B7 Digital Statement

Principles and recommendations for G7 Digital Ministers

April 2021

Contents

Chapters

Introduction

Never has it been more important that the G7 shows global digital leadership.

After decades of growing economies, digital technologies have this past year helped preserve them, acting as a bedrock of resilience during the pandemic.

Now is the moment where digital development will be increasingly transformative.

But this could take different forms. In our view, the best and fairest model of sustainable growth requires:

- Resilient network infrastructure through a diverse supply chain

- Free data flows, supported by data protection standards the public trust ('data free flow with trust')

- The strongest safeguards to keep public institutions, citizens and businesses cybersecure

- A stable regulatory environment which promotes innovation, investment and competition, while supporting democratic values

- Widespread alignment and adoption of tools to digitise trade and make it frictionless.

None of these is automatic or guaranteed. All will require government action and international co-operation. This B7 paper puts forward recommendations on each.

The task at hand is not one for governments alone. Industry stands ready to make its own contribution to an inclusive global recovery – investing, innovating and helping solve societal challenges. As the crisis has shown, so much can be achieved with strong partnership between government and industry.

With G7 leadership and business dynamism, we believe these proposals can support a common endeavour to build back better.

Resilient network infrastructure through a diverse supply chain

Principles:

- Digital infrastructure is the backbone of modern economies, supporting productivity and prosperity. Widespread industrial adoption of innovative technologies, such as the Internet of Things (IoT) and 5G private networks, rely on a robust and secure digital infrastructure. We recognise that open architecture of telecoms systems could contribute to diversification.

- Supplier telecoms diversification is vital for enhancing resilience, delivering security, promoting competition, and supporting investment in innovation. A diverse supply chain for telecoms infrastructure will provide significant opportunities to grow national supply bases, deliver economic growth, and create high value jobs.

- Technological advancements are enabling increased diversification in the base of telecoms equipment suppliers, creating opportunities for innovation and new entrants in the market by reducing barrier to entry. Supporting new entrants to the market will be facilitated in part by international agreement on regulation and standards to ensure systems are interoperable and secure by design.

Policy Recommendations:

1. The G7 should construct a formal mechanism to advance telecoms diversification and identify opportunities for policy collaboration, including on RD&I, to accelerate to market opportunities, such as virtualised networks.

2. The G7 should support continued cooperation on the international promotion of industry-led technical, consensus-based standards and advance technology-neutral approaches to encourage innovation, interoperability, and diversification in telecoms systems. International cooperation to create global standards is fundamental to realising economies of scale.

3. G7 governments in close collaboration with industry should stimulate demand for connectivity technologies through targeted support for business adoption and experimentation, such as industrial 5G applications. Promotion of demand is essential for vibrant markets and this will help enable a competitive ecosystem for new and existing suppliers.

4. G7 governments in the deployment of next generation telecommunications products, services, and processes should carefully consider alignment with the recommendations of the "[The Prague Proposals](#)".

Free data flows, supported by data protection standards the public trust ('data free flow with trust')

Principles:

- Cross-border data flows are indispensable to modern economies and supply chains. The free flow of data supports the development and functioning of the products and services we all rely on, by underpinning trade, RD&I (research, development, and innovation) and business operations across sectors.

- The significance of cross-border data flows for international innovation and collaborative research has been demonstrated as countries combat the Covid-19 pandemic – for example, as seen in the rapid sharing of the genetic sequence of the virus, which has supported the development of treatments.

- For societies and the economy to benefit fully from data, including both personal and non-personal data, trust and innovation must go hand in hand. Industry is committed to building public confidence in using data while unlocking its potential for RD&I, enhancing customer products and experience, and improving efficiency.

- Businesses are concerned about the rise of unjustified data localisation requirements, forced access to source code as a market access requirement, and other industrial policy interventions that are unjustly restrictive for data flows.

- In addition, fast-moving political and legal landscapes can add risk and complexity for businesses when it comes to international data transfers, for example as seen with the consequences following the European Court of Justice's recent Schrems II ruling.

- International collaboration between governments and regulators is vital to support a robust, trustworthy, and consistent approach to cross-border data transfers that limits fragmentation, challenges unjustified barriers, and reduces uncertainty for firms.

Policy Recommendations:

5. The B7 endorses the G7 goal to develop roadmaps on areas for international cooperation to support data transfers across G7 economies, across issues such as unjustified data localisation, regulatory cooperation, access to government data, and approaches to voluntary data sharing. The G7 should also oppose measures that require the transfer of or access to source code as a market access requirement.

6. There is a pressing need for regulatory cooperation and dialogue leading to greater consistency and enforceability around the application of rules and mechanisms for data transfers, building trust between nations. The G7 must lead by example by working together and with other nations to reemphasise that 'equivalent' standards do not necessarily translate as 'identical' standards on personal data protection. Policymakers, data protection authorities, and businesses must work towards pragmatic and reliable ways to enable flows of personal information while maintaining high privacy standards and agree the necessary frameworks to enable innovation and business growth.

7. The G7 should support regulatory and institutional data protection capacity-building in developing countries. This could build citizen trust and would also enhance understanding of different international approaches to privacy, facilitating improvements in international transfer mechanisms and support cross-border data flows.

8. The G7 Trade Ministers should seek substantial progress and agreement on the WTO e-commerce negotiations, advancing a 'high standard' principles-based outcome that promotes cross-border data flows.

9. The G7 should consider the thinking emerging from the OECD's research on key issues impacting cross-border data flows, for example working jointly to develop international norms in this space. The policy nexus between data, national security considerations, and government access are growing in complexity and it benefits nobody for industry to be caught in the middle.

The strongest safeguards to keep public institutions, citizens, and businesses cybersecure

Principles:

- The combined effort of G7 businesses and governments on cybersecurity is a fundamental enabler of future digital prosperity, wellbeing, and resilience. Rapid technology adoption and increased hybrid working among G7 countries during the pandemic have expanded cybersecurity risks, as well as the opportunities for digitally-driven growth if those risks are effectively mitigated.

- Effective global cybersecurity cooperation and enforcement while protecting human rights and fundamental common values of the G7 are essential for unlocking digital trade with developing countries, which will stimulate domestic growth and support global trade flows.

- The B7 recognises the applicability of international law online as well as offline which is essential to an open, secure, peaceful, and accessible internet. In particular, the most recent consensus adoption of the [UN Open Ended Working Group report](#).

- The 2018 [Paris Call for Trust and Security in Cyberspace](#) marked an important milestone in reaching greater unity within the international community around a set of principles to ensure peace and security in the digital space. It is essential that the G7 renew its emphasis on formal cooperation and information sharing to establish universal safety and security in cyberspace.

Policy Recommendations:

10. The B7 supports greater G7 government coordination on attribution and accountability of state conduct in cyberspace which violates international law, norms, rules, and principles of responsible behaviour by states. All legal options that exist to deter states engaged in supporting, enabling, tolerating, or neglecting the prevention of cyberattacks should be considered, including effective and proportionate ex-ante policy and diplomatic action where required to apply pressure on non-cooperative states.

11. G7 governments should lead efforts by the UN [Group of Governmental Experts](#) to strengthen the rules of the road for state conduct in cyberspace.

12. In line with the recommendations of the B7-France 2019, G7 should develop an international platform on cyber risks to allow businesses and governments to share data about cyber incidents all around the world to improve global knowledge, stimulate common actions, and help prevent attacks. This would support collective resilience and could be under the leadership of Interpol in coordination with other relevant entities.

13. G7 countries should review best practice and new methods of bilateral and multilateral cooperation, capacity building, confidence building, and voluntary information exchange on cybersecurity via trade deals, Mutual Legal Assistance Treaties, and RD&I collaborations.

14. G7 countries should look to enhance collaboration with the private sector on cybersecurity, recognising the agility of industry to respond to the rapidly changing threat landscape. The B7 supports leveraging industry expertise in the development of secure by design standards and cyber technology assurance standards.

15. G7 countries should continue to invest in technical support and awareness raising measures for business, particularly SMEs. The G7 should focus on improving basic cyber hygiene and skills across society to enhance overall resilience. Additionally, the promotion of skills for the cybersecurity profession to ensure a wider and more diverse pipeline of new and retrained talent is crucial.

A stable regulatory environment which promotes innovation, investment, and competition, while supporting democratic values
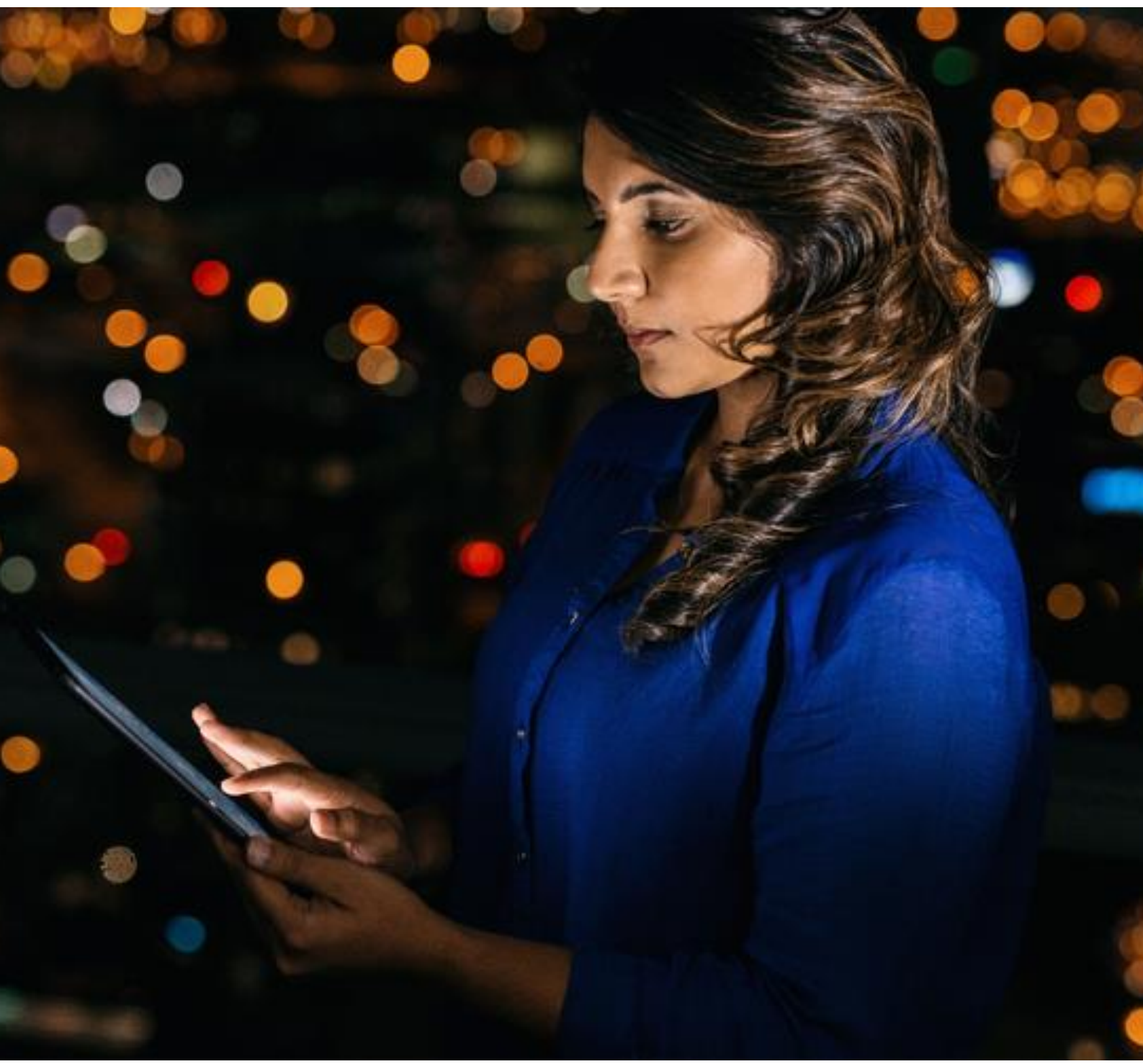
Principles:

- It is important that countries across the G7 look to promote the ethical and responsible adoption of emerging technologies, via measures to address online harms and support democratic values including freedom of speech. This should be done hand in hand with efforts to work beyond the G7, ensuring robust regulatory approaches and enforcement against illegal goods and content online.

- A stable regulatory environment which promotes investment, innovation, and competition in digital markets is essential to unlock the full potential of the digital economy, stimulate economic growth, and support long-term business investment.

- Due to the global nature of the digital economy, cooperation at an international level between regulators and governments is critical. As new digital regulatory models are developed, there is a pressing need for greater dialogue and collaboration with industry and amongst countries.

Policy Recommendations

16. The G7 should establish greater cooperation on next-generation regulatory frameworks governing emerging technologies like AI and fintech, illegal goods and content, and digital competition issues. Governments should work closely with industry and civil society to develop proportionate, effective and trusted policy, recognising the role of existing rules in governing digital technologies and looking to identify and discuss gaps, areas of divergence, and pinch points.

17. To this end, the B7 welcomes the UK government's proposal to establish and host a Future Tech Forum to bring together governments, industry, academia, and civil society in dialogue on a core set of principles to guide the evolution of the international technology ecosystem. The G7 should aim to convene a Future Tech Forum on a yearly basis, building political momentum on tackling long term challenges in the sector, and working closely with appropriate international organisations like the OECD.

18. The G7 should enhance cooperation between industry and government on measures to counter online harms to keep citizens safe and to protect democracies from misinformation and disinformation, while maintaining safeguards that support

free speech, pluralism, and digital skills. This cooperation should extend from G7 countries to the rest of the world.

19. Given the importance of the technical standards which underpin the internet and digital growth, the G7 should support the industry-led multi-stakeholder model, while focusing on capacity-building which allows industry and civil society to engage effectively.

20. As some of the world's leading digital nations, G7 nations should advance and expand upon OECD thinking on emerging issues in the digital economy – for example, government access to data (as outlined above) or ethical frameworks for AI.

Widespread alignment and adoption of tools to digitise trade and make it frictionless

Principles:

- Trade will be central to an inclusive pandemic recovery. Now is a crucial time for the G7 to show leadership, at a moment where global trading rules are struggling to keep pace with changes in technology. G7 countries should champion trade modernisation, building on a partnership between businesses and governments that helps firms, particularly SMEs, to grasp the opportunities of digital trade.

- Businesses will look to government to set the legal framework and create the right context for a balanced economic recovery. Equally, industry will play its part to support a better international trading system, which responds quickly to key issues like technology, net zero, and new forms of commerce.

- Digitising the estimated four billion paper documents that are used each year for shipment of goods and trade finance would cut costs, reduce delays, and support greater technology use throughout the supply chain. These improvements would make significant gains for the trade ecosystem, particularly SMEs, who often lack the time and the capacity to manage the estimated 15 documents required per trade transaction.

Policy Recommendations:

21. The G7 should identify the legal, regulatory, and technical obstacles to the use of Electronic Transferrable Records in G7 countries.

22. The G7 should commit to a timetable for aligning legal frameworks to the UN Commission of International Law (UNCITRAL) Model on Electronic Transferable Records (MLETR). Alignment with MLETR should include documents of transport, bills of lading, bills of exchange, promissory notes, and warehouse receipts.

23. Each G7 country should identify a single lead department who is responsible for digitising trade and report back on progress. This is because processes that need to be harmonised are complex, vary between countries, and often fall between different Ministers in each G7 state.

24. The G7 should commit to funding capacity-building for developing economies in this area. Businesses want to see as many countries as possible creating compatible systems to reduce friction and risk.