

Innovation and opportunity: review of the UK's national AI strategy

Emre Kazim¹ · Denise Almeida² · Nigel Kingsman¹ · Charles Kerrigan³ · Adriano Koshiyama¹ · Elizabeth Lomas² · Airlie Hilliard⁴

Received: 24 November 2021 / Accepted: 29 November 2021

Published online: 06 December 2021

© The Author(s) 2021 [OPEN](#)

Abstract

The publication of the UK's National Artificial Intelligence (AI) Strategy represents a step-change in the national industrial, policy, regulatory, and geo-strategic agenda. Although there is a multiplicity of threads to explore this text can be read primarily as a 'signalling' document. *Indeed, we read the National AI Strategy as a vision for innovation and opportunity, underpinned by a trust framework that has innovation and opportunity at the forefront.* We provide an overview of the structure of the document and offer an emphasised commentary on various standouts. Our main takeaways are: *Innovation First*: a clear signal is that innovation is at the forefront of UK's data priorities. *Alternative Ecosystem of Trust*: the UK's regulatory-market norms becoming the preferred ecosystem is dependent upon the regulatory system and delivery frameworks required. *Defence, Security and Risk*: security and risk are discussed in terms of *utilisation* of AI and *governance*. *Revision of Data Protection*: the signal is that the UK is indeed seeking to position itself as less stringent regarding data protection and necessary documentation. *EU Disalignment—Atlanticism?*: questions are raised regarding a step back in terms of data protection rights. We conclude with further notes on data flow continuity, the feasibility of a sector approach to regulation, legal liability, and the lack of a method of engagement for stakeholders. Whilst the strategy sends important signals for innovation, achieving *ethical innovation* is a harder challenge and will require a carefully evolved framework built with appropriate expertise.

Keywords Artificial Intelligence · Strategy · Innovation · Regulation · Compliance · Defence · Data · Data protection · Accountability · Governance

1 Introduction

The publication of the UK's National AI Strategy [1] represents a step-change in the national industrial, policy, regulatory, and geo-strategic agenda. Whereas AI has previously been discussed under the remit of other strategies (such as the Industrial Strategy and within the framework of Digital Regulations), with this publication AI takes centre stage. This represents the concretisation and maturation of perspectives of various bodies and institutions tasked with addressing various dimensions of AI research, innovation, industry, policy, and regulation (cf. Centre for Data Ethics and Innovation, Office for AI, The Alan Turing Institute, Information Commissioner's Office etc.). Although there is a multiplicity of threads to explore, both in terms of actionable steps ('short', 'medium' and 'long term', across the verticals of 'ecosystem', 'sectors/regions', and 'governance') this text can be read primarily as a 'signalling' document.

✉ Emre Kazim, emre.kazim@holisticai.com | ¹Holistic AI, London, UK. ²University College London, London, UK. ³CMS, London, UK. ⁴Goldsmiths University of London, London, UK.



Indeed, we read the National AI Strategy as a vision for innovation (research, SMEs) and opportunity (industry, economy), underpinned by a trust framework that has such innovation and opportunity at the forefront of any standard and regulatory framework.

In this white paper, we provide an overview of the structure of the document and offer an emphasised commentary on various standouts (Sect. 2). Following this, we offer our initial thoughts and feedback on strategic points of contention in the Strategy (Sect. 3—those interested in this commentary can move immediately to this section).

Below we succinctly reproduce our main takeaways (each point is expanded upon in Sect. 3):

- **Innovation first:** The clearest signal from the National AI Strategy is that it places the ability to innovate at the forefront of its approach to AI. AI innovation is read into all other streams, such as a vehicle for economic growth and competitiveness globally.
- **An Alternative ecosystem of trust:** Although the UK's Information Commissioner agreed on the adequacy for UK-EU data transfers quite early on in the Brexit negotiation process, the UK proposed a National Data Strategy [2] that in some ways steps away from the European framework and inches closer to a US approach to privacy, much more focused on economic outcomes and innovation. There is a delicate balancing act between incentivising innovation and indirectly encouraging isolationism and a retreat from being a trusted data custodian.
- **Defence, security and risk:** References to defence, security and risk are made throughout the text. Two dimensions are found: the first is *Utilisation*: in the form of research, utilisation and modernising the operations of the Ministry of Defence; the second is *Governance*: the Strategy suggests research and understanding of long term risk and a strategy to defend against the malign use of AI.
- **Revision of data protection:** It has been an open question as to whether or not the UK would move towards a data protection regime that is 'lighter' than the EU approach. Although talk is mainly of 'revision' and 'review', the signal is that the UK is indeed seeking to position itself as less stringent regarding data protection. The potential intent to minimise documentation requirements aligns to this potential shift.
- **EU disalignment—Atlanticism?:** A focus on innovation and economic advancement is continuously touted as a step away from the EU's regulatory strategy. Additionally, a potential move away from the European approach might have global implications as the GDPR holds some sway outside of the EU as well (since any business dealing with the bloc has to adhere to the rules when managing European's data). This raises the question—is the National AI Strategy simply pro-innovation or is it, in fact, a step back in terms of data protection rights? To this, we invite a deeper discussion regarding innovation enabling standards and regulation.

In conclusion, we briefly offer points of contention to stimulate the discussion further. These are:

- **Signal not strategy:** the Strategy is a signalling of geopolitical and economic plans, not as a strategy for the development of well governed AI.
- **Data flow continuity:** we have some concerns around the continuity of data flows between the EU and UK.
- **Sectors:** it will be a difficult task to produce rules that are specific enough to provide clarity for sector specific industry.
- **Liability:** the Strategy does not make clear the likely positions to be reached on legal liability.
- **Method of engagement:** the Strategy does not disclose the methodology for developing the regulation/rules or how stakeholders will be engaged in the process.
- **Accountability to citizens:** any replacement system does need to retain the intrinsic concept of 'privacy by design' whilst potentially rebalancing and reframing the systems that achieve this.

2 Overview

In this section, we provide an overview of the Strategy document. We reproduce the structure of the text and explicate in summary form. Whilst this section provides an overview, it is presented as a reading of the text within which the overview, together with commentary, is interwoven.

2.1 Ten-year plan

The document begins with an aspirational ideal of Britain as a 'global AI superpower'. It is noteworthy that from the outset the phrase 'race' is mentioned in the context of other countries—*signalling the geostrategic dimension*—both in terms of the economy and the delivery of 'technological transformations'. It is following this that the regulatory environment (ethical and regulatory) is mentioned, and this is done so explicitly with 'pro-innovation' as the guiding principle (underpinning the opportunity—innovation and economic—proclaimed in the aspiration).

'This National AI Strategy will signal to the world our intention to build the most pro-innovation regulatory environment in the world'

It is clear that this is an *industrial and geopolitical vision*, with strong positioning of the UK as both a leader in the development and deployment of AI but also as a leader in establishing market rules.¹

2.2 Executive summary

The executive summary not only summarises the document, but re-emphasises the vision that the UK will be a 'hive of global talent and a progressive regulatory and business environment'. The vision is explicated through action in three demarcated domains, namely *ecosystem*, *sectors/regions* and *governance*, each of which is truncated into *short term* (next 3 months), *medium term* (next 6–12 months) and *long term* (12+ months) actions and objectives. These are summarized below:

- Ecosystem: Investment and planning for leadership in science with a view to being an AI superpower
 - Short term: data availability, Cyber-Physical Infrastructure Framework, skills.
 - Medium term: publish skills agenda (grounded in the idea of supporting broader access to AI skills building and career opportunities), evaluate private funding, education programmes, careers, review compute power, UK-USA R&D declaration, new visa regimes.
 - Long term: review semiconductor supply chains, consider open and machine-readable government datasets, launch national research and innovation programmes, global partnerships, back diversity in AI, monitor protection of national security, include provisions on emerging technologies in any trade deals.
- Sectors/regions: Support transition to AI-enabled economy for all sectors and regions
 - Short term: strategy for health and social care, defence, intellectual property.
 - Medium term: strategy of diffusion, innovation missions, build an open repository of challenges, support for developing countries.
 - Long term: launch a programme for adoption of AI, develop trustworthiness, adoptability and transparency, using AI as a 'catalytic contribution' to strategic challenges.
- Governance: Ensure national and international governance to encourage innovation, investment, and protect the public and the UK's fundamental values
 - Short term: publish assurance roadmap, consultation on data protection and governance, use in defence, international AI activity.
 - Medium term: pro-innovation white paper, analysis of algorithmic transparency, pilot an AI Standards Hub, increase government's awareness of AI safety.
 - Long term: technical standards engagement, work globally on shared R&D challenges, update guidance on AI ethics and safety in the public sector, understand what public sector actions can safely advance AI and mitigate catastrophic risks.

¹ We note that others have focused on the document as a 'roadmap' i.e. within the context of tangible steps and actions. Our contribution focuses more on the strategic elements. see Goodson [3].

2.3 Pillar 1: Investing in the long-term needs of the AI ecosystem

We read the first pillar as touching upon three themes, namely research, infrastructure and economy.

- Research:

- National programmes: here research, development and innovation is touted via a National AI Research and Innovation (R&I) Programme. Designed to meet five main aims, the programme will
 - facilitate the discovery and development of new AI technologies,
 - maximise the creativity of researchers,
 - support the recruitment of AI innovators,
 - build collaborative partnerships,
 - and support innovation in the private sector.

The belief is that this will 'greatly increase the type, frequency and scale of AI discoveries which are developed and exploited in the UK'. Further, international collaboration on research and innovation is cited, with both *Horizon Europe* [4] and initiatives with the USA mentioned.

- Skills: increasing diversity and closing the skills gap through postgraduate conversion courses in data science and artificial intelligence (including visa programmes).
- Infrastructure:
 - Data and compute: Access to data, standardisation and infrastructure (cloud) are key areas to address. Within the public sector, data is to be used to support data-driven innovation to support public services. Access to compute capacity (for training AI systems) is a second *Infrastructure* priority since security and competition need to be considered.
- Economics:
 - Finance and VC: a continued evaluation of the state of funding specifically for innovative firms developing AI technologies across every region of the UK, to assess whether there are *significant investment gaps or barriers to accessing funding* that AI innovative companies are facing.
 - Trade: As the UK secures new trade deals, the government will include provisions on emerging digital technologies, including AI. These provisions will ensure that while personal data is protected, there will be no unnecessary barriers preventing data crossing borders.

2.4 Pillar 2: ensuring AI benefits all sectors and regions

We read the second pillar as touching upon two themes, the spread of AI (research, development, deployment etc.), and innovation.

- Spread:

- Diffuse and stimulate: diffusion of AI across the whole economy to drive economic and productivity growth due to AI, as well as to stimulate the development and adoption of AI technologies in high-potential, low-AI maturity sectors. A programme will be launched to support businesses and increase opportunities for growth and collaboration through incentivised learning.

- Innovation:

- Innovation missions: the government will develop a repository of short, medium and long term AI challenges to motivate industry and society to identify and implement real-world solutions to the strategic priorities (e.g. net zero, health and social care). To this end, AI will be pushed for use in the public benefit (conceiving of AI

as a 'catalytic contribution' [5]). Finally, the public sector will be enabled as a buyer (examples mentioned are the MoD which is using AI to optimise electricity supply, and the Crown Commercial Service which is working towards improving access to purchasing AI technologies) and also as a lever for stimulating innovation and adoption of AI.

- Intellectual property (IP): Creating and protecting Intellectual Property (which we read both in the context of fears regarding the ease with which IP theft is possible in the context of AI development and adoption, and in geopolitical terms).

2.5 Pillar 3: governing AI effectively

We read the third pillar as touching upon two themes, namely Trust Enabling Innovation and Standards/Regulations. We believe that the 'new direction' cited with respect to data protection is of particular importance.

- Trust Enabling Innovation:
 - Global: The government's aim is to build the most trusted and pro-innovation system for AI governance in the world, to support 'innovation and adoption while protecting the public and building trust'. Their plan for digital regulation [6] recognises the need for well-designed frameworks to drive the economy by balancing levels of privacy and restriction.
 - AI Assurance: To support the development of a mature AI assurance ecosystem, the CDEI is publishing an AI assurance roadmap. We eagerly anticipate this work, given our interest in AI assurance and having contributed to the development of this agenda through our research work and industry experience in AI Auditing [7, 8].
 - Public sector as an exemplar: this is a mechanism to use the public sector as both an adopter and innovator of AI. We note that this is particularly clear in the vision for the use and standardization of public datasets.
 - AI risk, safety, and long-term development: in this context the discussion is more speculative, touching on issues of existential risk, such as the development of AGI (artificial general intelligence) and (national) defence. The role of the Office for AI in exploring long-term risk is cited.
- Data protection:
 - Data protection framework and AI: a new direction for Data Protection geared towards innovation has been clearly spelled out by the government in its Digital Regulation Strategy proposal [6]. Whilst the National AI Strategy recognises the need for more regulation in this space, it does point to some legislative coverage by existing UK regulators for some parts of AI technologies. However, a few of these regulators have not actively enforced in this space, despite it being in their scope. An example of this is the Information Commissioner's Office, which, according to our perspective, has not always taken a strong stance on GDPR enforcement. In addition, this change needs to be set against the proposals to remove the Information Commissioner's autonomy making the Commissioner accountable to the Department of Digital, Culture, Media & Sport. As such, the ability to hold the Government to account will be severely reduced. *Whilst improvements to regulation are welcome, and very necessary in this space, we also need to bring the dialogue into practical terms and understand how this will be applied and enforced on real cases and real data.*
 - Data adequacy in post-Brexit UK: the document presents an approach and partnership in line with the EU AI act [9, 10]. However, some proposals have the risk of being a potential step back from measures introduced by the GDPR. It is still unclear what the potential impact is of the implementation of strategies such as the National AI Strategy on the current EU-UK GDPR adequacy decision [11].
- Standards/regulation:
 - Policy signal: Three perspectives are presented, namely:

- i. *Removing some existing regulatory burdens* where there is evidence they are creating unnecessary barriers to innovation.
 - ii. *Retaining the existing sector-based approach*, ensuring that individual regulators are empowered to work flexibly within their own remits to ensure AI delivers the right outcomes.
 - iii. *Introducing additional cross-sector principles or rules*, specific to AI, to supplement the role of individual regulators to enable more consistency across existing regimes. For some time there has been significant signalling that the UK will take a sector-specific approach, as such the inclusion of this cross-sector regulatory policy is an important shift.
- **Coordination:** coordination is presented at both the national level (UK regulators such as the FCA, CMA, ICO, Ofcom, etc.) and internationally (those mentioned are OECD [12, 13], Council of Europe, Global Partnership on AI (GPAI), UNESCO, NATO (AI Partnership for Defence)).
 - **(Global) Digital Technical Standards:** that the UK can lead in the development of technical standards is seen as a means to support R&D and innovation, trade, 'giving UK businesses more opportunities', 'delivering on safety, security and trust', and, 'supporting conformity assessments and regulatory compliance'. These technical standards, developed through an industry-led process, aim to benefit UK citizens, businesses, and the economy through safe and efficient AI [14].

3 Commentary

3.1 Innovation first

The clearest signal from the National AI Strategy is that it places innovation at the forefront.² Innovation is read into all other streams, such as a vehicle for economic growth and competitiveness globally. Indeed, research is discussed in the context of adoption (i.e. industry) and in terms of 'catalytic contribution' to national aims and challenges (such as in health and net zero). Further, the skills agenda (skill read in terms of vocation and ability, which is subtle but notably different than speak of education) is two-pronged, with both the facilitation of talent (via visa provision) and in the national educational programmes (to be consulted upon). Finally, innovation, in the pro-innovation sense, underpins the governance agenda, which is explicitly discussed in terms of enabling innovation.

3.2 An alternative ecosystem of trust

The UK's Information Commissioner agreed on the adequacy for UK-EU data transfers quite early on in the Brexit negotiation process. On the other hand, an opinion by the European Data Protection Board around the possibility of the adequacy of data transfers from the EU to the UK only materialised in March 2021. This opinion states the similarity of the UK data protection framework to that of the EU and grants adequacy but finishes by stating: '(...) whilst laws can evolve, this alignment should be maintained.' [15]. *Whilst this is a seemingly innocent statement, it is a reflection of months of tension and negotiations, in the middle of which the UK proposed a National Data Strategy [2] that in some ways steps away from the European framework and inches closer to a US approach to privacy, much more focused on economic outcomes and innovation.* It is also worth noting this decision is effectively temporary as, for the first time, it includes a sunset clause which effectively allows it to expire after 4 years. For a critique of the Data Strategy see [16]. This tension can have significant impacts in the tech sector in general [17] and AI technology in particular.

There is a particularly delicate balancing act to be done between incentivising innovation and indirectly encouraging isolationism and degradation of individual rights, or doing so by providing a space which creates opportunities for ethical and regulation innovation. We can state the opportunity and risk in terms of isolationism and an alternative ecosystem of trust:

² To cursorily evidence this claim, we note that the word innovation (116) and opportunity/opportunities (29) appear(s) a total of 145 times. Comparatively, the culmination of the incidence of terms associated with governance, such as, governance (25), trust/trustworthiness/trustworthy (23), safety (18), accountability (2), transparency, (11), appear a total of 79 times.

- **Isolationism:** here the concern is that the UK will become isolated in its regulatory and innovation ecosystem, where industries will choose to follow larger regulatory/market ecosystems—similar to how EU GDPR became the de facto global standard (and thus effectively universalising the EU ecosystem), the UK may find itself in a position that it will be, ultimately, compelled to conform to the larger regulatory-market force. An additional possibility is that the UK becomes an incubator—where testing and innovation occurs—thereby functioning as a launchpad viz. a more innovation-friendly space for start-ups and industry. Given the desire to be a global leader, these possibilities are read negatively with respect to the stated aims of the Strategy.
- **Alternative ecosystem of trust:** here the opportunity is for the UK's regulatory-market norms to become a preferred ecosystem for innovation and trust. The UK's approach may be thought of as an alternative trust scheme that is (just as) trustworthy (as the EU) but more pro-innovation. Through the UK's various influence mechanisms (soft power through language and culture; a permanent seat on the UN security council; the Commonwealth; etc.) a sufficiently large regulatory-market ecosystem can emerge (think of UK-Canada-India-Australasia etc.) to rival the EU (and perhaps even become the de facto global norm). However, to provide this level of assurance, the UK will need to have robust alternative frameworks in place and an accepted regulatory system.

In sum, there is a delicate balancing act between incentivising innovation and indirectly encouraging isolationism and a retreat from being a trusted data custodian.

3.3 Defence, security and risk

References to defence, security and risk are made throughout the text. The publication of a defence strategy through the Ministry of Defence (including regarding the governing of related defence implications) is a short term aim. More generally, two dimensions are found:

- **Utilisation:** The first is 'defence' in the form of research and utilisation of systems. Here a new Defence AI centre (viewed to become 'a science superpower in defence') is proposed—although not explicitly mentioned, we read this as a significant signal regarding military capabilities. Additionally AI is to be used in modernisation and operations of the Ministry of Defence.
- **Governance:** The second is governance based. The ethical (and legal) implications of AI in defence are likely to be central to the defence strategy—the Strategy suggests research and understanding of long term risk (safe advancement of AI and the mitigation of catastrophic risks) and a strategy to defend against the malign use of AI.

Given that it is often concerned with the use of AI in defence capacities that garners the most attention, the navigation of advancing AI research and utilisation with the need for good governance is particularly acute. Additionally, we have chosen to highlight this dimension because it indicated the seriousness with which the British state takes the development and deployment of AI. It is important to note the protected landscape in which defence operates and in fact to consider whether in this regard Britain could make changes whilst being more open and transparent than national norms.

3.4 Revision of data protection

Data protection provisions in the UK have been largely aligned with those of the European Union, with the UK taking a leading role in the development and implementation of the EU's approach to data protection, throughout its years as a Union member-state (c.f. UK GDPR).

It has been an open question as to whether or not the UK would move towards a data protection regime that is 'lighter' than the EU approach. Although talk is mainly of 'revision' and 'review', the signal is that the UK is indeed seeking to position itself as less stringent regarding data protection.

There are two dimensions to this:

- **Enablers:** here, opening access to data (including public data), data standardisation, and the cyber-physical infrastructure support is included in the Strategy. This is critical because access to quality and sufficient data is crucial to the development of AI. It is hoped that a more open regime with respect to data protection will increase the use and possibilities of innovation with respect to AI.

- Data protection as value: European GDPR (boldly) claims that data protection is a fundamental right—given such an explicitly stated value, the prominence of data protection in data governance is understandable. However, as we have discussed elsewhere, the relationship between data protection and AI performance (how accurate a system is), fairness (how does a system impact people with respect to protected characteristics, such as race and religion) and transparency (how much explainability a system is said to have) is one where it is often a *trade-off* [8]. An indicative example would be that securing a high level of data protection is likely to result in a diminished level of transparency. In effect, the UK strategy is challenging the primacy of data protection as the *foundational* value of data governance by putting forward other values (performance of a system, etc.) and opportunities (expressed in terms of the value ‘opportunity and innovation’). For our commentary on the interrelation between data and AI ethics see [18].

This signal in the shift with respect to the primacy of data protection in data governance will have implications on the economy (see point 3.1 above), innovation (what kinds of products may emerge, the make-up of the start-up ecosystem, etc.), governance (the nature of accountability) and law (revision of existing laws).

3.5 EU Disalignment—Atlanticism?

A focus on innovation and economic advancement is continuously touted as a step away from the EU’s regulatory strategy. However, in its own aspirations, economic development is a key factor of the European approach to privacy: data protection is intended to regulate and allow for the processing of personal data, when required and in a transparent manner, thus supporting economic goals [19]. Some propose the idea that “(...) some of the most important implications of the GDPR may not relate to privacy, but to antitrust and trade policy” ([20], p. 50).

Additionally, a potential move away from the European approach might have global implications as “the GDPR holds some sway outside of the EU as well, since any business dealing with the bloc has to adhere to the rules when managing European’s data” ([21], p. 3). Whilst some of the intended goals of driving innovation have merit on their own, the government must carefully assess the consequences of any changes which might disrupt existing data flows and enforcement cooperation.

This raises the question—is the National AI Strategy simply pro-innovation or is it, in fact, a step back in terms of data protection rights? Indeed, we believe it is critical to explore, at length and through consultation with all stakeholders (industry, startup, NGOs and academia) the nature of how a relaxing of some data protection provisions may impact innovation—this is not to deny the apparent maxim ‘more data—more innovation’ but instead to think about innovation as enabling standards and regulation (which the EU will claim is indeed their stated aim).³

4 Conclusion

In conclusion, we briefly offer points of contention to stimulate the discussion further. These are:

- Signal not strategy: Whilst the document is advertised as a National Strategy for Artificial Intelligence, the bulk of its contents certainly reads more as a signalling of geopolitical and economic plans and how AI can support those, not as a strategy for the development of ethical, innovative and well governed AI. As such we read this document not as a roadmap but instead as a point of departure with respect to the UK’s AI governance approach.
- Data flow continuity: We have some concerns around the continuity of data flows between the EU and UK if some of the points of this strategy are implemented, which could contribute to further isolation of the UK in the international digital space. This concern ties very much into the opportunity and risk associated with the UK positioning itself as a more relaxed ecosystem (which respect to data governance).
- Sectors: It is a laudable ambition to have cross-sector regulation but it will be a difficult task to produce rules that are specific enough to provide clarity for industry. Furthermore, it is not clear to what extent the new rules will build on work already done such as the various recent reports and guides issued by the Information Commissioner’s Office.

³ For example, see this discussion on how frameworks can enable commercial activity by the UK’s Solicitors Regulatory Authority.

- **Liability:** There are some big questions in AI regulation relating to, for example, responsibility and liability. The Strategy does not make clear the likely positions to be reached on those. Indeed, for some time we have highlighted broader questions on algorithms and the law, and the legal status of algorithmic systems.
- **Method of engagement:** The Strategy does not disclose the methodology for developing regulation/rules or how stakeholders will be engaged in the process. This is a concern raised by others (e.g. Goodson [3]) and something we too echo. Furthermore, in order to achieve this at a global level, significant expertise in diplomatic and subject matter competency would be required.
- **Accountability to citizens:** Clearly innovation does bring societal benefits but potentially at the expense of individual citizen rights if the frameworks that evolve are not ethical and robust. Whilst aspects of the GDPR may have been seen to be onerous nevertheless the concept of 'privacy by design' is at its heart to be commended. As such any replacement system does need to retain this intrinsic concept whilst potentially rebalancing and reframing the systems that achieve this.

We would call for ethical innovation. This requires both interdisciplinary subject expertise and global diplomacy if it is to be achieved. In addition those boundaries over which the UK will not step need to be more clearly articulated if it is to establish alternative data custody systems. New approaches to AI development and data protection are there to be seized but require a sophisticated analysis and resourcing to properly document and develop ethical AI innovation. Whilst this document sends important signals for fostering and growing innovation, achieving ethical innovation is a harder challenge and will require a carefully evolved framework built with appropriate expertise.

Authors' contributions EK was responsible for writing, conceptualisation and summary structure. DA was responsible for the section on data protection and the strategic view. NK was responsible for writing, geopolitical commentary and AI strategic view. CK was responsible for the conclusion and legal commentary. AK was responsible for conceptualisation. EL was responsible for the data protection section and strategic view. AH was responsible for conceptualisation. All authors read and approved the final manuscript.

Declarations

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Office for Artificial Intelligence. National AI strategy; 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020402/National_AI_Strategy_-_PDF_version.pdf
2. Department for Digital, Culture, Media & Sport. Government response to the consultation on the National Data Strategy; 2021b. <https://www.gov.uk/government/consultations/uk-national-data-strategy-nds-consultation/outcome/government-response-to-the-consultation-on-the-national-data-strategy>
3. Goodson M. The UK AI strategy: Are we listening to the experts?; 2021. <https://datasciencesection.org/2021/09/13/the-uk-ai-strategy-are-we-listening-to-the-experts/>
4. European Commission. Horizon Europe: Strategic plan 2021–2024. Publications Office of the European Union; 2021b. <https://data.europa.eu/doi/https://doi.org/10.2777/083753>
5. Prime Minister's Office. Prime Minister sets out plans to realise and maximise the opportunities of scientific and technological breakthroughs [Press Release]; 2021. <https://www.gov.uk/government/news/prime-minister-sets-out-plans-to-realise-and-maximise-the-opportunities-of-scientific-and-technological-breakthroughs>
6. Department for Digital, Culture, Media & Sport. Digital regulation: Driving growth and unlocking innovation; 2021a. <https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation/digital-regulation-driving-growth-and-unlocking-innovation>
7. Ahamat G, Chang M, Thomas C. The need for effective AI assurance. Centre for Data Ethics and Innovation Blog; 2021. <https://cdei.blog.gov.uk/2021/04/15/the-need-for-effective-ai-assurance/>
8. Koshiyama A, Kazim E, Treleaven P, Rai P, Szpruch L, Pavey G, Ahamat G, Leutner F, Goebel R, Knight A, Adams J, Hitrova C, Barnett J, Nachev P, Barber D, Chamorro-Premuzic T, Klemmer K, Gregorovic M, Khan S, Lomas E. Towards algorithm auditing: a survey on managing legal, ethical and technological risks of AI, ML and associated algorithms. SSRN Electron J. 2021. <https://doi.org/10.2139/ssrn.3778998>.

9. European Commission. Proposal for a regulation laying down harmonised rules on artificial intelligence; 2021c. <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence>
10. Kazim E, Kerrigan C, Koshiyama A. EU proposed AI legal framework. SSRN Electron J. 2021. <https://doi.org/10.2139/ssrn.3846898>.
11. European Commission. Commission adopts adequacy decisions for the UK [Text]. European Commission—European Commission; 2021a. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183
12. Koshiyama A, Kazim E, Treleaven P. Familiar methods can help to ensure trustworthy AI as the algorithm auditing industry grows; 2021. <https://oecd.ai/en/wonk/algorithm-auditing-trustworthy-ai>
13. Organisation for Economic Co-operation and Development. OECD principles on Artificial Intelligence; 2021. <https://www.oecd.org/going-digital/ai/principles/>
14. Kazim E, Polle R, Carvalho G, Koshiyama A, Inness C, Knight A, Gorski C, Barber D, Lomas E, Yilmaz E, Thompson G, Ahamat G, Pavey G, Platts K, Szpruch L, Gregorovic M, Rodrigues M, Ugwu-dike P, Nachev P, Goebel R. Towards AI standards: thought-leadership in AI legal, ethical and safety specifications through experimentation. SSRN Electron J. 2021. <https://doi.org/10.2139/ssrn.3935987>.
15. European Data Protection Board. European Data Protection Board—48th Plenary Session; 2021. https://edpb.europa.eu/news/news/2021/european-data-protection-board-48th-plenary-session_en
16. Taunton K. Government reveals plans for post-Brexit data regime. Panopticon; 2021. <https://panopticonblog.com/2021/09/17/government-reveals-plans-for-post-brexit-data-regime/>
17. McCann D, Patel O, Ruiz J. The cost of data inadequacy: The economic impacts of the UK failing to secure an EU data adequacy decision (UCL European Institute Report with the New Economics Foundation); 2020. https://neweconomics.org/uploads/files/NEF_DATA-INADEQUACY.pdf
18. Kazim E, Koshiyama A. The interrelation between data and AI ethics in the context of impact assessments. *AI and Ethics*. 2021;1(3):219–25. <https://doi.org/10.1007/s43681-020-00029-w>.
19. Johnson G, Shriver S. Privacy & market concentration: intended & unintended consequences of the GDPR. SSRN Electron J. 2019. <https://doi.org/10.2139/ssrn.3477686>.
20. Peukert C, Bechtold S, Batikas M, Kretschmer T. European privacy law and global markets for data. SSRN Electron J. 2020. <https://doi.org/10.2139/ssrn.3560392>.
21. Almeida D, Shmarko K, Lomas E. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*. 2021. <https://doi.org/10.1007/s43681-021-00077-w>.