THE
ROYAL
SOCIETY

The Royal Society's submission for the United Nations Global Digital Compact

Response to the United Nations Secretary-General's Envoy on Technology's consultation on core principles and key commitments, April 2023.

Background

This is the Royal Society's submission to the consultation undertaken by the United Nations (UN) Secretary-General's Envoy on Technology, to be considered for the development of the Global Digital Compact. This response was submitted in April 2023 and the Global Digital Compact is expected to be agreed in September 2024 at the Summit of the Future.

The Global Digital Compact aims to 'outline principles for an open, free and secure digital future for all'. It was proposed in the UN Secretary General's September 2021 report, Our Common Agenda[1]. The consultation sought input on several thematic areas and requested views on a) core principles that all governments, companies, civil society organisations and others should adhere to and b) key commitments, pledges, or actions that should be taken by different stakeholders.

Drawing upon various Royal Society reports related to data and digital technologies, this submission provides input on the thematic areas of protect data; accountability for discrimination and misleading content; regulation of Artificial Intelligence (AI); and digital commons as a global public good.

Royal Society secretariat
Areeq Chowdhury, Head of Policy, Data
Eva Blum-Dumontet, Senior Policy Adviser, Data
Dr June Brawner, Senior Policy Adviser, Data
Denisse Albornoz, Policy Adviser, Data
Charise Johnson, Policy Adviser, Data
Nicole Mwananshiku, Project Coordinator, Data

The Royal Society

The Royal Society is a self-governing Fellowship of many of the world's most distinguished scientists drawn from all areas of science, engineering, and medicine. The Society's fundamental purpose, as it has been since its foundation in 1660, is to recognise, promote, and support excellence in science and to encourage the development and use of science for the benefit of humanity.

The Society's strategic priorities emphasise its commitment to the highest quality science, to curiosity-driven research, and to the development and use of science for the benefit of society. These priorities are:

- The Fellowship, Foreign Membership and beyond
- Influencing
- Research system and culture
- Science and society
- Corporate and governance.

[1] United Nations. 2021. Our Common Agenda report of the Secretary-General. See: https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf (accessed 23 November 2022)

THEMATIC AREA: PROTECT DATA

CORE PRINCIPLE:

Responsible data governance is foundational to human flourishing.

Data on human behaviour and the natural world can enable significant benefits through research and development. Data-driven insights are helping solve key societal challenges and are supporting the achievement of the UN Sustainable Development Goals. Data use is foundational to human flourishing, and the risks of using data must be addressed responsibly and effectively[2]. Mechanisms for data governance should protect people's rights, be informed by good practice, be accountable and enhance existing democratic governance.

KEY COMMITMENTS

1. **Preserve the robustness of encryption for sensitive data sharing, including end-to-end encryption, and promote its widespread use.**
   The competent operation of trustworthy digital systems relies on fundamental security technologies, including encryption[3]. These technologies provide the technical assurance that enables people to entrust their personal data to digital systems. If strong encryption is properly implemented, deciphering an encrypted message without the key is extremely difficult, if not impossible.

   Encryption is a foundational security technology that is needed to build trust, improve security standards and fully realise the benefits of digital systems. Governments across the world should commit to preserving the robustness of encryption, including end-to-end encryption, and promoting its widespread use.

2. **Establish protocols and standards for privacy enhancing technologies (PETs).**
   Beyond data security applications, PETs have a role to play in facilitating data use across national borders. In this way, PETs have significant potential to improve international digital cooperation[4].

   Technical standards will support the interoperability of PETs for data collaboration. Codes of conduct for the responsible use of PETs will be critical for 'social interoperability' and acceptance in partnerships across borders or sectors.

   PETs will help put more data to use, but they will not replace the need for data minimisation, data curation and consideration of whether a particular use is ethical[5]. Therefore, PETs should be considered in the context of potential downstream harms, appropriate business models and auditing processes for data-enabled businesses and organisations.

3. **Incentivise the development of PETs for enabling data-driven solutions to grand challenges.**
   The UN should continue to build on initiatives such as the UN PET Lab. For example, test environments could be used to demonstrate the security, privacy, and utility potentials of specific PETs or configurations of PETs. An international PETs sandbox would allow national regulators to collaborate in evaluating PETs solutions for cross-border data use according to common data governance principles.

   Through these initiatives, researchers, regulators and enforcement authorities should investigate the wider social and economic implications of PETs. These could include how PETs might be used in novel harms or how PETs might affect competition in digitised markets.

[2] The Royal Society. 2017 Data management and use: Governance in the 21st century. See: https://royalsociety.org/topics-policy/projects/data-governance/ (accessed 27 April 2023).

[3] The Royal Society. 2016 Progress and research in cybersecurity: Supporting a resilient and trustworthy system for the UK. See: https://royalsociety.org/topics-policy/projects/cybersecurity-research/ (accessed 27 April 2023).

[4] The Royal Society. 2019 Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis. See: https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/ (accessed 27 April 2023).

[5] The Royal Society. 2023 From privacy to partnership: The role of privacy enhancing technologies in data governance and collaborative analysis. See: https://royalsociety.org/topics-policy/projects/privacy-enhancing-technologies/ (accessed 27 April 2023).

THEMATIC AREA: ACCOUNTABILITY CRITERIA FOR DISCRIMINATION AND MISLEADING CONTENT

CORE PRINCIPLE:

Society benefits from honest and open discussions on the veracity of scientific claims.

Science stands on the edge of error. It is a process of dealing with uncertainties, testing received wisdom, and continually revising our understanding of the world. The core ability of the scientific method to correct itself is a strength, rather than a weakness. This ability requires a safe, healthy and plural online information environment that allows robust and open scientific debate[6]. Although content removal can be an effective policy to mitigate the harms of illegal and discriminatory content (such as hate speech), there is little evidence to support the effectiveness of this approach for scientific misinformation. Deliberation and debate are important aspects of the scientific process and should be protected.

KEY COMMITMENTS

1. **Governments and social media platforms should not rely on content removal as a solution to scientific misinformation.**
   Identifying scientific misinformation is highly resource intensive and not always immediately possible to achieve, as some scientific topics lack consensus or a trusted authority. Furthermore, misinformation sometimes comes from citizens who, in good faith, believe in the content they are spreading, even if it may be harmful to others. They may regard direct action against their expression as censorship. Allowing content to remain on platforms with mitigations to manage its impact (such as reduced amplification) may be a more effective approach to prioritise.

2. **Social media platforms should establish ways to allow independent researchers to access data in a privacy-compliant and secure manner.**
   Understanding the nature of information production and consumption is critical to ensuring society is prepared for future challenges that arise from the online information environment. Analysis of the rich datasets held by social media platforms can help decision-makers understand the extent of harmful online content, how influential it is and who is producing it. It should also help enable transparent, independent assessments of the effectiveness of counter-misinformation interventions and support the development of best practice.

   This requires establishing privacy compliant and secure mechanisms to allow trusted third parties access to data, such as promoting the use of trusted research environments or other PETs for these purposes.

3. **Invest in lifelong information literacy initiatives.**
   Ensuring that populations can safely navigate the online information environment will require significant investment in information literacy, ensuring that people can effectively evaluate online content. In practice, this could include education on how to assess URLs, how to reverse image search and how to identify AI-generated content.

   This education should not be limited to those in schools, colleges, and universities, but extended to people of all ages. As the nature of the online information environment is likely to continue evolving over time with new platforms, technologies, actors and techniques, it is important to consider information literacy as a life skill, supplemented with lifelong learning. These initiatives should be carefully tailored and designed to support people from a broad range of demographics.

[6] The Royal Society. 2022 The online information environment: Understanding how the internet shapes people's engagement with scientific information. See: https://royalsociety.org/topics-policy/projects/online-information-environment/ (accessed 27 April 2023).

THEMATIC AREA: PROMOTE REGULATION OF ARTIFICIAL INTELLIGENCE

CORE PRINCIPLE:

Strong data protection regulations are essential for public trust and the safe and ethical development of AI.

AI applications are widespread and increasingly prevalent. For example, machine learning algorithms are just computer programs, and the range and extent of their use is extremely broad and diverse[7]. They are being applied across all industries and sectors, presenting significant challenges for generally applicable regulations for AI. As public concerns around the use of AI often relate to questions of data collection, privacy and misuse, there is a need for strong data protection regulations[8]. These provide a mechanism for accountability and help drive up standards, ensuring that society can have confidence in how AI is developed and applied.

KEY COMMITMENTS

1. **Adopt and promote strong data protection regulations.**
   There are many issues surrounding the use of data, including those concerning the sources of data and the purposes for which data is used. For this, strong data protection regulations that can keep pace with the challenge of data governance in the 21st century are necessary to address the novel questions arising from the development of AI applications. These should be underpinned by the need to protect individual and collective rights and interests, and ensure that trade-offs affected by data management and use are made transparently, accountably and inclusively[9].

2. **Develop scenario-specific data protection guidance for AI development.**
   Robust data protection regulations should be complemented with scenario-specific guidance from data protection authorities to ensure that the issues arising related to AI development can be more easily addressed, and to prevent unnecessary overcompliance[10].

3. **Enable an open data environment.**
   To create a data environment that supports the development of machine learning, governments should consider creating a new wave of open data for machine learning to enhance the availability and usability of public sector data. In areas where there are datasets unsuitable for general release, further progress in supporting access to public sector data could be driven by the adoption of PETs as well as rights-preserving agreements that make data available to specific users under clear and binding legal constraints to safeguard their use.

[7] The Royal Society. 2017 Machine learning: The power and promise of computers that learn by example. See: https://royalsociety.org/topics-policy/projects/machine-learning/ (accessed 27 April 2023).

[8] The Royal Society. 2023 Creating resilient and trusted data systems: The public perspective and recommendations for action. See: https://royalsociety.org/topics-policy/projects/data-for-emergencies/ (accessed 27 April 2023).

[9] The Royal Society. 2017 Data management and use: Governance in the 21st century. See: https://royalsociety.org/topics-policy/projects/data-governance/ (accessed 27 April 2023).

[10] The Royal Society. 2023 Post-Brexit divergence from GDPR: Implications for data access and scientific research in the UK. See: https://royalsociety.org/topics-policy/projects/data-protection-legislation/ (accessed 27 April 2023).

THEMATIC AREA: DIGITAL COMMONS AS A GLOBAL PUBLIC GOOD

CORE PRINCIPLE:

Data and digital technologies that can help to achieve net zero carbon emissions should be made accessible and, wherever possible, open.

From the design of energy efficient buildings to the digital twinning of wind farms, data-driven systems can contribute to achieving net zero carbon emissions[11].

For the net zero transition to be data-led, relevant data should follow the FAIR principles (it must be Findable, Accessible, Interoperable, and Reusable). Where data cannot be made fully open, robust frameworks should be in place (such as data access agreements). Alternatively, new data institutions such as data trusts, data commons, data collaboratives or data clubs may be appropriate. Open approaches to technology development more broadly will promote greater transparency, participation and trust in the digital infrastructure for net zero.

KEY COMMITMENTS

1. **The technology sector should be incentivised to lead by example, allowing for greater monitoring of its energy consumption and carbon emissions.**
The increasing energy demands and emissions of the tech sector will need to be understood and managed, particularly if digital technologies are to be widely deployed for monitoring and enabling net zero. The tech sector's carbon footprint can be reduced through multiple approaches, including the further uptake of renewables and the scrutiny of digital technologies' energy proportionality. This will require greater data availability, for example, through data commons or other appropriate arrangements.

   Governments should incentivise tech companies to publicly share the energy consumption of their digital systems and products. This should entail embodied and use phase emissions, in particular from data centres.

2. **Encourage open approaches to technology development for net zero.**
Barriers to the creation and deployment of new applications for net zero can be reduced through the widespread, low-cost availability of foundational intellectual property. Cooperative collaborations and broad public participation can also contribute to technology development.

   The adoption of open approaches would enable the participation of a more diverse community of developers, as well as greater scrutiny of data-driven systems.

   Intergovernmental organisations should continue using their coalition-building power to fill gaps of local expertise. For example, the UN Global Pulse labs facilitate access to expertise to develop local applications of data and AI for SDGs.

3. **Build capacity in existing data infrastructures for net zero.**
Expanding the role of existing data infrastructures could be more time- and cost-effective than creating new datasets. Existing high-quality datasets with applications for net zero can be repurposed and made accessible to enable more effective emissions monitoring. PETs can play a role in utilising data for net zero, such as smart meter data, or wherever data is personal or otherwise sensitive.

   To enable data access and sharing, intergovernmental bodies should encourage collaboration and coordinate agreements amongst member states for sharing data at national and international levels. This should entail, as a priority, capacity building in lower-income countries with less advanced data infrastructures to support equitable application of digital technologies for net zero.

[11] The Royal Society. 2020 Digital technology and the planet: Harnessing computing to achieve net zero. See: https://royalsociety.org/topics-policy/projects/digital-technology-and-the-planet/ (accessed 27 April 2023).