been normalized in everyday technologies such as image recognition and natural language processing, while applications of technologies such as generative AI are capturing the imagination and the fears of the public.

It is appropriate that policymakers and legislators around the world are thinking about new law and regulation to address AI, but it will take cool heads and clear minds to get this right.

[B] THE UK HAS FALLEN OFF THE PACE IN POLICY AND REGULATION

The discussion is lent some urgency by the sense that the UK has lost ground. For a while, the UK led the AI policy discussion, with groundbreaking research by the Royal Society and the British Academy, Dame Wendy Hall's formative paper on growing AI in the UK (Hall & Pesenti 2017) and the subsequent foundation of the AI Council, the Office for AI, the Centre for Data Ethics and Innovation and the Ada Lovelace Institute. Granted, there were many cooks in the kitchen during this period, but there was also a level of energy and cross-disciplinary engagement which was lacking elsewhere in the world.

The political crises around Britain's exit from the European Union (EU) meant that from 2019 onwards momentum was lost. Government thinking in the July 2022 paper on AI (Gov.uk 2022) and March 2023 International Technology Strategy (Gov.uk 2023b) used a lot of words to say that, essentially, not much new was going to happen.

Meanwhile, the rest of the world pushed on apace. The AI Principles of the Organization for Economic Cooperation and Development (OECD) (adopted in 2019) established broad intergovernmental agreement, followed by the United Nations Educational, Scientific and Cultural Organization (UNESCO) Standard on the Ethics of Artificial Intelligence (UNESCO 2022). The EU's draft AI Act 2023 led the way for AI-specific

legislation (for better or worse), and China introduced AI regulation for some use cases (Holistic AI 2023), including a framework for generative AI scheduled (at the time of writing) to go live in August 2023 (Ye 2023). In the US, the White House's Blueprint for an AI Bill of Rights (White House nd) set the policy tone and has been followed up with a Request for Information regarding federal rulemaking (Federal Register 2023) and a voluntary framework agreed with the largest US AI companies releasing foundation models to the general public (White House 2023). Congress has made a range of legislative proposals (Lenhart 2023) and the National Institute of Standards and Technology (NIST) AI Risk Management Framework (NIST 2023 (AI RMF 1.0)) has set a new standard for risk management and self-regulation.

In recent months, there has been a welcome re-engagement in the UK, perhaps reflecting the new Prime Minister's interest in the area. The AI Regulation White Paper (Gov.uk 2023b) is an excellent analysis of the current challenges. However, the White Paper shies away from legislative intervention, relying instead on an iterative approach by existing regulators, a vaguely defined "central risk function" to "identify, assess, prioritise and monitor cross-cutting AI risks" and a general intention to monitor the situation for now (Gov.uk 2023a).

[C] PASSIVITY EXPOSES THE UK TO MORAL PANIC

I am concerned that the current approach leaves the door open for knee-jerk legislation—whenever something awful happens that the media links to AI, a moral panic ensues.

We have a recent precursor, which happened during my time as a Deputy Commissioner at the ICO. In August 2020, we saw the first algorithmic (albeit not AI) backlash, as the public responded to the Government's approach to awarding exam grades during the Covid pandemic (Hao 2020). The until-then abstract policy debate felt much more real when crowds in Whitehall were chanting "F*** the algorithm".

That crisis dominated the headlines but—whilst damaging to many students' academic opportunities (Duncan & Ors 2020)—was remedied (as best as it could be) without legislation. The Government simply reversed its initial position. However, this episode may be a portent of things to come, as society engages with deepfakes, autonomous weapon systems, driverless cars, persuasive but inaccurate AI chatbots, and emotionally appealing AI companions.

Next time, the harms to individuals and society might not be sufficiently addressed by a simple government backdown. The gap between society's understanding of AI and its likely impact is too great. An AI moral panic, in some shape or form, feels inevitable.

[D] OVERREACTION CAN LEAD TO BAD REGULATION

My reservations about the UK's current inaction do not place me in the "something must be done" camp. Hasty law is unhelpful; the aforementioned Dangerous Dogs Act is shorthand in Whitehall for misguided and badly built legislation (MCB Chambers 2021). Heavy-handed regulation could hinder innovation and, ultimately, the UK's productivity and global competitiveness. There is undeniably a global race to harness the powers of AI with a sense that, to the victor, the spoils (AP News 2017; Schmidt 2022).

Furthermore, I think AI-specific regulation faces three major implementation challenges. It is hard to:

1. define AI;
2. identify new risks and harms from AI; and
3. envisage a new regime being sufficiently scalable and effective.

Challenge 1: it is hard to define AI

Firstly, what on earth is AI? When we issued our AI guidance at the ICO in 2020 we dodged the question, stating that: "We use the umbrella term 'AI' because it has become a standard industry term for a range of technologies." We discussed this approach at length internally and concluded it would be unproductive to get pulled into a discussion around exact definitions.

Currently, discussions around AI can point to at least three different scenarios:

- ◊ recently it has been used to describe different types of generative AI, and often simply an individual experience of ChatGPT;
- ◊ among more informed people, more formal definitions are utilized, such as those noted below;[1] and

[1] Giacomelli (2023) provides an excellent overview of how many use cases can be envisaged just from the commercial application from Large Language Model (LLM) AI tools.

- ◊ among those less engaged in the details of AI, the scope can expand somewhat, to be a vehicle for all our hopes and fears around new technology.

Any AI-specific law will have to find a meaningful definition to use.[2] Definitions used recently include:

- ◊ "Artificial intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal … they can also adapt their behaviour by analysing how the environment is affected by their previous actions" (European Commission 2019.)
- ◊ "an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy" (AI RMF 1.0) (adapted from: OECD Recommendation on AI 2019; ISO/IEC 22989:2022).
- ◊ "highly autonomous systems that outperform humans at most economically valuable work" (OpenAI Charter 2018).
- ◊ "by reference to the 2 characteristics that generate the need for a bespoke regulatory response.
  - The 'adaptivity' of AI can make it difficult to explain the intent or logic of the system's outcomes:
    - AI systems are 'trained' – once or continually – and operate by inferring patterns and connections in data which are often not easily discernible to humans.
    - Through such training, AI systems often develop the ability to perform new forms of inference not directly envisioned by their human programmers.
  - The 'autonomy' of AI can make it difficult to assign responsibility for outcomes:
    - Some AI systems can make decisions without the express intent or ongoing control of a human" (HM Government 2023).

[2] The recent report by the US Chamber of Commerce's Commission on Artificial Intelligence Competitiveness, Inclusion, and Innovation (2023) includes a thoughtful and thorough discussion of the challenges of defining AI.

Each of these definitions differs substantially, but all cast a wide net, and to the semantically ambitious interpreter, can cover most modern computing activities. This should be a warning light for AI-specific law. It is not a specific technology of AI that we are seeking to regulate, it is just the activity of completing tasks by processing data.[3]

The challenges here are evidenced by the EU's efforts to define AI in its draft AI Act 2021, which in March 2023 shifted from a long definition which incorporated machine learning to a definition more closely aligned with the OECD definition.[4] The March 2023 revisions also included additional wording to ensure that recent generative AI models were captured by the Act (Bertuzzi 2017). Overall, the evolution of the AI Act should be applauded. There has been genuine engagement and refinement in the drafting that will hopefully result in a better product through the trilogue process, but the need to redefine the most fundamental definition in the draft Act does not broker great confidence in any definition's durability.[5]

[3] The White House's Blueprint for an AI Bill of Rights comes full circle on this, ending up close to our original ICO position. Having positioned itself as an AI-focused document, and having covered the principles it espouses, the Bill then expands its scope by stating: "While many of the concerns addressed in this framework derive from the use of AI, the technical capabilities and specific definitions of such systems change with the speed of innovation, and the potential harms of their use occur even with less technologically sophisticated tools. Thus, this framework uses a two-part test to determine what systems are in scope. This framework applies to (1) automated systems that (2) have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services."

[4] The original definition read: "(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods.' (Annex 1 of the European Commission's Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)." And now reads: "'artificial intelligence system' (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments." Source: AI Act (14 June 2023).

[5] Some would argue this has been a structural challenge within data protection regulation in the last 20 years. The Data Protection Act 1984 was driven by fear that large central government databases could support an Orwellian future. The Act also addressed the private sector, but in hindsight the role of data in our lives was still rudimentary. The GDPR-driven Data Protection Act 2018 seeks to regulate aspects of personal data processing across the full data lifecycle, a huge challenge given how personal data permeates everyday life. Resource challenges for Data Protection Authorities, the slow buildup to meaningful enforcement, and an ongoing flow of cases to higher courts to establish precedent can all be seen as symptoms of building a "regulation of everything". Adding another such layer of regulation through defining "AI" to cover most new technology over the next few years does not seem wise.

Figure 1: From NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST 2023)

Challenge 2: it is hard to identify new risks and harms from AI

In these circumstances, I question why new AI-specific regulation is a worthwhile exercise. Clearly, advances in machine-learning technology are accelerating our capabilities and exacerbating existing challenges, but in terms of the risks of harm it presents, I struggle to see the novelty.

For example, the NIST Framework (Figure 1) provides a model for describing harms related to AI systems. The Framework identifies real risks, which can easily increase in likelihood and impact when AI is involved but are inherent in any decision utilizing data, whether it is a deep-learning model or a spreadsheet built on a home personal computer. I am reminded of the 2017 case the American Civil Liberties Union (ACLU) brought against the state of Idaho, where the Department of Health and Welfare refused to disclose the reasons for cutting individuals' Medicaid assistance, claiming the third-party AI software contained "trade secrets" (ACLU 2016). When the ACLU prevailed, it found a badly built Microsoft Excel spreadsheet using incomplete historical data and a flawed statistical approach (Stanley 2017). Closer to home, the Post Office Horizon scandal destroyed lives without a whiff of AI.[6]

Why should an individual receive less protection if they are harmed by a technology that falls outside an arbitrary definition of AI? Clever lawyers for the state of Idaho, or for the Post Office, could likely have argued that the algorithms used were not AI; the harm for postmasters in the UK, or Idahoans needing Medicaid, remains the same.

6 See the Post Office Horizon IT Inquiry website.

This is why I remain sceptical about specific AI regulation. Trying to define AI is a valid and challenging activity for academics and other experts, but it is a time sink for policymakers and a sitting duck for future legal challenge.

Challenge 3: it is hard to envisage a new regime being sufficiently scalable and effective

The current output from data protection authorities has to be compared with the time it would take to build new frameworks and the time it would then take new regulators to regulate AI effectively. In the realms of both online harms (Gov.uk. 2020) and digital competition (Digital Competition Expert Panel 2019), the UK Government was contemplating legal and regulatory responses at least four years ago. At the time of writing, legislation addressing these areas has not yet been passed.

Once laws are passed, there will be many months and years of a fledgling regulator working out how to promote, educate and enforce around a new regime. Across Europe, it took most data protection authorities the first 18 months to get up to speed after the General Data Protection Regulation (GDPR) went live. Thinking up new structures and regulators is fine, but it is easy to forget the gap between desk work and the real world.

Contrast this with the speed at which AI is evolving. I must admit some personal pain here; in the time I've been writing this article, GPT-4, BARD and various other generative AI technologies have been made available to the general public, the UK's AI White Paper has been published, and the plans for the UK's AI Summit have been announced. This piece needed to be tweaked numerous times to cover the way the world has changed in recent months. Some references will be out of date by the time it is published. This pace of change will only continue, with an ongoing growth stage that will commoditize and consumerize AI and place real strain on our ability to distinguish the real from the fake and the fair from the unfair. Innovation, yet again, will outstrip new law and regulation.

[E] AN ALTERNATIVE APPROACH

In some ways the UK AI White Paper is proposing a middle way, with its reliance on sectoral regulation and a willingness to consider legislation at a later date. But there are material gaps that need to be addressed in the current regime, both in terms of legislation to address harms and in the powers and resources available to regulators.

The pessimist may think that we have a choice between no regulation and bad regulation. I hope there may be scope for an alternative approach, which utilizes existing law—especially in the world of data protection—and adapts them for the new world. This is not to say that the current UK data protection regime addresses all the risks AI presents, or that the current ICO can regulate AI as-is, but rather that it provides a platform and framework through which a new era of information regulation can emerge relatively quickly, alongside a regulator with the competence and capability to quickly cover this new challenge. Domain expertise of regulators is a pre-requisite for understanding the risks AI may bring, and data protection regulators are best positioned among their peers to move quickly and effectively.

To assess the viability of this option, we need to assess the gaps and synergies between current data protection regulation and a future AI-driven world.

[F] THE GDPR AND AI: POTENTIAL GAPS

The gaps between existing data protection regulation and the harms arising from AI data processing were well explored in the early years of the GDPR. The most obvious are in scope; the GDPR only regulates personal data processing, and so does not address societal or environmental harms, and struggles when harms are visited on a group rather than an individual.

Wachter & Mittelstadt argued that there were also potential limitations on how well the GDPR protects people even when their personal data is processed, stating:

> even if inferences are considered personal data, data subjects' rights to know about (Art 13-15), rectify (Art 16), delete (Art 17), object to (Art 21), or port (Art 20) them are significantly curtailed, often requiring a greater balance with controller's interests (e.g. trade secrets, intellectual property) than would otherwise be the case. Similarly, the GDPR provides insufficient protection against sensitive inferences (Art 9) or remedies to challenge inferences or important decisions based on them (Art 22(3)) (Wachter & Mittelstadt 2018; 2019).

Furthermore, there are specific pain points that different proposals for AI-specific regulation seek to address, many of which reflect our recent experience. These include:

- ◊ addressing issues in training datasets for AI, especially around bias, which some would argue could be covered by the "fairness" within

the GDPR, but at the risk of straining that concept to its breaking point;

- ◊ further developing the *ex ante* nature of the current data protection regime to fully address the risks posed by AI models being deployed rapidly and irreversibly—the GDPR already places some obligations on data controllers to undertake privacy assessments and sometimes pre-emptively engage with regulators, but does not envisage the speed and scale with which harmful AI could be deployed and propagated; and
- ◊ addressing redress and rectification when harms have been caused through data to generate a model, but the value (and possibly traces of the original data) resides in the model, and not the data in its original form. As noted below, the US Federal Trade Commission (FTC) has been experimenting with "algorithmic destruction", which may be part of the response to this new scenario, but this approach was not envisioned by legislators as current data protection/ consumer protection law was drafted.

Finally, there is a conceptual difference between the GDPR and the EU's prospective AI Act that could be seen as a feature or a bug. The AI Act utilizes a "product safety" approach, placing the onus on the developer of the AI system, as opposed to the GDPR, which focuses on the data controller, being the entity that determines the means and purposes of the processing. Crudely, the AI Act focuses on the maker of an algorithm, whereas the GDPR follows the activity of who is deciding what to do with the data.[7]

Overall, I have a preference for the GDPR approach, which seems better suited for a world of flexible foundational models, easily distributed functionality and long supply chains. However, it may be that we see a best-of-both model evolve, with some responsibilities on developers for taking a safety-by-design approach for reasonably anticipated usages, and then further obligations on entities taking subsequent decisions on how they deploy the technology.

[7] This is an oversimplification in both directions. The GDPR enshrined the concept of "data protection by design and default" which looks squarely at the developer of a personal data processing system whilst the EU draft AI Act places some obligations on deployers of AI systems, as explored in a blog by Demircan (2023).

[G] THE GDPR AND AI: POTENTIAL SYNERGIES—ARTICLE 22

More recently, there has also been a focus on what AI activities and harms are covered by the GDPR. This question is explored in a May 2022 Report (Barros Vale & Zanfir-Fortuna 2022a) from the Future of Privacy Forum (of which I am a Senior Fellow) which reviewed over 70 court judgments, decisions from data protection authorities, specific guidance and other policy documents issued by regulators, as they applied to real-life cases involving automated decision-making (ADM).

The report notes that much existing commentary has been focused on article 22 of the GDPR. Article 22 addresses data processing "which produces legal effects concerning him or her or similarly significantly affects him or her". It limits the lawful bases for processing personal data (to the performance of a contract, if required or authorized by domestic law, or with the data subject's explicit consent) and gives the data subject the right not to be subject to a decision based solely on automated processing.[8]

This represents a meaningful check on many AI use cases, introducing a form of appeals process for higher-impact decisions about people and requiring that data controllers "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests".[9] There remain challenges with this mechanism, both in ensuring that there is sufficient transparency so that people know when they should appeal,[10] and also in placing a reliance on fallible humans to form judgements on an appeal, but it is currently the most direct, established regulation we have.

[8] The scope of the "right" here is a bit unclear. In the eyes of the EDPB—comprised of the EU Data Protection Authorities—(which coordinates some work between those regulators, produces its own guidance, and sometimes makes decisions on enforcement cases) it is essentially a prohibition on higher-risk automated processing without a human in the loop, as the Article 29 Working Party noted in its 2016 Opinion, that was re-adopted by the EDPB in 2018: "The term right in the provision does not mean that Article 22(1) applies only when actively invoked by the data subject. Article 22(1) establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data."

The EDPB's position carries a lot of weight in Europe, of course, and may still serve as a reference point in the UK, but it is a strong interpretation of the article. This feels like an aspect of both the EU and UK GDPR that may become subject to case law in the future.

[9] This involvement of humans and automated decisions remains appealing to policymakers and the public alike. When the Prime Minister-commissioned Taskforce on Innovation, Growth and Regulatory Reform recommended removing article 22 from UK GDPR, in June 2021, the suggestion was picked up by the Department for Digital, Culture, Media and Sport in its September 2021 consultation "Data: A New Direction". Following substantial criticism from civil society, this was subsequently dropped as an idea in the Government's subsequent consultation in 2022.

[10] The Public Law Project "Tracking Automated Government register" is a good example of this visibility and how it can particularly affect vulnerable groups.

[H] THE GDPR AND AI: POTENTIAL SYNERGIES—BEYOND ARTICLE 22

Although Article 22 clearly has direct relevance to many AI use cases and is already subject to a wide range of case law and ongoing cases, it is not the only part of the GDPR relevant to ADM. As the authors of the FPF Report note:

> there are several safeguards that apply to such data processing activities, notably the ones stemming from the general data processing principles in Article 5, the legal grounds for processing in Article 6, the rules on processing special categories of data (such as biometric data) under Article 9, specific transparency and access requirements regarding ADM under Articles 13 to 15, and the duty to carry out data protection impact assessments in certain cases under Article 35 (Barros Vale & Zanfir-Fortuna 2022b).

This is, of course, then supported by the broader sweep of the GDPR, and its reliance on principles which are broadly similar to those in the 1995 Data Protection Directive, and to other data protection regimes around the world. In particular, the concept of "fairness" in the GDPR is both promising and open to challenge. Fairness is enshrined in Article 5 of the GDPR, and was also in the preceding Data Protection Directive 1995. For a long time, data protection authorities and courts only referred to fairness in the context of transparency and privacy notices, but the lack of further definition of fairness in the GDPR means the term can be interpreted widely to cover many of the challenges of AI. When discussing AI, data protection authorities often lean heavily on fairness, although the scope of this concept, in the context of the GDPR, has not yet been fully explored through case law. The ICO attempted to bridge this gap in March 2023 (ICO 2023c) as part of this updated guidance on AI (Hunton Andrews Kurth 2023).

It is important to note that in these areas of overlap there is already extensive enforcement and, to some degree, emerging case law. This is unsurprising. Data protection regulation in Europe is now fairly mature, and data protection regulators have had time to staff up, communicate expectations and start their work. Recent enforcement cases range from inadequate disclosures by Klarna Bank (*Klarna Bank* 2022) during credit applications, Uber's allocation of rides to drivers (*Uber* 2023), and the Slovakian Tax Authority's profiling of entrepreneurs for risk of tax fraud (*Slovakian Tax Authority* 2021). It is striking how clear the risk of harm

is in such cases, and how existing principles are already being used to address new challenges.[11]

[I] IN DEFENCE OF DATA PROTECTION AUTHORITIES

Data protection authorities have often been criticized for a lack of speed and/or ambition, and it is true that regulators can be cautious, given their constraints of resources and scope. But data protection regulators are increasingly intervening with confidence and sophistication.

- ◊ There is now meaningful global coordination, reflected in the increased activity and professionalism of the Global Privacy Assembly,[12] that has already taken action on Clearview AI (Swift 2022).
- ◊ There is a focus on deepening specialist skills in AI; in the last year, many regulators have followed the lead of the ICO in establishing a specialist AI function, including the Coordination Algorithms Directorate as part of the Dutch Data Protection Authority (Autoriteit Persoonsgegevens 2023; Iapp Daily Dashboard 2023), and its French counterpart, establishing an Artificial Intelligence Department (Commission Nationale de l'Informatique et des Libertés 2023).
- ◊ There are efforts to support innovation, with the ICO and subsequently many other data protection authorities introducing sandbox schemes to encourage engagement with innovators and specific projects.
- ◊ There is a wider use of enforcement powers beyond fines. The FTC is utilizing the sanction of "algorithmic destruction" to ensure that the inappropriate use of data does not result in a residual benefit to the controller in terms of a better-trained model (Caballar 2022; Federal Trade Commission 2022; Riley 2023). European regulators have leaned heavily on accountability provisions, in particular expecting or mandating the use of a data protection impact assessment, effectively forcing the data controller to fully engage with and address any risk that may arise from the processing (Hunton Andrews Kurth 2021).
- ◊ There has been a (relatively) rapid response to new developments in AI, with the ICO's swift updates to its AI guidance (as noted above) and the Italian regulator taking unilateral action against OpenAI,

[11] A common theme is how often AI is being used to make decisions about the less advantaged and the vulnerable; children, gig workers, benefits claimants. In the real world, AI is often used to make quick decisions about people who cannot push back.

[12] See the Global Privacy Assembly.

which resulted in changes to its disclosures and management of individual's rights (Mukherjee & Vagnoni 2023)—followed by the European Data Protection Board (EDPB) establishing a working group to engage with OpenAI on ChatGPT (EDPB 2023).

Here in the UK, the ICO continues to comment, guide and intervene on AI matters with increasing confidence, providing practical guidance on how to assess risk (ICO 2020), warning against risky applications of AI (ICO 2022b), enforcing in the most harmful cases (ICO 2022a) and maintaining a flow of blogs that provide guidance and insight as AI continues its rapid evolution (2023a; 2023b). The ICO's confidence reflects a competency built on years of experience gained from engaging with AI since its seminal paper on Big Data in 2017.

The ICO, now with the help of the Digital Regulation Cooperation Forum (DRCF), is also doing a great job at being a horizontal regulator in a world of (predominantly) sectoral regulators. Over the last few decades every sector has been digitalized and often personalized, meaning that the ICO has had to engage with different sectoral regulators over time. The same is true of AI, but we do not have the same luxury of time. Retailers are using AI at the same time as financial services firms and the Government. Understanding how to play well with other regulators—and avoiding a spiral into conflicting sectoral rules—will be a thematic challenge for AI regulation.

Put this all together, and you have a network of regulators that, albeit within their current scopes and not always with the speed others would like, are nevertheless building up an impressive competency and capacity to guide and intervene on AI cases.

[J] EVOLVING THE UK'S EXISTING INSTITUTIONS BRINGS SPEED, NOT HASTE

Given how long any AI-specific regulation would take, I think it is preferable that we use existing regulators and regulatory instruments, utilizing resources, skills and muscle memory to face the challenges of AI now, rather than in the second half of the decade.

The potential benefits go beyond speed and convenience. I believe that the GDPR approach of placing responsibility on the data controller, as opposed to the AI Act approach of placing more responsibility on the original developer of the AI, is more flexible and practical. The former approach links responsibility to data usage, which makes more sense when dealing with foundational applications with a broad scope of usage,

which may be utilized across a long supply chain. As I note above, it may be that in time we could evolve a best-of-both approach that places further obligations on AI developers, but we can leverage the existing data protection model to cover a lot of issues quickly.[13]

This is not to say that the current UK data protection regime covers all the risks arising from AI. As we have noted, there are some key limitations—both in the GDPR not fully addressing harm to individuals from their data being used in automated decision making, in terms of societal harms through the use of generative AI for misinformation/disinformation, and environmental harms incurred through the huge carbon costs of many deep-learning algorithms. And there are broader questions around areas such as IP, liability for harm, and discrimination which may sit outside of this overlap. But the large majority of use cases that advocates, policymakers and legislators refer to when discussing AI regulation are around the direct negative impacts on individuals through the use of their data.[14]

The remaining harms can then be addressed by adjustments to the existing UK data protection regime. These are unlikely to threaten the UK's "adequacy" status in the eyes of the EU, as they will be additive to the UK GDPR.

In terms of the UK's global competitiveness, the ICO has had to have regard for the UK's economic growth since the Deregulation Act 2015 (HM Government 2017), so this could easily be tweaked if it was felt AI was not adequately covered.

The heavier lift here is ensuring that the ICO has the resources to have adequate competency and capacity to develop AI guidance and pursue AI cases, which will require agility and technical skills that any regulator struggles to maintain. This would probably require additional funding for the ICO, but likely at a fraction of the cost of setting up a brand new regulator.

It should be noted that much of this approach is similar to the UK AI White Paper (in terms of avoiding brand new AI law for its own sake and

[13] I think in the medium term the global model will settle on a "best of both" approach, placing obligations on developers of AI to build transparent, explainable, controllable models, and obligations on users to deploy them responsibly. If this is the case, the UK can evolve its approach from a position of strength, in having moved swiftly to address the challenge of AI using its existing tools in the first instance.

[14] Using the EU AI Act as an example, the European Parliament's LIBE Committee proposed bans on remote biometric identification systems in publicly accessible spaces, predictive policing systems and emotion recognition systems. All these areas involve personal data processing and have been considered by Data Protection Authorities in various cases through the years.

leaning on existing regulatory frameworks) and the Ada Lovelace Institute's report "Regulating AI in the UK" (Davies & Birtwistle 2023) (which notes the need for urgency and recommends changes to the UK data protection regime, and also the creation of an AI ombudsman scheme). And it also mirrors some of the current trends we are seeing, such as the Dutch Data Protection Authority taking on formal responsibility for algorithms. But this approach goes further and faster by leaning into existing frameworks, and reduces the risk of the UK being slow off the mark.

[K] WHAT ELSE NEEDS TO BE DONE?

We are contemplating new regulation in a period of great uncertainty. AI is both an immediate use case in this new world, but is also a secondary factor in driving ongoing change in how technology is shaping our society and economy, such as through the hoarding of training data by large technology companies to gain market dominance against competitors. During my time at the ICO we recognized that the traditional boundaries of digital regulation were collapsing and worked with the Competition and Markets Authority (CMA) and Ofcom to set up the Digital Regulation Co-Operation Forum (DRCF) (which now also includes the Financial Conduct Authority).

The DRCF is already doing fantastic work on the intersection and tensions arising from our new world (CMA 2021), and the approach is being utilized in several other countries (Authority for Consumers and Markets nd). It feels like it could have a critical role to play in keeping up with the fast-moving world of AI, supporting all regulators in co-ordinating their efforts. The DRCF already plays this role to an extent,[15] but it feels like the DRCF could be fortified, formalized and better funded to ensure regulation is informed and fit for purpose. Depending on the role it had to play, this could include placing it on a statutory basis with some powers to intervene to meet its mandate.

To me, this makes much more sense than creating a new body as envisaged by the UK AI White Paper, which proposes a somewhat nebulous "central control function" to oversee the activities of existing regulators. The DRCF is already maximizing what can be achieved without supporting legislation, and is the ideal body to support further coordination between regulators in terms of obligations to mutually

[15] Objectives 4 and 5 of the DRCF are "Anticipate future developments by developing a shared understanding of emerging digital trends, to enhance regulator effectiveness and inform strategy" and "Promote innovation by sharing knowledge and experience, including regarding innovation in the approaches of regulators".

inform, support and even resolve differences between the regulatory scopes the existing regulators work under.

[L] CONCLUSION

The only thing we can be sure of is change. AI continues to surprise, delight and challenge us in equal measure, and there will be applications released that we cannot yet imagine. To anticipate this through rigid regulation is hubris, but to do nothing is equally unwise and risks us ending up with law written in haste. Otherwise, we risk chasing our tail, writing law with misguided aims (such as defining AI) to be enforced by regulators that will be late to the party.

For these reasons I think we should be planning for new regulation, but seeking to build on existing foundations, leveraging the substantial overlap in data processing and automated decision regulation that already exists with the UK GDPR, expanding the scope and resourcing of the ICO to enable it to match the speed and the complexity of the challenge we face, and asking the DRCF to help coordinate the mosaic of regulators to keep up with this new world.

That way we can create an environment which reassures the public that AI can be a force for good and support the innovation that will benefit us all.

About the author

Simon McDougall *is the Chief Compliance Officer of ZoomInfo, a B2B data company, and formerly Deputy Commissioner at the Information Commissioner's Office. He sits on the Board of the International Association of Privacy Professionals and is a Senior Fellow at the Future of Privacy Forum.*

Email: simon.mcdougall@zoominfo.com.

References

American Civil Liberties Union. "Federal Court Rules against Idaho Department of Health and Welfare in Medicaid Class Action" *Press Release* 30 March 2016.

Authority for Consumers and Markets. nd. "The Digital Regulation Cooperation Platform (SDT)" .

Autoriteit Persoonsgegevens. "Algoritmetoezicht AP van start." *Actueel* 16 January 2023.

Barros Vale, Sebastião & Gabriela Zanfir-Fortuna. *Automated Decision-Making under the GDPR: Practical Cases from Courts and Data Protection Authorities*. Future of Privacy Forum, May 2022 (2022a).

Barros Vale, Sebastião & Gabriela Zanfir-Fortuna. "FPF Report: Automated Decision-Making under the GDPR—A Comprehensive Case-Law Analysis." Future of Privacy Forum 17 May 2022 (2022b).

Bennett, O. "Dangerous Dogs." House of Commons Briefing Paper 4348, 10 August 2016.

Bertuzzi, Luca. "EU Lawmakers set to Settle on OECD Definition for Artificial Intelligence." *Euractiv* 7 March 2023.

British Board of Film Classification. nd. "The Video Recordings Act."

Burke, D. "GM Food and Crops: What Went Wrong in the UK?" *EMBO Report* 5(5) (May 2004): 432-436.

Caballar, Rina Diane. "'Algorithmic Destruction' Policy Defangs Dodgy AI: New Regulatory Tactic of Deleting Ill-gotten Algorithms Could Have Bite." *IEEE Spectrum* 15 April 2022.

Commission Nationale de l'Informatique et des Libertés. "The CNIL Creates an Artificial Intelligence Department and Begins to Work on Learning Databases." 26 January 2023.

Competition and Markets Authority. "Digital Regulation Cooperation Forum: Plan of Work for 2021 to 2022." 10 March 2021.

Davies, Matt & Michael Birtwistle. "Regulating AI in the UK: Strengthening the UK's Proposals for the Benefit of People and Society." London: Ada Lovelace Institute, 2023.

Demircan, Muhammed. "Deployers of High-Risk AI Systems: What Will Be your Obligations under the EU AI Act?" *Kluwer Competition Law Blog* 2 June 2023.

Department for Digital, Culture, Media and Sport. "Consultation Data: A New Direction." September 2021.

Digital Competition Expert Panel. *Unlocking Digital Competition*. HM Treasury 2019.

Duncan, P & Ors. "Who Won and Who Lost: When A-Levels Meet the Algorithm" *The Guardian* 13 August 2020.

European Commission. "Ethics Guidelines for Trustworthy AI." Brussels: High-Level Expert Group on Artificial Intelligence, 2019.

European Data Protection Board. "EDPB Resolves Dispute on Transfers by Meta and Creates Task Force on Chat GPT" *News* 13 April 2023.

Federal Register. "Request for Information: National Priorities for Artificial Intelligence." Science and Technology Policy Office, 5 May 2023.

Federal Trade Commission. "FTC Takes Action against Company Formerly Known as Weight Watchers for Illegally Collecting Kids' Sensitive Health Data" *Press Release* 4 March 2022.

Giacomelli, Gianni "GPTs and Business Process Industrialization." *Medium* 1 May 2023.

Gov.uk. "Online Harms White Paper: Full Government Response to the Consultation." CP 354, 15 December 2020.

Gov.uk. "Establishing a Pro-innovation Approach to Regulating AI: An Overview of the UK's Emerging Approach." Policy Paper: Department for Science, Innovation and Technology, Office for Artificial Intelligence, Department for Digital, Culture, Media and Sport & Department for Business, Energy and Industrial Strategy, 18 July 2022.

Gov.uk. "A Pro-Innovation Approach to AI Regulation". Policy Paper CP 815, 29 March 2023 (2023a).

Gov.uk. "The UK's International Technology Strategy." (AI White Paper) Policy Paper CP 810. Department for Science, Innovation and Technology & Foreign, Commonwealth and Development Office, March 2023 (2023b).

Gov.uk. "UK to Host First Global Summit on Artificial Intelligence" *Press Release* 7 June 2023.

Hall, Wendy & Jérôme Pesenti. "Growing the Artificial Intelligence Industry in the UK." Department for Science, Innovation and Technology, Department for Digital, Culture, Media and Sport & Department for Business, Energy and Industrial Strategy, 15 October 2017.

Hao, K. "The UK Exam Debacle Reminds Us that Algorithms Can't Fix Broken Systems." *MIT Technology Review* 20 August 2020.

Harvey, F. "Genetically Modified Food a Step Closer in England as Laws Relaxed" *The Guardian* 29 September 2021.

HM Government. "Growth Duty: Statutory Guidance." London: Department for Business, Energy and Industrial Strategy, 2017.

HM Government. "White Paper: A Pro-Innovation Approach to AI Regulation." HM Government, 2023.

Holistic AI. "Making Sense of China's AI Regulations." 22 August 2023.

Hunton Andrews Kurth. "Italian Garante Fines Deliveroo 2.5M Euros for Unlawful Processing of Personal Data" *Privacy and Information Security Law Blog* 5 August 2021.

Hunton Andrews Kurth. "UK ICO Issues Updated Guidance on AI and Data Protection" *Privacy and Information Security Law Blog* 16 March 2023.

IAPP Daily Dashboard. "Dutch DPA Begins Algorithm Enforcement Work." 18 January 2023.

Information Commissioner's Office. *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. London: ICO, 2017.

Information Commissioner's Office. "Guidance: Artificial Intelligence." London: ICO, 2020.

Information Commissioner's Office. "ICO Fines Facial Recognition Database Company Clearview AI Inc more than £7.5m and Orders UK Data to Be Deleted" *News* 23 May 2022 (2022a).

Information Commissioner's Office. "'Immature Biometric Technologies Could Be Discriminating against People' Says ICO in Warning to Organisations" *News* 26 October 2022 (2022b).

Information Commissioner's Office. "Blog: Addressing Concerns on the Use of AI by Local Authorities" *Blog* 19 January 2023 (2023a).

Information Commissioner's Office. "Generative AI: Eight Questions that Developers and Users Need to Ask" *Blog* 3 April 2023 (2023b).

Information Commissioner's Office. "How Do We Ensure Fairness in AI?" 2023c.

Lenhart, Anna. "Federal AI Legislation: An Analysis of Proposals from the 117th Congress Relevant to Generative AI Tools." Institute for Data, Democracy and Politics, George Washington University, June 2023.

MCB Chambers. 2021. "Thirty Years of the Dangerous Dogs Act: Time for Change."

Mukherjee, Supantha & Giselda Vagnoni. "Italy Restores ChatGPT after OpenAI Responds to Regulator" *Reuters* 28 April 2023.

National Institute of Standards and Technology. "Artificial Intelligence Risk Management Framework (AI RMF 1.0)." Information Technology Laboratory, NIST, 2023.

Riley, Tonya. "The FTC's Biggest AI Enforcement Tool? Forcing Companies to Delete Their Algorithms" *Cyberscoop* 5 July 2023.

Stanley, Jay. "Pitfalls of Artificial Intelligence Decisionmaking Highlighted In Idaho ACLU Case" *American Civil Liberties Union* 2 June 2017.

Swift, M. "Clearview AI, Adtech, Focus of Growing Global Data Protection Cooperation" *Mlex* 12 April 2022.

UNESCO. "UNESCO Adopts First Global Standard on the Ethics of Artificial Intelligence." 8 April 2022.

United States Chamber of Commerce. *Report of the Commission on Artificial Intelligence Competitiveness, Inclusion, and Innovation*. Washington, 2023.

Warren, Samuel D & Louis D Brandeis. "The Right to Privacy." *Harvard Law Review* 4(5) (1890): 193-220.

Wachter, Sandra & Brent Mittelstadt. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI" *Oxford Business Law Blog* 8 October 2018.

Wachter, Sandra & Brent Mittelstadt. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." *Columbia Business Law Review* 2 (2019).

White House. "Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People." Office of Science and Technology Policy, nd.

White House. "Fact Sheet: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI." *Briefing* 21 July 2023.

Ye, Josh. "China Says Generative AI Rules to Apply only to Products for the Public" *Reuters* 14 July 2023.

Legislation, Regulations and Rules

Dangerous Dogs Act 1991

Data Protection Act 1984

Data Protection Act 2018

Deregulation Act 2015

European Union. Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending Certain Union Legislative Acts, COM(2021) 206 final, 21 April 2021 (Draft AI Act)

ISO/IEC 22989:2022: Information Technology – Artificial Intelligence – Artificial Intelligence Concepts and Terminology, July 2022

OECD Legal Instruments. "Recommendation of the Council on Artificial Intelligence", adopted on 22 May 2019

OpenAI Charter, 9 April 2018

Video Recordings Act 1984

Cases Cited

Klarna Bank AB 31 March 2022

Uber BV 4 April 2023 (C/13/692003 / HA RK 20-302)

Ústavného súdu Slovenskej republiky (*Slovakian Tax Authority*), Case 492/2021 Z. z., 10 November 2021