Written evidence submitted by IBM (ADM0017)

IBM welcomes the opportunity to respond to the Science and Technology Committee's inquiry into algorithms in decision making.

1. IBM has been researching, developing and investing in AI technology for more than 50 years. The public became aware of a major advance in 2011, when IBM's Watson won the Jeopardy! exhibition on US television, widely seen at that time to overcome particularly difficult AI challenges, such as natural speech recognition. Since that time, the company has advanced and scaled the Watson platform, and applied it to various industries, including healthcare, finance, commerce, education, security, and the Internet of Things. We are deeply committed to this technology, and believe strongly in its potential to benefit society, as well as transform our personal and professional lives.

2. To this end, we have engaged thousands of scientists and engineers from IBM Research and Development, and partnered with our clients, academics, external experts, and our competitors to explore all topics around AI. We are leveraging our understanding of real world business problems to develop AI systems which address the challenges of a wide range of industry sectors. And we have developed a unique point-of-view, informed by decades of research and commercial application of AI.

3. We expect AI systems to pervasively support the decisions we make in our professional and personal lives in just a few years. In fact, this is already happening in many industries and governments. However, if we are ever to reap the full spectrum of societal and industrial benefits from artificial intelligence, we will first need to trust it.

4. Trust in AI systems will be earned over time, just as in any personal relationship. Put simply, we trust things that behave as we expect them to. But that does not mean that time alone will solve the problem of trust in AI. AI systems must be built from the outset to operate in trust-based partnerships with people.

5. Trust is built upon accountability. As such, the algorithms that underpin AI systems need to be as transparent, or at least as interpretable as possible. In other words, they need to be able to explain their behaviour in terms that humans can understand — from how they interpreted their input to why they recommended a particular output.

6. To do this, we recommend all AI systems should include "explanation-based collateral systems"[1]. The provided explanations should be meaningful to the targeted users. For example, in AI decision support systems whose aim is to help doctors identify the best therapy for a patient, such AI systems need to provide useful explanations to doctors, patients, nurses, relatives, etc.

[1] Explanation based collateral systems provide guidance as to how decisions were made thus providing explainability and assisting when discrimination or bias in the system needs to be addressed see http://www.research.ibm.com/software/IBMResearch/multimedia/AIEthics_Whitepaper.pdf

7. More generally, existing AI systems support many advanced analytical applications for industries like healthcare, financial services and law. In these scenarios, data-centric compliance monitoring and auditing systems can visually explain various decision paths and their associated risks, complete with the reasoning and motivations behind the recommendation. And the parameters for these solutions are defined by existing regulatory requirements specific to that industry.

8. Explanations are definitely needed where laws and regulations require them (such as the GDPR[2]). However, even when regulations do not require it, we believe that they should be provided to achieve the best collaboration environment for humans and AI, and to create the correct level of trust between them. If explanations are not available, the main risk is that such systems will not be trusted and thus will not be used. We believe that trust is a precursor to adoption, and that adoption is the only path to business success and societal benefits.

9. Since IBM believes all AI systems should always include explanation-based collateral systems, we go beyond transparency about data and algorithms. For cognitive systems to fulfill their world-changing potential, it is vital that people have confidence in their recommendations, judgments and uses. Therefore, IBM is committed to make clear when and for what purposes AI is being applied in the cognitive solutions we develop and deploy. Moreover, we will also clarify the major sources of data and expertise that inform the insights of cognitive solutions, as well as the methods used to train those systems and solutions.

10. Another key area of focus is to recognise and minimise bias. Bias could be introduced into an AI system through the training data or the algorithms. The curated data that is used to train the system could have inherent biases either because the data itself is skewed, or because the human curators displayed bias in their choices. The algorithms that process that information could also have biases in the code, introduced by a developer, intentionally or not. The developer community is just starting to grapple with this topic in earnest. But most experts believe that by thoroughly testing these systems, we can detect and mitigate bias before the system is deployed.

11. Managing bias is an element of the larger issue of algorithmic accountability. That is to say, AI systems must be able to explain how and why they arrived at a particular conclusion so that a human can evaluate the system's rationale. Many professions, such as medicine, finance, and law, already require evidence-based audit ability as a normal practice for providing transparency of decision-making and managing liability. In many cases, AI systems may need to explain rationale through a conversational interaction (rather than a report), so that a person can dig into as much detail as necessary.

12. In addition, AI systems can and should have mechanisms to insert a variety of ethical values appropriate to the context, such as the task, the individual, the

[2] EU GDPR regulation, which comes into effect in May 2018, and will be mirrored in UK Data Protection law, calls for the right of explanation in AI systems (Recital 71)

profession, or the culture. This is not as difficult as it sounds. Ethical systems are built around rules, just like computer algorithms. These rules can be inserted during development, deployment, or use.

13. From working closely with international organisations such as the European Commission, the World Economic Forum, and the OECD, we believe that a policy approach to AI should be holistic, covering technology, economic, environmental and social issues. A mature, responsible approach to AI should take into account all aspects we have outlined above – the need to address ethical issues, avoiding discrimination through algorithmic transparency, addressing societal needs and dealing with the skills question as well as workplace transformation.

14. The second insight from dealing with international organisations and governments is that the question of ethics and AI cannot be dealt with by one government alone – there is a role for a supra governmental approach, with international organisations working closely with industry to develop high level approaches or codes of practice. In this area, IBM is a founding partner of the Partnership on AI[3], a multi-stakeholder initiative where both corporate and not-for-profit organisations intend to study and formulate best practices on AI technologies, to advance the public's understanding of AI, and to provide an open platform for discussion and engagement about AI and its influences on people and society.

15. IBM has published a public commitment to our approach to the responsible use of data, included in full below and available at https://www.ibm.com/blogs/policy/dataresponsibility-at-ibm/.

16. Data is the phenomenon of our time. It is the world's new natural resource, growing exponentially not only in quantity but more importantly in form. Every action and interaction, every decision and relationship, every event occurring in any of the world's complex systems, natural and human-made, is now being expressed as data.

17. To extract the profound insight, business value and societal potential in these flows of data, we require artificial intelligence – specifically, AI that can make sense of data from every source and in every form: structured data from transactional systems like e-commerce, financial markets and supply chains; natural language data like social media; data in the form of images and video; and data from Internet of Things sensors.

18. Through the pervasive instrumentation of everything, combined with networks of increasing speed and capacity, the world's activities and processes are becoming real- time. This will increasingly require systems that learn, predict, make recommendations and aid decision-making with confidence. And that will enable the transformation of business and society, the solution of previously intractable challenges, lives that are healthier, opportunities that are more varied, and homes and cities that are safer, fairer and more vibrant.

[3] https://www.partnershiponai.org/

19. This profound shift is compelling enterprises and institutions of all kinds to adopt new technology and business architectures, based on artificial intelligence and cloud; and new business processes, skills and forms of engagement. At IBM, we call this the cognitive enterprise.

20. But to realise this enormous promise and ensure the success of these new platforms, businesses, governments and all of civil society must address significant societal and policy implications. In the rush to harness the potential from data, we must not lose sight of basic expectations that individuals, enterprises and communities rightly have regarding security, trust, privacy, jobs, skills – and, increasingly, the data they own or that is collected from them.

21. In January 2017, IBM Chairman Ginni Rometty issued an initial set of Principles for the Cognitive Era [https://www.ibm.com/blogs/think/2017/01/ibm-cognitive-principles/], describing IBM's commitments regarding the purpose of our cognitive systems; the transparency we will bring to its use; and the commitment we have made to help current and future generations develop the skills required to succeed in this new world.

22. But even before the deployment of AI, we believe that organisations that collect, store, manage or process data have an obligation to handle it responsibly. That belief – embodied in our century-long commitment to trust and responsibility in all relationships – is why the world's largest enterprises trust IBM as a steward of their most valuable data. We take that trust seriously and earn it every day by following these responsible beliefs and practices:

23. **DATA OWNERSHIP & PRIVACY**

A world being reshaped by the phenomenon of data requires clarity around the principles and rules of the road to ensure that the rights of those who own it and use it are protected. We have defined the following key areas of policy to ensure that trust for our clients and communities.

24. **DATA OWNERSHIP**

We at IBM have always believed that our clients' data is their own, and that government data policies should be fair and equitable and prioritise openness.

- Clients are not required to relinquish rights to their data to have the benefits of IBM's Watson solutions and services.
- We believe the unique insights derived from clients' data are their competitive advantage, and we will not share them without their agreement.
- IBM client agreements are transparent. We will not use client data unless they agree to such use and we will limit that use to the specific purposes clearly described in the agreement.
- IBM employs industry-leading security practices to safeguard data.

25. **DATA PRIVACY**

IBM is fully committed to protecting the privacy of our clients' data, which is fundamental in a data-driven society.

- While there is no single approach to privacy, IBM complies with the data privacy laws in all countries and territories in which we operate.
- IBM was an early leader in developing and adopting the European Union (EU) Data Protection Code of Conduct for Cloud Service Providers for several offerings, securing certification under the U.S.-EU Privacy Shield and the APEC Cross-Border Privacy Rules, and will be fully compliant with the EU's General Data Protection Regulation.
- IBM will advocate for strong and innovative means to enhance privacy and data protection, and will continue to invest in privacy-enhancing technologies.
- IBM supports global cooperation to facilitate mutual recognition of privacy regimes to enhance and facilitate cross-border data flows.

DATA FLOWS & ACCESS

26. CROSS-BORDER DATA FLOWS

IBM views the free movement of data across borders as essential to 21st century commerce.

- IBM supports digital trade agreements that enable and facilitate the cross-border flow of data and that limit data localisation requirements.
- We believe clients, not governments, should determine where their data is stored and how it is processed. Mandating that data be kept or processed within national boundaries does not make it safer from hackers or cyber criminals.
- IBM is making significant investments in cloud data centres around the world to give clients the flexibility to decide where to store and process their data. These decisions generally should be driven by client choice rather than government mandate.

27. GOVERNMENT ACCESS TO DATA

IBM has stated in detail our stance on government requests for access to client data.

- IBM has not provided client data to any government agency under any surveillance program involving bulk collection of content or metadata.
- In general, if a government wants access to data held by IBM on behalf of an enterprise client, we would expect that government to deal directly with that client.
- We do not provide access to client data stored outside the lawful jurisdiction of any government requesting such data, unless the request is made through internationally recognised legal channels such as mutual legal assistance treaties (MLATs).
- If we receive a request for enterprise client data that does not follow processes in accordance with local law, we will take appropriate steps to challenge the request through judicial action or other means.
- If we receive a government request for enterprise client data that includes a gag order prohibiting us from notifying that client, we will take appropriate steps to challenge the gag order through judicial action or other means.4

- We will continue to work closely with governments and clients to balance the protection of data with law enforcement's obligation to conduct lawful investigations of criminal activity.
- IBM supports measures to increase the transparency, oversight and appropriate judicial review of government requests for data, including modernised international agreements on legal assistance.

28. DATA SECURITY AND TRUST

As a global leader in enterprise security, IBM has a unique perspective on the rapidly growing threats of an increasingly open marketplace and public sphere. We are devoting our powerful engines of technology innovation to create the tools to protect our clients and global trade – from AI to blockchain. And we are drawing on our global array of trusted relationships to convene business, government, academia and all of civil society to address our collective need, while striking the crucial balance among security, privacy and freedom.

29. ENCRYPTION

IBM opposes any effort to weaken or limit the effectiveness of commercial encryption technologies that are essential to modern business.

- IBM does not put 'backdoors' in its products for any government agency, nor do we provide source code or encryption keys to any government agency for the purpose of accessing client data.
- In response to the global data breach epidemic, IBM will continue to develop new technologies to enhance the protection of our clients' data and transactions, which are the foundation of the worldwide digital economy.
- IBM supports the use of internationally-accepted encryption standards and algorithms, rather than those mandated by individual governments.

30. CYBER SECURITY

IBM employs industry-leading security practices and technologies to safeguard data, and is at the forefront of applying artificial intelligence capabilities to stay one step ahead of emerging digital threats.

- IBM believes in public-private partnerships to raise cybersecurity awareness and tackle current and future threats to data security. The most effective approach involves voluntary, industry best practices and flexible risk management, such as the NIST Cybersecurity Framework.
- IBM also supports voluntary, real-time sharing of actionable cyber threat information between government, business and academia to collaboratively prevent and mitigate attacks.
- We believe that securing the Internet of Things - including all data, communications and processing associated with those systems - can only be achieved if their designs put data security and privacy first.

31. DATA & ARTIFICIAL INTELLIGENCE

From our long history of pioneering AI technology and the work we are doing to help our clients apply it around the world, we have learned that these capabilities – which are better understood as "augmentation" than "artificial" – represent a positive and transformative force for businesses, institutions, governments and individuals. We have also learned that they must be developed in thoughtful and responsible ways.

- The value in AI lies in human augmentation, not replacement. AI systems will not become conscious or sentient beings; rather, they will be integrated into the world's processes, systems and interactions. Artificial intelligence cannot and will not replace human decision-making, judgment, intuition or ethical choices.
- IBM supports transparency and data governance policies that will ensure people understand how an AI system came to a given conclusion or recommendation. Companies must be able to explain what went into their algorithm's recommendations. If they can't, then their systems shouldn't be on the market.
- As society debates the implications of AI systems, IBM does not believe in taxing automation or penalising innovation. Rather, IBM will work with policymakers and clients to prepare the workforce with the skills needed to work effectively in partnership with AI systems.

32. DATA SKILLS AND "NEW COLLAR" JOBS

IBM is leading efforts to ensure workers worldwide are prepared for technological and business shifts that are changing the way work gets done, and that are driving productivity, economic growth and job creation.

- IBM is working with policymakers to modernise education systems to emphasise in-demand skills rather than specific academic degrees. Preparing more students and workers for careers in well-paying new collar jobs will help ensure that more workers have an opportunity to benefit from technology-driven economic growth.
- IBM encourages governments to:
    - Better align education with in-demand skills and competencies;
    - Support business investment in retraining employees; and
    - Encourage individuals to invest in skills for career advancement.

31. CONCLUSION

The data economy is evolving rapidly, and new technologies are changing the way we live and work – and so these views on data responsibility will continue to evolve. By offering this comprehensive view of our principles and practices, we aim to spark dialogue across all sectors of society. And we will continue to earn the trust of our clients and the communities in which we work in moving, storing, managing, analysing and learning from the data that powers the modern world, and the new

capabilities – in both technology and business – that offer so much promise for turning it into economic value and societal progress.

October 2017