Written evidence submitted by Microsoft (TFP0017)

About Microsoft

Microsoft has been present in the UK for over 30 years, and today we employ over 4,500 people and work with over 20,000 partners across the UK helping them to digitally transform, exploit the opportunities presented by our digital tools and gain data insights that help them serve their customers. Our mission is to empower every person and organisation on the planet to achieve more, and we measure our success by the success of our customers and partners.

We are proud to work with customers across the UK government to find new ways for technology to drive opportunities for all and to support the UK's policy ambitions, including in foreign and security policy.

We have partners all over the UK, and recently announced a partnership with UK cyber security company Darktrace, to provide our mutual customers with enterprise-scale, self-learning AI that detects and autonomously responds to cyber-threats. We also recently announced our partnership with UK company Improbable, which will transform defence capabilities across operational planning, policy design, collective training, national resilience and defence experimentation. These examples of collaboration with UK companies are at the heart of our mission to support democracies to defend themselves and create and deploy the best technologies.

Our response focuses on three out of the eight questions: 2, 4 and 5.

1. Question 2 - How can the FCDO engage with private technology companies to influence and promote the responsible development and use of data and new technologies?

1.1. In a new age of systemic state competition, it is vital that democratic Governments build a coalition of partners from public and private sectors, to commit to responsible use of technologies. As Microsoft President Brad Smith has said, the past 12 months has seen the rapid evolution and increased sophistication of cybersecurity threats, and we face a moment of reckoning, requiring to look with clear eyes at the threats we face and accelerate and deepen our collective commitment to work collaboratively.

1.2. In order for the FCDO to collaborate most effectively with the private sector, a coherent and strategic approach is required, that is grounded in a robust assessment of where digital technology is going and the nature of global competition in technology markets. The Integrated Review (IR) provides a helpful starting point, and is right to highlight the centrality of science and technology to the UK's future global standing. As the IR recognises, the UK must move more quickly to advance broad-

based technology innovation and pursue new approaches to use, secure, and adapt commercial technological advances. This will require an even closer partnership between the government and the tech sector. This strategic partnership should include:

1.2.1. **Promoting trust and defending democracy.** FCDO is both an important customer for technology companies, and a much broader influencer in the UK and international markets through its influence and soft power. Therefore, its commitment to values of trust, and working with and through private companies on this basis, can have a powerful positive impact. Establishing and maintaining high trust is fundamental to success in leveraging data across all industries. Upholding the highest standards of compliance, quality and ethical use is the cornerstone of building this trust. FCDO can influence this both as a data user itself, and by promoting the highest ethical standards in the creation, storage, sharing, handling and lifecycle management of data. Advocacy of ethical usage, innovative use of data based on real world examples and championing standards and working practices through exemplar projects will be important areas for impact. More broadly, the public language used by government and particularly the FCDO is important: a new lexicon for diplomacy will need to emerge so that the UK is able to find its voice in the promotion of responsible use of data, AI and technology globally.

1.2.2. **Developing a UK industrial base that can provide the capabilities and skills for the future.** FCDO can have an important role in supporting UK industry to innovate and embrace future technologies. We welcome a recent Cabinet Office review into the UK's Science and Technology strategy in this regard. This approach needs to take a UK-wide view, and to support delivery on the ambition of making the UK a global science leader. Skills will be a core component of success, and Microsoft has been both campaigning and contributing to this for many years. As we stated in our submission to the Government's National Data Strategy consultation, it is important to offer multiple access routes to these roles to ensure diversity of background in the industry and to drive outcomes that reflect the communities being served. The Integrated Review rightly recognised the importance of building a stronger UK skills base given the Government's ambition to have secured its status as a Science and Tech Superpower by 2030. The FCDO can be the global spearhead of this critical agenda. It must draw on talent from all over the country, and in turn, find opportunities globally and link them back to the UK in a virtuous cycle.

1.2.3. **Driving integration and interoperability.** On the flipside of the UK leading in certain technologies, recognising gaps in UK capabilities should not necessarily be seen as failure, but can encourage the identification of new commercial and state partners with whom the UK can cooperate in the next decade. A new model of thinking about competition and the relative advantage for the UK will

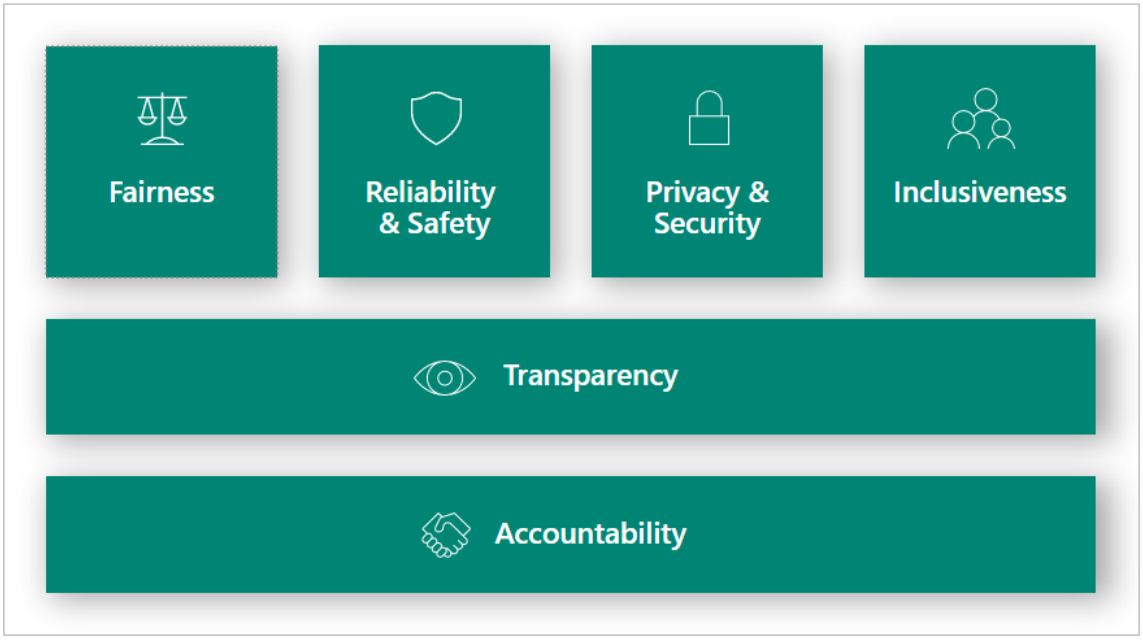
be important. Fostering greater inter-operability between the UK and allies—new and old—will be important here. The benefits of interoperability with allies in NATO and the Indo-Pacific include economies of scale and ensuring that R&D and the best technologies can benefit likeminded democratic nations. In addition, using the same technology in practice can foster more effective working between allies and coalition building, because equipment, knowledge and skills are interchangeable.

1.2.4. **Encouraging sustainable and responsible development and use of technology**. Climate change poses a challenge not just to the UK tech sector, but the global economy. Sustainability therefore needs to be at the heart of our sector's future. Data insights, for example, should be at the heart of helping the government to deliver policy priorities such as the drive to Net Zero. The FCDO have a critical role, and should work in coalition with the private sector globally to drive forward a common agenda of creating a sustainable planet for all. In January 2020, Microsoft CEO Satya Nadella announced that the company would be carbon negative by 2030. These announcements are part of our wider drive to be a sustainable company and help tackle the global climate crisis. Alongside our carbon negative announcement, we launched a $1 billion Climate Innovation Fund that will invest in emerging technologies that will help to reduce the impact of human activity on the environment.

1.2.5. **Cooperation with the private sector in the context of NATO** - NATO can play a key role by facilitating policy collaboration with key technology industry actors. Notwithstanding existing NATO-industry engagement formats, we believe there is a clear benefit to creating new avenues for a strategic engagement with key technology providers. NATO may consider the establishment of a format that will bring together the NAC and executives of key technology companies. Such a format would feed well into the NATO 2030 initiative as it would allow for including new perspectives into the strategic and political efforts at NATO. Moreover, it may be worth considering the creation of a policy consultation mechanism between NATO IS and tech industry actors. NATO could consider establishing a process that allows technology players within the Alliance to contribute to policy issues that relate to technology, innovation, and digital affairs. Discussion and co-operation among all relevant stakeholders are a key prerequisite for effectively dealing with threats emanating from cyberspace today and tomorrow. Many industry actors would be interested in engaging in regular and formalized engagements as it helps to understand the objectives of the key decisions and changes, and provides an opportunity to knowledge-share impacts.

1.3. As part of our own drive to promote the responsible development and use of data and new technologies, Microsoft has set up three interlinked groups. First, the Office of Responsible AI which is charged with developing company-wide

rules for enacting responsible AI. It also reviews sensitive use cases to hope ensure that Microsoft's AI principles are upheld in our development and deployment work. This office also shares its experience to help shape new laws, norms and standards. Secondly, the AI Ethics and Effects in Engineering and Research Committee—the AETHER Committee—cuts across multiple groups and disciplines within the company, and includes experts from outside the company. It conducts research and makes recommendations on responsible AI issues, technologies, processes, and best practices. Thirdly, our Responsible AI Strategy in Engineering group works to enable our engineering teams to implement responsible AI processes through systems and tools.



Microsoft's AI Principles

2. **Question 4 - How can the FCDO use its alliances to shape the development of, and promote compliance with international rules and regulations relating to new and emerging technologies? Is the UK taking sufficient advantage of the G7 Presidency to achieve this?**

2.1. In an increasingly polarised, complicated, and unstable world, the UK has an opportunity act as a leader of co-operation amongst allied nations - this includes working together to ensure digital security and resilience against hostile actors. The G7 Presidency provides a particular opportunity, although this agenda will need to be much longer term.

2.2. The UK can lead on the responsible development of international standards, including cyber standards, working with technological partners to keep pace with change, while also increasing its own capabilities to meet the rising challenges from cyber warfare. The increasing use of "grey zone" offensive cyber tactics by nation states means that it is important that likeminded governments and the private sector

work together on this agenda. While the world has important international norms and laws to address nation-state attacks, we continue to believe it is important to fill in gaps and continue to develop clear and binding legal obligations for cyberspace. The FCDO can use its alliances to be a champion of this important agenda.

2.3. Microsoft supports the UK using alliances with likeminded parties to promote the international rule-based system. Through broader international organisations, such as Five Eyes and NATO, the UK must continue to be at the forefront of this effort, challenging state actors that wish to export authoritarianism and corruption around the world. International rules should include stronger protections of democratic and electoral processes, as reflected in the principles of the Paris Call for Trust and Security in Cyberspace, which now has more than 1,200 signatories – the largest multi-stakeholder group ever assembled in support of an international cybersecurity-focused agreement.

2.4. Looking ahead, the FCDO should look for opportunities to work with partners to pursue greater international agreement on the prohibition of malicious uses of digital technology. Attacks over the last 5 years have grown in frequency and sophistication, highlighting why the global community must do more to find international consensus. Both governments and businesses need to do everything possible to share data about the threats and work together to combat them.

2.5. In addition, governments should take new and concerted steps to thwart the rise of private sector offensive actors (PSOAs). These companies in effect have created a new ecosystem to support offensive nation-state attacks. The sooner governments take action to put this ecosystem out of business, the better.

2.6. As a leader in G7 and NATO, the UK is well placed to lead an alliance of likeminded democracies, to establish a new rules-based order for emerging technologies. This extends beyond G7 countries. Japan, Korea, India and Australia are strategically important partners in facing threats from China and Russia. The UK was right to broaden the scope of countries attending recent G7 meetings, these countries will be pivotal in building a global collation, including to strengthen international rules around new technologies. The UK has experience in producing independent regulators, Ofcom being a good example, meaning it can lend this expertise when setting new international organisations to regulate emerging technologies.

2.7. For a number of reasons, the UK is also well-placed to have a prominent voice globally on the importance of ethics in technology through multilateral forums:

2.7.1. The UK's public cloud-first approach and no regulatory blockers on the development, adoption or deployment of Artificial Intelligence solutions. This approach is supported by independent sectoral regulators and the work of the UK Data Protection Authority, the ICO, and the Centre for Data Ethics and

Innovation (CDEI). The approach takes an ethics centric approach to the deployment of new technologies, that recognises that they will only be of use if the public has confidence in them and a feeling of agency over issues such as bias and discrimination. This is backed up by the ability of individuals to challenge the deployment of solutions, such as the use of facial recognition by law enforcement – as indeed happened when South Wales Police were challenged.

2.7.2. As a leader in independent economic regulation and advice to government the UK is well placed to engage and lead the public policy debate at the OECD and in the international standards setting regime. This continued engagement and approach would see the elevation of the ethical conversation to a global level and support those proponents of a rules based multilateral approach to technology.

2.7.3. The UK is a leader in multistakeholder engagement and should thus maintain a strong relationship with the EU on cyber and emerging technology issues, The multistakeholder forum for discussions established among governments, private sector and civil society, the European Cyber Agora, provides a platform to discuss a unified European value-based approach to global cyber issues.

2.8. Finally, we need stronger steps to hold nation-states accountable for cyberattacks. Governments and private companies have taken clear steps in recent years to hold nation-states publicly accountable for cyberattacks. We need to build on this course and continue to press forward with it, with Governments ensuring that there are greater real-world consequences for these attacks to promote stability and discourage conflict.

3. Question 5 - Should the Government's approach to meeting the challenges of technology nationalism and digital fragmentation be based on self-sufficiency, joining with allies or like-minded nations or supporting a coherent global framework?

3.1. Self-sufficiency, joining with allies and like-minded nations and supporting a coherent global approach all have their place. The Government's real challenge is to make sound decisions on where each is most appropriate to further the UK's priorities and lead among liberal democratic countries looking to use technology as a force for good.

3.2. The issue of data localisation is a timely aspect of this, and all countries need to strike a balance between desire for strengthening self-determination and competitiveness in the digital space, while also promoting open, modern, and trustworthy digital infrastructure that allows businesses and citizens to benefit from the value of their data. We believe that as countries seek to strike this balance, it is

crucial to avoid fragmentation, protectionism or hurdles for SMEs. The UK is well placed to play a leading role on these important issues.

3.3. At Microsoft, we want to play an active role in contributing to Europe's global competitiveness with technology that is built with respect for European values and fundamental rights and meets the highest standards of privacy, security, transparency, and sustainability.

3.4. In the Integrated Review and the subsequent Command Paper, the UK Government emphasised the importance of working with allies and partners in an increasingly fragmented world. Microsoft welcomes the renewed focus on the question of where it is necessary for the UK to build sovereign capabilities, and where it is more appropriate to work closely with partners to develop shared capabilities. International threats posed by rogue cyber state actors and independent criminal actors aligned to rogue states, affect all like-minded liberal democracies. At the same time, the rapid emergence of technological solutions or weapons does not respect boundaries. There is therefore a critical opportunity to work together with key partners in order to protect and diversify technology supply chains, and outpace adversaries in the race for developing the technologies of the future.

3.5. We see providing our best technology to support democratic governments as a logical and necessary step in our commitment to defending democratic values. As our President Brad Smith recently said, Microsoft believes that "there is no value that is more fundamental and timeless [...] than our commitment to democracy". The increasing frequency of cyber-attacks from hostile states to critical national infrastructure, and the illiberal use of emerging technologies to transgress human rights, demonstrate that this is a pressing issue.

3.6. The UK should therefore join forces with like-minded partners to defend democracy and secure the safe use of future technologies. More practically, maintaining and growing alliances for these ends will require interoperability of technologies. The Queen Elizabeth Carrier preparing for its maiden voyage with 250 of the 1600 crew members of the US Marine Corps, was a strong symbol of this cooperation. As technology increasingly becomes a feature of all of the domains of warfare, a level of technological interoperability with allies will be crucial.

3.7. Microsoft also sees the opportunity for UK industry, through the creation of interoperable technologies that can be exported to international partners. An example of this is the partnership between Microsoft Philanthropies and FCDO around Common Data Models and Standards to enable the seamless sharing of data across global aid agencies. Innovation in this way can also support the Government's agenda to build back better.

May 2021