cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS

PRESERVING CONVERGENCE AND ORGANISING CO-EXISTENCE

PASCAL LAMY
BRUNO LIEBHABERG
et al.

November 2022

As provided for in CERRE's bylaws and procedural rules from its "Transparency & Independence Policy", all CERRE research projects and reports are completed in accordance with the strictest academic independence.

The project, within the framework of which this report has been prepared, has received the support and/or input of the following CERRE member organisations: Huawei, Meta, Qualcomm, and Vodafone. However, these bear no responsibility for the contents of this report. The views expressed are attributable only to the authors in a personal capacity and not to any institution with which they are associated. In addition, they do not necessarily correspond to those of CERRE, of any sponsor, or members of CERRE.

info@cerre.eu – www.cerre.eu

TABLE OF CONTENTS

ABOUT CERRE

Providing top quality studies and dissemination activities, the Centre on Regulation in Europe (CERRE) promotes robust and consistent regulation for the network and digital industries. CERRE's members are regulatory authorities, companies, and university centres.

CERRE's added value is based on:

- its original, multidisciplinary and cross-sector approach;
- the widely acknowledged academic credentials and policy experience of its team and associated staff members;
- its scientific independence and impartiality;
- the direct relevance and timeliness of its contributions to the policy and regulatory development process applicable to markets and corporations.

CERRE's activities include contributions to the development of norms, standards, and policy recommendations related to the regulation of goods and service providers, the specification of market rules, and improvements in the management of infrastructure in a changing political, economic, technological, and social environment. CERRE's work also aims at clarifying the respective roles of market operators, governments, and regulatory authorities, as well as at strengthening the latter's expertise.

ABOUT THIS PROJECT

With a view to coming up with a set of policy recommendations focusing on the features of a global governance system that would efficiently address and respond to the new challenges of digitalisation, the **Centre on Regulation in Europe (CERRE)** launched in October 2021 a strategic initiative titled "**Global Governance for the Digital Ecosystems**". CERRE is a Brussels-based think tank widely acknowledged and respected for its independence and its leading-edge expertise and influence on regulation and policy for digital and other network industry sectors.

This new initiative has been co-led by **Pascal Lamy**, President of the Paris Peace Forum, former Director of the World Trade Organisation, and member of the Board of CERRE, and **Bruno Liebhaberg,** founder and Director General of CERRE.

It has involved some 30 top level contributors, including not only some of the **CERRE academic principals**, but also other **first-class experts from Europe, the United States, China, and other countries**.

Given the width of relevant issues for which the question of global governance patterns is relevant, it has been decided that, at this stage – which could possibly have been just the first year of a potentially longer initiative – the project scope would be focused and limited to four broad areas – hereafter workstreams – which constitute some of the key blocks of the digital ecosystems. These are **infrastructure**, **online platforms**, **data**, **and digital trade.**

Each workstream has produced a comprehensive report as well as a set of recommendations. An executive summary has then been drafted with a view to providing, on the basis of the workstreams' papers, a number of select policy recommendations which capture the main messages conveyed by this initiative. This document includes all five papers.

This project has benefited from the engagement and support of the following CERRE member organisations: Vodafone, Qualcomm, Meta, and Huawei. These organisations' representatives have, along with the workstreams' academic leaders, select top level regulators, and external academics, been part of the project's Central Steering Committee which has regularly followed up and commented on work progress.

Experts from the supporting organisations have also had the opportunity to follow up and comment upon progress in the various workstreams, within the framework of one specific Steering Committee set up for each workstream.

Finally, in line with CERRE's bylaws and with its Guidelines on Transparency and Independence, the research team has worked with full academic independence. The contents of both the workstreams' reports and the covering note are attributable to their respective authors only and do not commit any other individual or organisation, whether they have, in one or another way, or have not been involved in this project.

RESEARCH TEAM

Co-Leads

Pascal Lamy

President, Paris Peace Forum and member of the Board, CERRE

Pascal Lamy is the President of the Paris Peace Forum, a member of the Board of CERRE, and President Emeritus of the Institut Jacques Delors. He co-ordinates the Jacques Delors Institutes in Paris, Berlin, and Brussels. He is also President or member of various boards with a global, European or French vocation (Mo Ibrahim Foundation, European Climate Foundation, European Branch of the Brunswick Group, and others). He is an affiliated professor at the China Europe International Business School CEIBS (Shanghai) and at HEC (Paris).

From 2005 to 2013, Pascal Lamy served two consecutive terms as Director General of the World Trade Organization (WTO). He was previously the EU Trade Commissioner (1999-2004), Director General of Crédit Lyonnais (1994-1999), Chief of Staff of the President of the European Commission, Jacques Delors and his G7 Sherpa (1985-1994), Deputy Chief of Staff of the French Prime Minister (1983-1985) and to the French Minister of the Economy and Finance (1981-1983). His last publication was “Strange new world” (Odile Jacob, 2020).

Bruno Liebhaberg

Founder and Director General, CERRE

Bruno Liebhaberg is the Director General of the think tank Centre on Regulation in Europe (CERRE) which he founded in 2010. From 2018 to 2021, he was also the first Chairman of the European Union Observatory on the Online Platform Economy. He is also an Honorary Professor at the Université Libre de Bruxelles’ Solvay Brussels School of Economics and Management (SBS-EM ULB) where he taught from 1979 to 2018. Earlier in his career, he advised former European Commission President Jacques Delors on industry and R&D matters related to the completion of the EU Single Market. He holds a Master in Management Sciences from SBS-EM ULB and a Ph.D. in Industrial Relations from the London School of Economics and Political Science.

Workstream Leads

Marc Bourreau

CERRE Academic Co-Director and Professor, Télécom Paris

Marc Bourreau is an Academic Co-Director at CERRE and Professor of Economics at Télécom Paris (Institut Polytechnique de Paris). He is affiliated with the interdisciplinary institute for innovation (i3). His research focuses on competition policy and regulation, digital markets, and telecommunications. Marc holds a Ph.D. in Economics from the University of Paris Panthéon Assas.

Alexandre de Streel

CERRE Academic Director and Professor, University of Namur

Alexandre de Streel is an Academic Director at CERRE and a Professor of European Law at the University of Namur and the Research Centre for Information, Law and Society (CRIDS/NADI). Since April 2021, he is also the Chair of the European Union Observatory on the Online Platform Economy. He is a Hauser Global Fellow at New York University (NYU) Law School and visiting professor at the College of Europe and Sciences-Po Paris, and also an assessor at the Belgian Competition Authority. His main areas of research are regulation and competition policy in the digital economy as well as the legal issues raised by the developments of artificial intelligence. Recently, he advised the European Commission and the European Parliament on the regulation of online platforms. Previously, Alexandre worked for the Belgian Deputy Prime Minister, the Belgian Permanent Representation to the European Union, and the European Commission (DG CNECT). He holds a Ph.D. in Law from the European University Institute and a Master's Degree in Economics from the University of Louvain.

Richard Feasey

CERRE Senior Advisor, Tech, Media & Telecom

Richard Feasey is a Senior Advisor at CERRE and an Inquiry Chair at the UK's Competition and Markets Authority. He lectures at University College, King's College London, and the Judge Business School. He has previously been a Member of the National Infrastructure Commission for Wales, a Senior Adviser to the UK Payments Systems Regulator, and an adviser to the House of Lords EU Sub-Committee and various international legal and economic advisory firms. He was Director of Public Policy for Vodafone plc between 2001 and 2013.

Jan Krämer

CERRE Academic Co-Director and Professor, University of Passau

Jan Krämer is an Academic Co-Director at CERRE and a Professor at the University of Passau, Germany, where he holds the chair of Internet & Telecommunications Business. Previously, he headed a research group on telecommunications markets at the Karlsruhe Institute of Technology (KIT), where he also obtained a diploma degree in Business and Economics Engineering with a focus on computer science, telematics and operations research, and a Ph.D. in Economics, both with distinction. He is the editor and author of several interdisciplinary books on the regulation of telecommunications markets and has published numerous articles in the premier scholarly journals in information systems, economics, management and marketing research. Professor Krämer has served as an academic consultant for leading firms in the telecommunications and internet industry, as well as for governmental institutions, such as the German Federal Ministry for Economic Affairs and the European Commission.

Patrick Low

Fellow, University of Hong Kong

Patrick Low is currently a Fellow at the Asia Global Institute of the University of Hong Kong and a Senior Adviser for Tulip Consulting. Between 1997 and 2013, Patrick was the Chief Economist of the WTO, where he was responsible for economic research and statistics within the WTO. He was also responsible for the WTOs flagship publication, the World Trade Report, and several statistical publications.

Senior Advisor to the Co-Leads

Adrien Abécassis

Chief Policy Officer, Paris Peace Forum

Adrien Abécassis is the Chief Policy Officer of the Paris Peace Forum, where he leads the team dedicated to running wide-ranging initiatives strengthening the governance of global commons. A career diplomat, he served from 2012 to 2017 as Senior Political Advisor to the President of France. He has worked for over 15 years in international policy, science and technology policy, and global governance. He was an International Affairs Fellow at Harvard, a Fellow at the University of California and an appointee at the Harvard Kennedy School's Mossavar-Ramani Center for Business and Governance.

Other Co-Authors

The academics in this list co-authored the workstream paper entitled “Prospects for Harmonisation of Global Data Governance” co-ordinated by Professor Jan Krämer.

Anupam Chander
Professor, Georgetown University

Dr. Alice de Jonge
Senior Lecturer, Monash University

Moritz Hennemann
Professor, University of Passau

Marcelo Thompson
Assistant Professor, University of Hong Kong

ACKNOWLEDGEMENTS

The co-leads of this project, Pascal Lamy and Bruno Liebhaberg, wish to thank the project research team for their involvement and invaluable contributions. They also express their gratitude to the CERRE sponsoring members and all participants of the Central and Workstreams' Steering Committees for their constructive comments, support, and engagement throughout the project, with full respect to our think tank's strict academic independence. The Central Steering Committee consisted of top-level representatives of the sponsoring members, as well as other senior experts, including: Catherine Chen Lifang, Executive Member of the Supervisory Board and President of the Public Affairs and Communications Department at Huawei Technologies; Wassim Chourbaji, Senior Vice President, Government Affairs and Public Policy EMEA at Qualcomm Incorporated; Nick Clegg, President, Global Affairs at Meta; Merit E. Janow, Dean Emerita and Professor of Practice, International Economic Law & International Affairs at the School of International and Public Affairs (SIPA) of Columbia University; Tony Jin Yong, Vice-President West-Europe, Public Affairs and Communications and Chief Representative to the European Institutions at Huawei Technologies; Elina Noor, Director, Political-Security Affairs and Deputy Director, Washington, D.C. Office at the Asia Society Policy Institute; Markus Reinisch, Vice President Public Policy EMEA at Meta; Joakim Reiter, Group External and Corporate Affairs Director at Vodafone Group; Alex Rogers, President of Qualcomm Technology Licensing and Global Affairs at Qualcomm Incorporated; Michel Van Bellinghen, Chairman of the Council at the Belgian Institute for Postal Services and Telecommunications (BIPT) and Chair 2021 of BEREC; David Wang, President Global Governance Affairs at Huawei Technologies; and Henry Huiyao Wang, Founder and President of the Center for China and Globalization. Finally, the co-leads praise the achievements of the CERRE secretariat, and in particular of Konrád Ferenczy and his colleagues, for having managed with great dedication a one-year-long project which, due to its complexity and global scope involving participants based in many parts of the world from San Diego to Shenzhen, has not always been easy to organise logistically.

EXECUTIVE SUMMARY

The growing dominance of the digital economy provides considerable economic and socio-political opportunities. It also generates significant new challenges in terms of regulation and governance. While innovation accelerates, geopolitical frictions, and the reassertion of States' control on cyberspace are changing the landscape of both digital regulation and the globalisation process.

The principle that digital ecosystems are interconnected at a global scale can no longer be taken for granted. The world is moving at an increasing pace towards a technological decoupling that will have a profound impact on all aspects of the modern economy.

Developing divergent or non-compatible systems across geopolitical blocs will create technological lock-in for decades and will have ripple consequences well beyond the tech economy. Therefore, given the magnitude of the resulting impact of these developments, it would be wise to stop for a moment and carefully weigh the alternatives and consequences.

Strong forces are still pushing in both directions: convergence to foster a deeper global digital economy, and segmentation of that same digital economy into divergent sub-parts.

Open markets and international trade have brought collective benefits to businesses and citizens in recent decades. They have contributed to scientific advancement and to building the global technological ecosystems and supply chains that we know today. Increasing returns to scale produced by data accelerate these dynamics and apply at national and international levels alike. These are results that should not be overlooked. An argument is frequently made that the enhancement of open high-tech markets could reproduce the waves of innovation and shared progress of the late 20th century.

However, one of the digital economy's specificities is that it is not 'neutral' in terms of values. Unlike trading steel, shoes or consultancy services, trading data and other digital services often affects strongly held collective preferences such as privacy or freedom of speech in the public sphere. While digital players are becoming indispensable operators for a growing number of social activities – occasionally assuming quasi-sovereign functions, from regulating the public discourse to developing currencies – the extent of legitimate norm-setting capacity by those players and by States varies across jurisdictions, with different views of legitimacy. This may lead to divergent policies.

In the name of collective preferences, market dynamics and optimisation of economic efficiency are impacted, sometimes profoundly. The overall tension between economic and other social and political objectives often leads to a new *precautionism*, tilting the world towards digital fragmentation.

Furthermore, as the digital economy emerges as a key arena of international competition, there is a growing trend toward actively curtailing some technological linkages and supply chains on the grounds of national security and/or national economic interests. This primarily affects technologies considered strategic or fundamental to national power and welfare. The full extent that this active segmentation will reach is still uncertain, but it is increasingly having a considerable effect on important parts of the digital economy – affecting, beyond semiconductors, a growing number of equipment and services.

The outcome of the tension between convergence and segmentation of the digital economy will have a decisive influence on the global economy and on the balance of power. Arguably, it is one of the most pivotal choices that will define the future of the world economy.

In this CERRE report, we argue that **the general objective for the global governance of the digital ecosystems should be to preserve, and promote where possible, convergence and organise coexistence where convergence is not possible**. Convergence should be promoted in order to reap the benefits of economies of scale and of a level playing field, and coexistence should be organised when divergences are unavoidable.

A full, comprehensive convergence would be neither realistic nor, in many instances, appropriate. Some divergence in digital regulatory policies is both inevitable and desirable. Diverse preferences and priorities among countries must be respected and accommodated. But, if those preferences do not yield to market optimisation, inflexibility on preferences should also not lead to unnecessary costs in terms of economic welfare. Both risks must be avoided. The benefits that can be derived and shared from a relatively open, cross-border digital economy should be carefully balanced with appropriate protection of public policy objectives.

A distinction must be made here between decoupling and divergence. Decoupling is the active restriction of the way technology products, services, and inputs move between countries and continents. It involves extensive use of technology restrictions: export controls, divestment orders, license denials, visa bans, and sanctions. Divergence is the accumulation of distinctive national or regional regulations in an unco-ordinated manner, each responding to specific collective preferences. In that respect, divergence is not an absolute, binary concept, that is, yes/no – it is relative, and its assessment will be based on the compliance cost it imposes.

While decoupling occurs mainly between the United States and China, divergence occurs at all levels (e.g., privacy in the transatlantic framework). However, the line between the two concepts may sometimes be blurred. This is due to reasons for trade restrictions that are not always explicit, as well as to a growing acceptance of an expanded definition of national security that includes economic security and, as such, may go beyond the national security exception of the WTO framework. In both cases, segmentation between major digitally-enabled or data-intensive cross-border systems will be extremely costly. The freezing or failure of a financial system, global value chains and the management of global public goods – including space, weather, and civil aviation – could wreak havoc.

The reports of the four workstreams around which this project has been built, that is **online platforms, data, infrastructure, and digital trade**, fully recognise the decoupling trend. It comes down to a fundamental policy choice that must be properly debated. Divergence is more often a consequence of a multitude of implicit choices. In this sense, better constructed governance mechanisms can mitigate any unintended effects. This is what the reports focus on. We must nonetheless recognise that the risks of triggering escalation spirals should not be overlooked: decoupling measures could set in motion a series of retaliatory measures and incentivise actors to pre-emptively reduce technology linkages to avoid future costs.

To enhance the considerable economic and socio-political benefits and opportunities provided by the digital economy and meet, at global level, the new challenges the latter raises in terms of regulation and governance, the report from each of the four workstreams contains recommendations organised around four policy objectives: **efficiency, compatibility, resilience, and coherence**.

Efficiency

Wherever convergence can be achieved at a lower cost to collective preferences, it should be sought. This means reaffirming that openness must be the rule, with justified restrictions being an exception. This involves setting-up procedural and co-ordination mechanisms that can facilitate the functioning and regulation of the digital economy, reduce transaction costs, and increase efficiency for all stakeholders involved, including regulators.

Specific recommendations under the efficiency heading include the following measures:

- International standards on transparency measures imposed on platforms should be harmonised. Common methodologies and requirements should be developed regarding the transparency obligations and the technical and practical implementation measures (such as, API and standards for access to data and algorithms, standards and metrics for transparency reports on content moderation, or criteria for disclosing recommenders' parameters).
- To limit the risk of escalation of decoupling measures, governments should jointly commit to an international agreement stating the principles of openness and non-discrimination while recognising exceptions for legitimate national public policy imperatives.
- Governments should agree to align bilateral and regional digital trade agreements with the above two principles. Preferential trade agreements can intensify co-operation, and governments should seek out combinations of preferential trade agreements (PTA) that, together, would get as close as possible to a multilateral outcome.
- Rather than pursuing a comprehensive multilateral agreement on digital trade, the specific results already emerging from the ongoing WTO-based negotiations in relation to consumer protection, electronic signatures, spam, open government data, and electronic contracts should be formally consolidated while negotiations continue on other outstanding issues. These agreements should encompass both the regulation of digital ecosystems and open market access with respect to the relevant services and goods sectors.
- International consensus-building and co-operation amongst public bodies engaged in overseeing major digital platforms should be reinforced. In that respect, the current formal and informal international networks of regulators should be strengthened to ensure better exchange of expertise and confidential information-sharing between agencies. The structure and functioning of the Basel Committee on Banking Supervision (BCBS) and/or of the

International Competition Network (ICN) could be considered as potential models to identify the most effective format.

- A new WTO Reference Paper for digital platforms should be proposed to consolidate pro-competitive regulation.

Compatibility

For many years, it has been considered that national security-related trade restrictions were outside the scope of WTO jurisdiction. In recent years, however, the number and scope of measures taken on that ground and constituting trade barriers have particularly increased. **Restriction of trade for national security reasons should be selective, targeted and co-ordinated** as much as possible.

Furthermore, everything that allows the compatibility of systems that are not convergent must be actively sought and prioritised to maximise the mutual benefits. There are encouraging examples, such as the adequacy approaches, that make it possible to maintain a high degree of openness in exchanges between blocks with slightly divergent preferences, for example on privacy. This also means preserving global standards at the technical level, as long as they can be detached from values; and anticipating future regulatory issues now to identify and bridge possible divergences in the future.

Specific recommendations under the compatibility heading include the following measures:

- Adequate accountability and transparency levels should be ensured regarding public policy exceptions to digital trade openness and non-discrimination. These could include requirements to pre-notify intended measures and to justify in writing the reasons for and the extent of measures taken.
- Global standards in key, current and future tech networks (5G and 6G) should be preserved and consolidated.
- Future technological developments (and current developments such as network virtualisation and edge computing) should be anticipated more efficiently to avoid lock-in of technical choices which would subsequently be undone at high cost after the infrastructure has been deployed on a large scale.
- Divergence in data and privacy regimes should be accepted, but mutual recognition should be used to enable the transfer of data (likely non-personal) between regimes wherever possible. Mutual recognition should be aimed and tested at a global level (such as, an “adequacy” approach) when direct harmonisation of preferences is unlikely (such as, privacy), while recognising that the transfer of particularly sensitive data may remain subject to more restrictive conditions (such as, personal genomic data). In that respect, the progress of discussions on the Privacy Shield is encouraging. The United States and European Union authorities could take advantage of a renewed interest in privacy rules to seek greater convergence, even though it will remain far from a global standard.

- New avenues for data regulation should be explored, such as a Model Law on Data Trusts, an International Global (Framework) Agreement on Data Commons, and an International Agreement / Soft Law on Non-Personal Data Contract Rules.

Resilience

The stability of transnational digital infrastructures is a prerequisite for the functioning of digital ecosystems. However, these infrastructures are still structurally fragile and subject to increasing offensive pressures. A series of measures concerning the interoperability of operators, approval procedures for critical equipment and security reinforcement for submarine cables must address these weaknesses and reinforce the resilience of the global digital infrastructure.

Specific recommendations under the resilience heading include the following measures:

- Users in all States should be able to rapidly switch between wireless networks in the event of network disruption. To ensure this, States should define the conditions under which regulatory authorities can direct operators to reserve capacity in their networks and enable rapid switching under emergency conditions.
- A process of pre-approval of critical digital infrastructure equipment before deployment, irrespective of country of origin, should operate in each State. This should ensure that equipment is secure to be deployed and that it is deployed by individual firms in a way which contributes to resilience and diversity across the system as a whole. Firms may be required to alter their commercial plans as a result. States should pool information and knowledge about equipment in order to assist in this process.
- Regulators should have a duty to consider resilience when reviewing mergers or network sharing arrangements, and when regulating networks generally.
- Coordinated action should be taken with regard to the global submarine cable infrastructure whilst recognising that some parts of the system are currently more resilient than others. Points of greatest vulnerability in international waters should be identified and co-ordinated measures should be taken by States to improve diversity with respect to both ownership and routing of these cables. National action is also required to ensure security and resilience at cable landing stations and that, for future undersea cables, monitoring systems are installed where required.

Coherence

The global governance of the digital economy cannot be based on a single regime or institution. It can only be a **"regime complex"**, that is, a loosely coupled set of specific regimes providing different sets of norms at diverse levels involving a wide variety of stakeholders. That said, coherence of the system requires **new co-ordinating venues**. On such a crucial subject for the future of the global economy, international co-ordination is clearly underdeveloped. Dialogues happen often in silos preventing the proper integration of competing policy objectives, and national interventions are multiplying without a global institution being mandated to monitor them and assess their effects.

We are mostly moving forward blindly. We therefore propose the establishment of a Digital Stability Board, which would provide for organised processes involving a broad set of stakeholders.

Specific recommendations under the coherence heading include the following measures:

- Enhanced coherence in the global governance of the digital ecosystems requires rejuvenated roles for existing institutions as well as a new, multi-stakeholders co-ordinating forum. Alongside existing institutions, such as the ITU and the WTO, non-decisional instances are needed. They would hold two types of dialogues: monitoring and exchanging on emerging issues where co-ordinated action would be beneficial in the future; and facilitating immediate agreements in dedicated forums where national actions exist, and convergence seems feasible.
- The G20 should establish a Digital Stability Board (DSB). Designed like the Financial Stability Board, this forum would gather representatives from national governments (including security agencies) and regional institutions, regulators in charge of digital, privacy, consumer protection, finance and competition, industry, think tanks, and relevant non-governmental organisations. The DSB mandate could be as follows:
    - identify, observe, and monitor technological and regulatory developments and business practices, including related "vulnerabilities";
    - identify risks and detect issues where policy choices will have to be made, without, however, having any decision-making power;
    - outline, once or twice a year, issues that merit further debate and examination; and
    - report annually directly to the G20 to inform the leaders' discussions.

Towards a New Digital World Order

Even in a "**globalisation with firewalls**", the world would strive to reap the benefits of an open digital economy. The above set of recommendations has been developed with a view to maximising the benefits of such an economy. They also recognise the legitimate divergences and the always interacting and often conflicting objectives of growth, competition, fair and stable social organisations, national security, and ethics.

We are convinced that global, well-regulated, and dense exchange flows of both data and digital technology are crucial to preserving scientific progress, increasing further innovation speed, and hence, providing optimal responses to major global challenges, such as development, climate change, health, and inequalities.

Our recommendations are not exhaustive and other actions will certainly be needed, but we are convinced that their implementation will represent important steps towards a new digital world order.

cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS

TOWARDS A GLOBAL GOVERNANCE OF ONLINE PLATFORMS

ALEXANDRE DE STREEL

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The lead of this paper, Prof. Alexandre de Streel, wishes to thank the academic team for their involvement and invaluable contributions to the discussions in the Workstream Steering Committee. The latter, included Prof. Christoph Busch, Professor of German and European Private and Business Law and Private International Law at the University of Osnabrück; Prof. Amelia Fletcher CBE, Professor of Competition Policy at the Centre for Competition Policy of University of East Anglia and Non-Executive Director at the Competition and Markets Authority of the UK; Prof. Liyang Hou, Professor of Law at KoGuan Law School of the Shanghai Jiao Tong University; Dr. Martin Husovec, Assistant Professor of Law at The London School of Economics and Political Science; Daphne Keller, Director, Program on Platform Regulation at Stanford's Cyber Policy Center; Michele Ledger, Head of Practice at Cullen International and Researcher and Assistant Lecturer at University of Namur; Prof. Fiona Scott Morton, Theodore Nierenberg Professor of Economics at the Yale School of Management; and Prof. Marco Ruediger, Professor, Director of Public Policy Analysis at Fundação Getulio Vargas (Brazil).

1. INTRODUCTION

Until very recently, since their inception in the 1990s, digital platforms have not been subject to regulation and heavy state intervention[1] for several reasons: they invented new business models, some of which escaped existing regulatory categories; their growth – which brought enormous economic and societal benefits – had to be protected from public intervention (akin to an 'infant industry argument'); and there was a general belief that technological innovation should be encouraged, while State intervention should remain proportionate, which often meant minimalist. This is probably best exemplified by the conditional liability exemption provisions found in most e-commerce laws across the world, as well as the promotion of self- or co-regulation, where rules are applicable.

This 'digital exceptionalism', combined with several characteristics of the platform economy such as economies of scale and scope, network effects, and data feedback loops, has led to the rapid growth of some platforms which brought massive technological innovation to society. Hence, the strategy of digital policy makers has worked extremely well and probably delivered beyond their expectations.

However, over time, some platforms have become the orchestrators of key ecosystems, and policy makers are starting to realise that their global economic and informational powers are not without risks for economies and society at large.[2] Policy makers' first reaction[3] has been to strengthen self- and co-regulation, but this is now seen as insufficient in a number of policy areas,[4] and **many jurisdictions across the world are considering new regulations to control the use of the power of Big Tech platforms**.[5] To remain concise, the scope of this report is limited to the regulatory initiatives in three main world jurisdictions: the EU, US, and China, as summarised in Table 1 below, and only occasionally covers other jurisdictions.

Among those three jurisdictions, the EU leads the march of tech regulation. Since 2010, it has strengthened its antitrust enforcement against US Big Tech companies; DG COMP has already adopted three decisions against Google and opened many ongoing cases against Apple, Amazon, and Facebook. More recently, under the Digital Single Market Strategy of the Juncker Commission, European Union lawmakers adopted several new regulations:[6]

- In 2018, the reform of the Audiovisual Media Services Directive (AVMSD) to improve the safety of users by video sharing platforms;
- In 2019, a law to better protect copyrighted material online (Directive on Copyright in the Digital Single Market), and another law to improve transparency and dispute resolution

[1] As espoused by the libertarian John Perry Barlow, in his famous 'Declaration of the Independence of Cyberspace' made at Davos in 1996: https://www.eff.org/fr/cyberspace-independence
[2] As shown for instance by Cohen (2019), Wu (2018) and Zuboff (2019).
[3] For an insightful account of the evolution of platform regulation, see Bietti (2021).
[4] Cusumano, Gawer and Yoffie (2021).
[5] As shown in Internet & Jurisdiction Policy Network (2019). The Internet & Jurisdiction Retrospect Database tracks monthly trends since 2012: https://www.internetjurisdiction.net/reports
[6] Next to those hard law, several Codes of conducts and co-regulatory initiatives were also taken to reduce the dissemination of illegal and harmful online content, such as hate speech or disinformation.

mechanisms of intermediation platforms, the so-called Platforms-to-Business Regulation (P2B); and

- In 2021, a law on terrorist content moderation (TERREG).

The von der Leyen Commission continued going further, and this legislative inflation culminated in 2022 with the adoption of the Digital Markets Act (DMA), which aims to increase online markets' contestability and fairness, and the Digital Services Act (DSA), which aims to prevent the dissemination of illegal material (both content and products) online, while also protecting freedom of expression.

China intervened later in its platform economy, but did it very forcefully by adopting several antitrust decisions against Chinese Big Tech in 2020-2021, in what has been described as a 'tech crackdown'.[7] The State Administration for Market Regulation (SAMR) has adopted a series of decisions condemning the abuse of dominant positions and prohibiting tech acquisitions. In parallel, Chinese lawmakers amended their antitrust legislation in 2022 to better take into account the effects of data and algorithms, after having submitted two important draft laws for public consultation in 2021 to classify online platforms and regulate them more strictly.

The United States is the least interventionist jurisdiction, but the current Biden administration is committed to better regulating digital platforms. The Federal and State antitrust agencies have opened several cases against the US Big Tech. In parallel, the United States Congress is now debating several Bills which aim to increase innovation and choice in the US digital markets, such as the American Innovation and Choice Online Act (AIOCA), the Open App Markets Act (OAMA), as well as to improve content moderation practices and their transparency, such as the Platform Accountability and Consumer Transparency Act (PACT Act).[8]

[7] For the reasons behind this crackdown, see Zhang (2022).
[8] Many of the proposed reforms of Section 230 are listed in a US Congressional Research Service publication (2021: Appendix B) and at https://www.brookings.edu/techstream/legislative-efforts-and-policy-frameworks-within-the-section-230-debate/

Table 1: Main Regulations and Draft Regulations Applicable to Digital Platforms

EU	US	China
- TFEU: Competition law - E-Commerce Dir. (2000)[9] - AVMSD (2018)[10] - Copyright (2019)[11] - P2B (2019)[12] - TERREG (2021) [13] - DMA (2022)[14] - DSA (2022)[15]	- Sherman Act - Section 230 CDA (1996)[16] - AICOA Bill[17] and OAMA Bill[18] - PACT Bill[19]	- Anti-Monopoly Law (2022)[20] - E-Commerce Law (2018)[21] - Draft Platform Laws (Oct 2021)[22]

While each jurisdiction has a legitimate claim to regulate – and take control of – 'its' own cyberspace, the worldwide multiplication of public policy initiatives in an unco-ordinated manner may be less effective and more costly for platforms and their users because it will lead to the fragmentation of global platforms, and therefore, the loss of economies of scale and scope, and network effects which are massive for digital technologies.[23] Thus, **global co-ordination of those regulatory initiatives is very desirable**.

However, global co-ordination may not be easy to achieve because it deals with digital services which, on the one hand, have become foundational for the economy, hence a key strategic asset in geo-political world competition, and on the other hand, carry societal values which are different across jurisdictions. Therefore, a co-ordinated approach to digital regulation could bring high benefits, but with difficulty.

[9] Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce), OJ (2000) L 178/1.
[10] Directive 2018/1808 of the European Parliament and of the Council of 14 November 2018 Amending Directive 2010/13 on the Co-ordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audio-Visual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities, OJ (2018) L 303/69.
[11] Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9 and 2001/29, OJ (2019) L 130/92.
[12] Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on Promoting Fairness and Transparency for Business Users of Online Intermediation Services, OJ (2019) L 186/55.
[13] Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJ (2021) L 172/79.
[14] Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives 2019/1937 and 2020/1828 (Digital Markets Act), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A265%3ATOC&uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG
[15] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A277%3ATOC
[16] See: https://www.law.cornell.edu/uscode/text/47/230
[17] See: https://www.congress.gov/bill/117th-congress/senate-bill/2992
[18] See: https://www.congress.gov/bill/117th-congress/senate-bill/2710
[19] See: https://www.congress.gov/bill/117th-congress/senate-bill/797
[20] See: https://www.chinalawtranslate.com/en/anti-monopoly-law-2022/
[21] See: https://www.chinalawtranslate.com/en/p-r-c-e-commerce-law-2018/
[22] An unofficial translation can be found at: https://www.ianbrown.tech/2021/11/01/chinas-new-platform-guidelines/
[23] As noted in the Internet & Jurisdiction Global Status Report (2019) p. 14.

This report aims to contribute to the global co-ordination efforts by identifying the regulatory trends across three of the main world jurisdictions and, on that basis, by identifying global convergence potential and proposing paths to unleash it. To that end, the report is structured as follows: after this introduction, section 2 deals with transparency and risk assessment regulation; section 3 deals with competition and innovation regulation; section 4 deals with content moderation regulation, and; section 5 deals with regulatory principles and enforcement modes.

2. IMPROVING TRANSPARENCY AND RISK ASSESSMENT

One of the main difficulties of digital public policy, is the very significant asymmetry of information between, on the one hand, platforms and, on the other hand, the users of the platforms and public authorities. This difficulty is not new in regulatory studies,[24] but is exacerbated in the platform economy because many digital technologies and business models are new, they evolve quickly and can be very complex. To deal with this feature, the first and most basic measure is to improve transparency of platforms and algorithms. To do that, the (draft) regulations in the European Union, United States, and China show three types of transparency obligations, with an increasing level of intrusiveness for the regulated platforms.

The **first type of transparency obligations is limited to the benefit of public authorities** (and in some cases independent researchers), they include:

- the **investigative power** of regulatory agencies, in particular on the power to request information on databases and algorithms to fully understand business models that are increasingly based on data and AI;[25]
- the possibilities to **transfer data and information to other authorities** in the same countries or across countries to increase the efficiency of each agency; and
- the possibilities to **transfer data and information to vetted independent researchers** in order to get their support in analysing those data, which is often a very complex task necessitating deep expertise.[26]

The first type of obligations mostly aims at ensuring the effectiveness of the oversight of regulated platforms and the enforcement of the new rules. As the information is only given to authorities - and not their users, competitors, or the general public - the limits of Intellectual Property (IP), trade secret, and business confidentiality should not apply, provided that they are respected by the authorities when they use such information.

The **second type of transparency obligations not only benefits the authorities and independent researchers, but also the users of the regulated platforms and, often, the public at large**; they include:

- transparency on the **terms of use and rules** they apply to their services, which are key as the platforms play the role of 'the regulator' of their cyberspaces;[27]
- transparency obligations on the **main parameters used in algorithms**, in particular in recommender systems;[28]

[24] Baldwin et al (2012).
[25] EU DSA, Articles 41, 52-54, 57; EU DMA, Articles 21-23.
[26] EU DSA, Articles 31; US PACT Bill, Section 5(j).
[27] EU DSA, Article 12; US PACT Bill, Section 5(a); Chinese draft platforms law, Article 14.
[28] EU P2B Regulations, Article 5, and Commission Guidelines of 7 December 2020 on Ranking Transparency Pursuant to Regulation 2019/1150 of the European Parliament and of the Council, OJ (2020) C 424/1; EU DSA, Article 24a; Chinese draft platforms law, Article 19.

- **transparency reports** on the conditions and practices to moderate illegal and harmful content online;[29] and
- transparency obligations on the key components of the **online advertising** value chain, such as the use of personal data and profiling parameters,[30] the price paid to the platforms by publishers and advertisers, or performance indicators.[31]

This second type of obligations allows users and authorities to better understand the platforms' functioning, their business models, and underlying algorithms. In turn, this allows the market to work better as the users are better informed and may switch to another platform if they are not satisfied with the product, and when there are alternatives available. This also allows the regulation to work better as any violation of the rules will be more easily detected. However, because the information is given to users who may also compete with the regulated platforms, it is key that this second type of transparency obligations are limited by IP, trade, and business secrets protections.

A **third, and more intrusive, type of transparency obligations consists of requiring the regulated platforms to conduct risk assessments for the products and services they provide**.[32] Those assessments increase the knowledge of the platforms, the authorities, and the public at large on the risks created by the digital services on a number of factors to be determined by the lawmaker, such as competition, fundamental rights, the stability of the economy, and democracy. In turn, this improved information on the risks should lead to mitigation measures by the platforms[33] and/or policy intervention by public authorities.

[29] EU DSA, Article 23 and 33; US PACT Bill, Section 5(d).
[30] EU DSA, Article 24 and 30; Chinese draft platforms law, Article 21.
[31] EU DMA, Article 5(9) and (10) and Article 6(7).
[32] EU DSA, Article 26; Chinese draft platforms law, Article 6.
[33] EU DAS, Article 27; Chinese draft platforms law, Article 7.

Global Convergence Potential

Among all the public policy interventions reviewed in this report, **transparency measures probably have the highest potential for global convergence**, and they can have a significant impact on digital markets. Three categories of issues should be discussed, co-ordinated, and ideally agreed at a global level.

The first category relates to the **investigation powers** of regulatory agencies, which are national, while the regulated platforms are global. To increase such effectiveness, regulators could agree on the technical means (API, standards, and so on) for accessing data and algorithms, so the platforms use the same means in all jurisdictions. Regulators should also agree on a robust global framework to exchange information among them while respecting due process and the right of defence of the regulated platforms, as well as of their IP, and trade secrets rights. In that regard, the model followed by antitrust agencies for international merger control could be an interesting example to follow.

The second category relates to the **technical and practical standards to implement these transparency obligations**. This category includes, for instance, the standards and metrics for content moderation transparency reports, and the criteria for disclosing recommenders' parameters.[34] A global convergence on these measures would be extremely beneficial for the platforms and their users because, on the one hand, it reduces compliance costs for global platforms and, on the other hand, it may increase the effectiveness, and therefore the benefits, of regulation if authorities agree on the best technical implementation measures. To do that, an international digital transparency standards organisation, comprised of all involved stakeholders, could be established. In this regard, the model followed for accounting standards, with the key role played by the *International Financial Reporting Standards (IFRS)* Foundation, may be an example to follow.[35]

The third category relates **to the risk assessment of digital services** provided by regulated platforms. An international discussion and co-ordination should take place on the types of risks to be evaluated, the concrete ways to evaluate them, and the policy measures to be taken to mitigate or deal with those risks. To do that in the most effective manner, an institutional multi-stakeholder forum with a strong expert basis could be established. In that regard, the model of the *Financial Stability Board* may be an example to follow.[36]

[34] Those issues are discussed, for instance, in the EU-US Trade and Technology Council, see Joint Statement of 16 May 2022, Conclusions on Working Group 5 – Data Governance and Technology Platforms, point 3.
[35] https://www.ifrs.org/
[36] https://www.fsb.org/

3. INCREASING COMPETITION AND INNOVATION

In 2019-2020, several policy reports from across the world analysed the features of the platform economy.[37] Some characteristics are not new, such as the multi-sidedness of the markets, the important economies of scale and scope on the supply side, and the substantial network effects on the demand side, but their combinatorial effects raise new policy issues. Other characteristics are new, such as the importance of data and their feedback loops, as well as the extensive use of algorithms and Artificial Intelligence (AI), often machine-learning based. These reports show that those characteristics may naturally lead to the concentration of economic and informational power. This, in turn, may require new policy actions, such as an adaptation and a strengthening of antitrust enforcement and/or the enactment of complementary economic regulation.[38]

While these reports have substantially increased the knowledge and understanding of the platform economy by policy makers, its dynamics are new and evolving[39] and many unknown elements remain. In particular, the innovation dynamics of the platform economy are not yet fully understood, and a key consideration is that policy intervention does not impede such dynamics, but on the contrary, unleashes their potential innovation.

3.1 Antitrust Policy

An **international consensus is emerging that antitrust laws are one of the key public policy tools to deal with an economic concentration in the platform economy**. Antitrust laws have two important features which make them particularly apt to do so. First, they are (economic) principles based, hence they can adapt to technologies and market evolutions. Second, they are globalised, in the sense that many countries have similar types of laws and their national enforcers are part of very developed and active networks (in particular the International Competition Network), hence they can more easily deal with global firms.

3.1.1 Adapting the application of antitrust law and policies

To be fully effective, the application of antitrust laws and policies needs to be adapted to the characteristics of the platform economy.[40] Several international fora contribute to those adaptations. First, the OECD has run a series of competition best practice roundtables on the digital economy since 2018.[41] These roundtables, whose outcome is summarised in OECD (2022), have dealt with several key issues of the platform economy, such as: multi-sided markets, ecosystem markets, digital advertising markets, big data, non-price issues, algorithms and collusion, hub-and-spoke arrangements, data portability and interoperability, merger control in dynamic markets, conglomerate mergers, and killer acquisitions. Second, the International Competition Network (ICN) has also published several reports on antitrust policy in the digital economy, in particular on

[37] In the EU: Cremer et al (2019); in the US: House Investigation in Digital Markets (2020); in the UK: Furman et al (2019); in Australia: ACCC (2019). They are summarised in Lancieri and Morita Sakowski (2021).
[38] Alexiadis and de Streel (2020).
[39] As explained by Galloway (2018) or Parker et al (2016).
[40] Some adaptations are suggested in Jenny (2021).
[41] See: https://www.oecd.org/daf/competition/roundtables.htm

dominance/substantial market power in digital markets,[42] on conglomerate mergers,[43] and on advocacy in digital markets.[44] Third, the G7 antitrust agencies adopted a useful Compendium of approaches in 2021 to improve competition in digital markets.[45]

Thanks to these efforts and internal policy thinking, several countries have recently amended their antitrust (hard and soft) laws to better take into account the features of the digital economy. For example, China adopted the Anti-Monopoly Guidelines for the Platform economy in February 2021, which clarify how the different pillars of the Chinese antitrust law (market definition, monopoly agreements, abuse of dominance, and concentration) apply to the platform economy.[46] In particular, the Guidelines deal with the most common types of abuses of dominance in the platform economy, namely: unfair pricing, refusal to deal, restrictive or exclusive dealings, as well as tying and discrimination. Then in June 2022, China amended its Anti-Monopoly Law[47] to better take into account the effects of data and algorithms in the assessment of market power and abuses of dominance. This reform also allows the review of mergers that are below the notification thresholds, which is often the case for killer acquisitions.

In Europe, Germany has been at the forefront of legislative reforms with the 9th amendment to its competition law in 2018 and the 10th amendment in 2021, to better take into account the characteristics of the platform economy.[48] The United Kingdom's Competition and Market Authority (CMA) has made its merger control stricter after reviewing its merger guidelines in 2021,[49] while the European Union has modified its merger referral system to allow national competition authorities to notify the European Commission of mergers that are below the turnover thresholds.[50] This allows big tech acquisitions to be notified to the Commission, as illustrated by the Facebook acquisition of Kustomer.[51]

In the United States, the federal antitrust agencies are currently reviewing the Merger Guidelines and may include changes in them to, among other things, better deal with the characteristics of digital markets.[52]

---

[42] See: https://www.internationalcompetitionnetwork.org/portfolio/dominance-substantial-market-power-in-digital-markets-survey-report/

[43] See: https://www.internationalcompetitionnetwork.org/portfolio/conglomerate-mergers-project-report/

[44] See: https://www.internationalcompetitionnetwork.org/portfolio/conducting-competition-advocacy-in-digital-markets/

[45] See: https://www.gov.uk/government/publications/compendium-of-approaches-to-improving-competition-in-digital-markets

[46] See: http://english.www.gov.cn/policies/latestreleases/202102/07/content_WS601ffe31c6d0f72576945498.html

[47] For an unofficial translation of the new law, see: https://www.chinalawtranslate.com/en/anti-monopoly-law-2022/ For a briefing on the changes brought by the 2022 revision, see: https://www.china-briefing.com/news/what-has-changed-in-chinas-amended-anti-monopoly-law/ For instance a new Article 9 has been introduced and provides that: "business operators shall not use data, algorithms, technologies, capital advantages, and platform rules to engage in any monopolistic practices prohibited herein." See also amended Article 22.

[48] See: https://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.html The 9th amendment dealt with multi-sided markets as well as data and algorithms, while the 10th amendment deal with ecosystem effects and dependency relationships.

[49] See: https://www.gov.uk/government/news/updated-cma-merger-assessment-guidelines-published

[50] Commission Guidance of 26 March 2021 on the application of the referral mechanism set out in Article 22 of the Merger Regulation to certain categories of cases, O.J. (2021) C 113/1. The legality of such a power to refer otherwise non-notifiable mergers has been confirmed by the General Court in Case T-23/22 *Ilumina v. Commission,* ECLI:EU:T:2022:447.

[51] See: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_652

[52] See: https://www.ftc.gov/news-events/news/press-releases/2022/01/federal-trade-commission-justice-department-seek-strengthen-enforcement-against-illegal-mergers, noting that: "The agencies seek information on how to account for key areas of the modern economy like digital markets in the guidelines, which often have characteristics like zero-price products, multi-sided markets, and data aggregation that the current guidelines do not address in detail."

3.1.2 Strengthening antitrust enforcement

In parallel to the adaptation of laws and policies, an **increasing number of antitrust agencies have prioritised the platform economy and strengthened their enforcement** in this sector with regard to abuse of dominant positions, as shown in Table 2 below, as well as with regard to merger control.

Table 2: Main Abuse of Dominance Decisions Against Big Tech Companies, 2017-21

Year	Jurisdiction	Company	Conduct	Fine ('000 000 Euros)
2017	Europe	Amazon (e-books)	MFN clauses	Commitments
2017	Europe	Google (Shopping)	Self-preferencing	2,420
2018	Europe	Google (Android)	Paying for default	4,340[53]
2019	Europe	Google (AdSense)	Exclusive dealing	1,490
2019	Germany	Facebook	Exploitative terms	--
2019	France	Google (Search ads)	Exploitative terms	150
2021	France	Google (AdTech)	Self-preferencing	220
2021	Italy	Google (Auto)	Refusal of access	102
2021	Italy	Amazon (Logistics)	Self-preferencing	1,128
2021	Netherlands	Apple (Dating)	Tying of payments	Up to 50
2021	South Korea	Google (Android)	Anti-forking agreements	154
2021	China	Alibaba	Exclusive dealing	2,600
2021	China	Meituan	Exclusive dealing	500
2022	UK	Google (Privacy Sandbox)	Exclusion	Commitments

Source: Fletcher (2022)

In the European Union, the Commission has already adopted three decisions against Google condemning its abuse of dominance: for self-preferencing Google Shopping on Google Search,[54] for bundling Android with Google Search and Google Play,[55] and for imposing exclusive dealings when using AdSense.[56] The Commission also forced Amazon to remove several MFN clauses in the context of its e-books.[57] Currently, the Commission has opened several cases against Apple for refusing to give third parties access to its app store[58] and other functionalities, like the NFC chip, for payment services;[59] against Meta for using third party data to benefit its own services;[60] and against Amazon for using third-party seller data for its benefit,[61] and self-preferencing in the Buy Box on its

[53] The amount of this fine has been reduced by the General Court of the EU to 4,125 m euros.
[54] Commission Decision of 27 June 2017, Case 39 740 *Google Search (Shopping)* which has been upheld by the General Court in Case T-612/17 *Google v. Commission*, EU:T:2021:763. An appeal of this judgement is still pending before the Court of Justice in Case C-48/22P.
[55] Commission Decision of 18 July 2018, Case 40 099 *Google Android* which has been upheld by the General Court in Case T-604/18 *Google v. Commission*, EU:T:2022:541.
[56] Commission Decision of 20 March 2019, Case 40411 *Google Search (AdSense)*. This case is under appeal at the General Court in Case T-334/19 *Google v. Commission.*
[57] Decision of the Commission of 4 May 2017, Case 40 153 *Amazon ebooks*.
[58] Case 40 437 *Apple - App Store Practices (music streaming)*; Case 40 716 *Apple - App Store Practices*.
[59] Case 40 452 *Apple - Mobile payments*.
[60] Case 40.684 *Facebook Marketplace*.
[61] Case 40 462 *Amazon Marketplace*.

marketplace website.[62] Furthermore in Europe, the United Kingdom's CMA prohibited the acquisition of Giphy by Meta in 2021.[63]

In China, the SAMR took several decisions condemning abusive exclusive dealings:[64] it condemned Alibaba[65], the big tech conglomerate, as well as Meituan,[66] a large food delivery platform because they were imposing a "choose one from two" clause on their users. SAMR also prohibited several anti-competitive mergers. It blocked the merger between Huya (controlled by Tencent) and DouYu, which are videogame live-streaming platforms because it would have given Tencent control of the two most popular video games in China.[67] It also condemned the already consummated merger between Tencent and China Music Group because of the substantial horizontal effects on the online music broadcast sector. [68]

In the United States, the Department of Justice (DoJ) and several State Attorney Generals, have opened a case against Google alleging that it maintained its monopoly in the search and search advertising markets through anti-competitive and exclusionary practices.[69] The Federal Trade Commission (FTC) and several State Attorney Generals have also opened a case against Meta, alleging that Facebook has engaged in a systematic strategy to eliminate threats to its monopoly in social networks through the acquisition of potential competitors (Instagram in 2012 and WhatsApp in 2014), and the imposition of anti-competitive conditions on software developers.[70]

3.2 Pro-Competitive Regulation

While an international consensus is emerging that antitrust laws and enforcement need to be adapted and strengthened to deal with the concentration of power in the platform economy, many jurisdictions are still **hotly debating whether antitrust should be complemented with new economic regulation**.

Those in favour of such regulation point to the insufficiency and ineffectiveness of antitrust to deal with some competition issues in the platform economy.[71] Antitrust which is implemented after a long case-by-case analysis may be too slow, in particular, given the rapid pace of evolution of digital technologies and markets. Moreover, antitrust remedies are not effective enough because they often cannot restore the competition which existed before the anti-competitive conduct occurred and, more crucially, they are not good at imposing pro-competitive measures, such as access and interoperability, on incumbent platforms. Moreover, fines may not have sufficient deterrent effects, and just be a part of the cost of doing (anti-competitive) business.

[62] Case 40 703 *Amazon - Buy Box*.
[63] See: https://www.gov.uk/cma-cases/facebook-inc-giphy-inc-merger-inquiry
[64] For a very good description of those cases, see Marco Colino (2022).
[65] SAMR Administrative Penalty Decision No. 28 of April 2021.
[66] SAMR Administrative Penalty Decision No. 74 of Oct 2021.
[67] SAMR Press Release and Announcement of 10 July 2021.
[68] SAMR Administrative Penalty Decision (Dec. 2021) No. 67.
[69] See: https://www.justice.gov/atr/case/us-and-plaintiff-states-v-google-llc
[70] See: https://www.ftc.gov/legal-library/browse/cases-proceedings/191-0134-facebook-inc-ftc-v
[71] Fletcher (2022, section II); Scott Morton et al (2019).

Those against economic regulation point to the novelty and the diversity of technologies and business models which are not yet fully understood, and for which an analytical framework does not yet exist. They caution that regulation may slow down or impair the undeniably important level of innovation of online platforms.[72] In the end, they advise those for economic regulation to 'wait and know more' by doing additional market studies and possibly antitrust cases, which can then serve as a sandbox for possible future regulation.[73]

The European Union firmly chose the former camp with the adoption of the Digital Market Acts in 2022, which is the world's first comprehensive economic regulation dealing with Big Tech platforms. This new law will prohibit a number of conducts deemed per se anti-competitive, but also, and more importantly, open up incumbent platforms and data to their complementors, competitors and disruptors. The objective is to increase market contestability and fairness, and ultimately, it is hoped, innovation and choice in the European Union's platform economy.

The other main jurisdictions around the world are still deliberating whether to adopt similar economic regulations. The United States Congress is currently debating a series of Big Tech Bills, in particular, the American Innovation and Choice Online Act (AIOCA) which contains similar obligations to the DMA, in order to increase innovation and choice in the United States' digital economy, and the Open App Markets Act (OAMA), which is focussed on app stores. Additionally, the Chinese administration has put into consultation two important platform Bills, one to classify and the other to regulate big tech platforms.

It is interesting to observe that the European Union, United States, and Chinese laws and proposals show similarities in their objectives (promotion of innovation and choice), their scope (Big Tech), and their obligations (preventing anti-competitive conduct and reducing entry barriers to support the entry of new and smaller platforms). They also show some differences, in particular, in the use of detailed rules (in the European Union) or broader standards (in the United States and China), as well as the possibility to rely on an efficiency defence (in the United States) or not (in the European Union).[74]

3.2.1 Scope of pro-competitive regulation

The scope of pro-competitive regulation is generally determined by a combination of specific digital services and specific providers of those services.

The European Union's DMA applies to a closed list of ten digital services (the so-called 'core platform services') which have been identified because their characteristics may lead to market concentration, as well as dependency and fairness issues that cannot be addressed effectively by antitrust law. Then, only the providers of those services which meet a cumulative three-criteria test (the so-called 'gatekeepers') will be regulated; there is a rebuttable presumption that these gatekeeper criteria are met when some financial and user size thresholds are achieved.

[72] Petit (2020). For a sharp critique of the innovation rationale of the DMA, see Teece and Kahwaty (2021).
[73] Jenny (2021).
[74] For an EU-US comparison, see Schnitzer M. et al., (2021).

- The United States' AIOCA would apply to some platforms which provide three types of broadly defined digital services. Additionally, only the providers which meet very high financial and user size thresholds, and are critical trading partners for business users, would be regulated.
- The Chinese draft laws cover a large number of digital services grouped into 5 categories, each divided into several subcategories (for a total of 31 subcategories). Some obligations would only apply to the biggest platforms (so-called 'super platforms'), while others would apply to large platforms.

Table 3: Digital Services and Platforms in the Scope of Pro-Competitive Regulation

	European Union	United States	China
Digital Services	**Core Platform Services**[75] - Intermediation, incl. market place and app stores - Search engines - Social networks - Video-sharing - Instant messenger - Web browsers - Virtual assistants - Cloud computing - Operating systems - Online advertising	**Platforms**[76] - Website, online or mobile application, operating system, digital assistant, or online service that enable: - User generate content - Intermediation - Search **App Stores**	**Platforms**[77] - Online market[78] - Everyday services[79] - Social and entertainment[80] - Information[81] - Financial[82] - Computing applications[83]
Digital Platforms	**1. Significant impact on internal market**[84] - Annual European Union Turnover > € 7.5bn or Market cap > € 75 bn - and active in at least 3 Member States **2. Important gateway to reach end-users** - Monthly European Union active end-users > 45m	**1. Financial size**[85] United States revenue or Market cap > USD 500 bn (€ 501 bn) **2. User size** - Monthly United States active end-users > 50m	**1. High economic value** Market cap >1tr (€ 144 bn) for super large > 100bn RMB (€ 14bn) for large **2. Large user scale** Yearly Chinese active users > 500m / 50 m

[75] DMA, Article 2(2).
[76] AIOCA, Section 2(h8).
[77] Draft Guidelines for Internet Platforms Categorization and Grading.
[78] Include comprehensive goods trading, vertical goods trading and supermarket group-buying.
[79] Include transit services (such as bike shares), ride-hailing, travel services, delivery category (such as take-out dining), home management category as housekeeping, home rental and sales.
[80] Include instant messaging, gaming and leisure, audio-visual services, video streaming, short videos and literature.
[81] Include news portals, search engines, user generated content, audio-visual information, news organizations.
[82] Include comprehensive financial services, payment and billing, consumer finance, financial information, securities investing.
[83] Include intelligent terminals, Operating systems, Mobile phone application (APP) software, information management, cloud computing, network services, industrial Internet.
[84] DMA, Article 3(1) and (2).
[85] AIOCA, Section 2(h4). The OAMA would apply to app sores with more than 50m US users: Section 2(3).

	- and Yearly European Union active business users > 10 000 **3. Entrenched and durable**	- or Yearly European Union active business users > 100 000 **3. Critical trading partner**	**3. Strong restrictive ability**

It is interesting to note that laws and draft laws of the European Union, United States, and China follow the **same two-step process to determine their scope of application**.

- The first step is a closed list of legally defined digital services; the Chinese draft contains the longest list (hence has the broadest scope of application), while the United States' drafts have the shortest list;
- The second step is a combination of financial and user size thresholds, with gatekeeping power criteria to designate the regulated platforms. Here, the European Union has the lowest criteria (hence the broadest scope of application), while the United States has the highest criteria.

None of the three regimes rely on antitrust methodologies to identify the platform power which triggers regulation. Indeed, the first step (legal delimitation of services) replaces the definition of relevant markets, and the second step (identification of large gatekeepers) replaces the dominance assessment.

It is also interesting to note that **the concept of 'gatekeeper power' is close, albeit not identical, to the concept of 'major supplier' used in the WTO Reference Paper of 24 April 1996 on telecommunications services**.[86] In this paper, a major supplier is defined as a "supplier which has the ability to materially affect the terms of participation (having regard to price and supply) in the relevant market for basic telecommunications services as a result of: (a) control over essential facilities;[87] or (b) use of its position in the market."

3.2.2 Prohibitions and obligations

The (adopted and drafted) pro-competitive regulations contain a **list of more or less detailed prohibitions and obligations** imposed on the regulated platforms. To understand the underlying economic logic of those obligations and facilitate the comparison between jurisdictions, Table 4 clusters them into three categories: (i) prevention of anti-competitive conduct, in particular, leverage from one service to another, (ii) facilitation of users mobility in order to decrease entry barriers on the demand-side, and (iii) opening access to platforms and gatekeepers' data in order to decrease the entry barriers on the supply-side.

[86] See: https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm. On this Reference Paper, see Bronckers and Larouche (1997). It has been adopted in full or in part by 61 countries.

[87] Essential facilities are defined as "facilities of a public telecommunications transport network or service that (a) are exclusively or predominantly provided by a single or limited number of suppliers; and (b) cannot feasibly be economically or technically substituted in order to provide a service."

Table 4: Obligations Imposed on Regulated Platforms

	European Union	United States	China
Prevent anti-competitive conducts, *in particular leverage*	- Prohibition tying[88] - Prohibition self-preferencing in ranking[89] - Prohibition of use of third-party data[90] - Prohibition combine personal data without user consent[91]	- Prohibition self-preferencing[92] - Prohibition of use of third-party data[93]	- General prohibition of anti-competitive and unfair conducts[94] - Prohibition self-preferencing[95] - Prohibition combine personal data without user consent[96]
Reduction of entry barriers on demand side: *Facilitating business and end users switching and multi-homing*	- Prohibition MFN clauses[97] - Prohibition against anti-steering and anti-disintermediating clauses[98] - Prohibition against disproportionate conditions to terminate service[99] - Prohibition to limit to user complaints to public authorities[100] - Obligation to ensure that it is easy to install apps or change defaults[101] - Obligation to ease data portability[102]	- Prohibition MFN clauses[103] - Prohibition to use platform in-app payment[104] - Retaliation in case user complaints to public authorities[105] - Prohibition of additional restrictions for uninstalling software, search or ranking functionality[106]	

[88] DMA, Articles 5(7) and 5(8).
[89] DMA Article 6(5).
[90] DMA, Article 6(2).
[91] DMA, Article 5(2).
[92] AIOCA, Sections 2(a1) and (b6); OAMA, Section 3(e) for ranking in app.
[93] AIOCA, Section 2(b3); and OAMA, Section 3(c).
[94] Chinese draft platforms law, Articles 16 and 17.
[95] Chinese draft platforms law, Article 2.
[96] Chinese draft platforms law, Article 18.
[97] DMA, Article 5(3).
[98] DMA, Articles 5(4) and (5).
[99] DMA, Article 6(13).
[100] DMA, Article 5(6).
[101] DMA, Articles 6(3) and 6(6).
[102] DMA, Article 6(9).
[103] OAMA, Sections 3(a2) and (a3).
[104] OAMA, Section [to confirm].
[105] AIOCA, Section 2(b7).
[106] AIOCA, Section 2(b5).

Reduction of entry barriers on supply side: *Opening platforms and data*	- Obligation of vertical and narrow horizontal interoperability[107] - Access to data for business users and data sharing among search engines on FRAND terms[108] - Fair, reasonable and non-discriminatory (FRAND) access to app stores, search engine, social networks[109]	- Obligation of interoperability[110] - Access to data for business users[111]	- Obligations of interoperability[112] - Prohibition of unreasonable fee to access platform[113]

While the DMA contains the longest list of obligations (with some drafted in a more detailed manner than the United States or Chinese proposals, hence giving them a narrower scope of application), it is striking to note that several obligations are very similar in at least two regimes. Also, **two obligations are mentioned in the three regimes: the prohibition of self-preferencing and the obligations of vertical and horizontal interoperability**.[114]

Interestingly, **those two obligations were also imposed by the WTO Reference Paper on telecommunications services**. The Reference paper contains a series of six commitments related to competitive safeguards, interconnection, universal service, public availability of licensing criteria, independence of regulatory agencies, and allocation and use of scarce resources. In particular,

- the first commitment prohibits anti-competitive conduct,[115] specifically through cross-subsidisation across different services, use of information obtained from competitors with anti-competitive results, and refusal to give access to key infrastructure;
- the second commitment imposes interconnection arrangements that are non-discriminatory, cost-oriented, transparent, and subject to dispute resolution.

Although telecommunications operators and digital platforms show many differences in terms of business and innovation models, it would be interesting to know whether some obligations which were imposed on the telecommunications operators to increase competition and innovation, would have the same effects on the platform economy. If this is the case, then the global legal technique which was used to impose those obligations in the telecommunications sector may also be appropriate for the platform sector.

[107] Respectively. DMA, Article 7 for horizontal interoperability and Articles 6(4) and 6(7) for vertical interoperability, including side loading.
[108] DMA, Articles 6(10) and 6(11).
[109] DMA, Article 6(12).
[110] AIOCA, Section 2(b1), OAMA, Section 3(d).
[111] AIOCA, Section 2(b4).
[112] Chinese draft platforms law, Article 3.
[113] Chinese draft platforms law, Article 29.
[114] On the usefulness of imposing interoperability obligations, see Bourreau et al., (2022) and Scott Morton et al., (2021).
[115] It is interesting to note that the WTO Reference Paper contains a competitive assessment of the conduct, whilst this is not the case of the DMA.

Global Convergence Potential

There is an international recognition that **digital platforms have brought enormous benefits** to the global economy and society, they have been extremely innovative, and continue to have huge innovative potential that should not be undermined by ill-advised public intervention. At the same time, there is a growing international consensus that the specific features of the platform economy led to important **concentrations of economic and informational power, which should be kept in check** to ensure that innovation and user choice are maintained and maximised.[116]

There is also a growing international consensus that **antitrust policy is an important tool to control the power of the biggest digital platforms, and that antitrust law and practice need to be adapted to the specific characteristics of the platform economy**. Two international fora, the OECD and the ICN, are important places to exchange best practices and find the best way to adapt antitrust methodologies**.**

Antitrust enforcement may also need to be strengthened. To be effective, this will require a close international co-operation among antitrust agencies because, on the one hand, cases tend to be transnational as the biggest digital platforms are global and, on the other hand, authorities are still learning 'on the job', hence exchange of experience of each agency can accelerate the learning curve of all. Therefore, the co-operation on digital cases among antitrust agencies needs to be strengthened and, as already indicated above, to allow a robust exchange of information (even confidential) among agencies. Such co-operation is particularly important for merger control, as merger remedies tend to be non-divisible and, particularly merger prohibitions, even though imposed by one antitrust agency, tend to be implemented globally.

The next policy question, which is still very much debated in most countries, is whether an adapted and strengthened antitrust framework is enough to deal with platform power, or **whether pro-competitive regulation is needed as a complement**. Several jurisdictions across the world (such as the United States, China, United Kingdom, Australia, South Korea and Japan) are seriously considering the adoption of such regulation, but, at this stage, only the European Union has adopted such a law. Thus, the experience in implementing the European DMA should be closely watched to determine whether such pro-competitive regulation is necessary and effective.

If in the future other countries decide to follow the European path, then, on the basis of the draft laws reviewed in this report, a global consensus could emerge on the:

(a) objectives of such regulation, which are the **promotion of market contestability, innovation, and user choice**;

[116] See, for instance, the G7 Digital Ministers Declaration of 11 May 2022, at paragraph 25: "Competitive digital markets have demonstrated potential for innovation and strong, sustainable, inclusive growth of the global economy. We also recognise the need for effective competition policy instruments in view of dynamic developments in digital technologies and markets, and that new or updated regulatory and competition frameworks that address competition concerns raised by online platforms may be required to complement or adjust the existing competition policy instruments. This may be particularly important in connection with safeguarding contestability and fairness."

(b) scope of such regulation, which would only apply to **very large gatekeeping platforms providing digital services prone to market concentration;** and

(c) imposed obligations, which would **prohibit anti-competitive discrimination or leveraging, and encourage more interoperability**.

Interestingly, both obligations have already been imposed on the major telecommunications suppliers by the 1996 WTO Reference Paper for telecommunications services. If in the future, pro-competitive regulation proved to be beneficial for consumers, and an international consensus could be reached on the imposition of these obligations for the major digital platforms, then the same global technique could be followed by agreeing within the **WTO, on a new Reference Paper for digital platforms**.

In the hypothesis that more jurisdictions would adopt pro-competitive regulation, it would be appropriate that **close co-operation is organised among the (national and regional) regulatory agencies** in charge of such regulation, for the same reasons mentioned above, in favour of a strengthened co-operation among antitrust agencies: the transnational effect of most of the regulatory interventions, and the need to learn from others' experiences. Ideally, such co-operation should be set up and organised from the very beginning of implementing this new regulatory regime, with the establishment of an international network of digital regulators. In that regard, the model followed by the banking regulatory agencies with the *Basel Committee on Banking Supervision* (BCBS)[117] could be an interesting example to follow.

[117] See: https://www.bis.org/bcbs/

4. REDUCING ILLEGAL AND HARMFUL CONTENT

The **secondary liability exemption,** or immunity for illegal content and products, that is granted to digital platforms under some conditions, is the cornerstone of online content regulation. Limiting the liability risk contributes to platform growth and limits private censorship or over-removal of online content. This exemption can be found in many countries,[118] for example, the European Union, the United States, and China. [119]

Such a liability exemption is, in general, complemented by an **obligation to co-operate with administrative and judicial authorities** to remove illegal content when ordered to do so by those authorities.[120] In those cases, the platforms are co-enforcers of the law together with public authorities in the cyberspace they control. However, the liability exemption may lead to the under-removal of illegal content and products, which can be very harmful to society given the growth and size of some platforms. This is why several countries are imposing – or envisaging to impose – **due diligence obligations that complement this exemption and are proportionate to the risks caused by the dissemination of illegal content or products**.

With reference to content moderation, the European Union is also the first jurisdiction in the world to adopt a comprehensive online content moderation regulation with the Digital Services Act (DSA), which includes proportionate due diligence obligations. In particular, the DSA imposes at the European Union level, the establishment of a robust notice and take-down process for digital platforms, allowing their users or trusted flaggers to easily notify any illegality to the platforms and, on that basis, obliging the platforms to swiftly remove such content, while allowing the person having uploaded the content to contest the notification.[121]

In China, the draft platform law also foresees the imposition of an effective content moderation system that avoids the spread of illegal content and includes a notice and take down process (it is however less thorough than the one imposed by the European DSA).[122]

In the United States, the Congress and States are divided on the reform of Section 230 of the Communications and Decency Act. Some, mostly Democrats, want to follow the European path and impose more content moderation obligations on platforms in order to reduce the dissemination of illegal content online.[123] On the other hand, others, mostly Republicans, want to limit the content moderation rights of platforms in order to alleviate private censorship by platforms perceived as having a bias against conservative views.[124]

---

[118] Grasser and Schulz (2015).
[119] In the EU: e-commerce Directive, Articles 12-15 which will be replaced by DSA, Articles 3-6; in the US: Section 230 of the Communications and Decency Act; in China: E-Commerce law of 31 August 2018, Articles 37-38.
[120] DSA, Articles 8-9; Chinese draft platforms law, Article 34.
[121] DSA, Articles 15-15 and 19.
[122] Chinese draft platforms law, Article 12.
[123] For instance, the PACT Bill, Section 5(c). Some academics are also advocating for more due diligence obligations: Citron (2022).
[124] For instance, the Stop the Censorship Act: https://www.congress.gov/bill/116th-congress/house-bill/7808

It is also interesting to note that **content moderation obligations tend to be stricter when the potential harm created by the illegal content is higher, either because the content is more harmful or because the recipients are weaker**. In the European Union, several content-specific rules, which can be co-regulatory, impose stricter moderation obligations on the platforms: this is the case for terrorist content, child sexual abuse material, hate speech or disinformation, and fake news.[125] In most countries' online content laws, there is also additional protection for minors.[126]

Global Convergence Potential

It will be more **difficult to achieve global convergence on the regulation of online content moderation** than on the rules for transparency or competition and innovation, because content is more closely linked to societal values, therefore the heterogeneity of preferences across countries will be higher. However, some existing convergence across the European Union, United States and China (among others) is interesting to note:

(a) As already noted in Section 2, increased **transparency** on content moderation practices, conditions, and outcomes;

(b) The principle of **exemption of secondary liability** for illegal content online, even though the conditions for the exemption vary across countries;

(c) The obligation for platforms to **co-operate closely with public authorities** to co-enforce the content laws within their cyberspaces;

(d) The application of a **risk-based principle** in content moderation laws, with the imposition of stricter obligations for more harmful content (such as terrorist content) and weaker platform users (such as children).

Besides the convergence on regulatory principles, some jurisdictions have adopted – or are thinking of adopting – additional **due diligence obligations** in order to reduce the dissemination of illegal, or sometimes legal but harmful, content online. Those due diligence obligations, such as the establishment of a notice and take-down process to improve and speed up the removal of illegal content, complement (but do not replace) the liability exemption, which remains the cornerstone of the regulation of content moderation. Besides convergence on the process of content moderation, an international convergence on the outcome of the process, in particular on which content should be removed from platforms, would not be possible nor desirable given the important heterogeneity of preferences across countries. However, the **territorial effect of content removal orders** by public authorities is an issue which should be discussed within an international forum, as the orders are national, but their effects may be trans-national.

[125] On those rules, see de Streel and Ledger (2021). For terrorist content, see: Regulation 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online, OJ (2021) L 172/79; for child sexual abuses material, see: Proposal of the Commission of 11 May 2022 for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse, COM(2022) 209; for hate speech, see: Code of Conduct of May 2016 on Countering Illegal Hate Speech Online; for disinformation, see: Strengthened Code of Practice of 16 June 2022 on Disinformation.

[126] Chinese draft platforms law, Article 31.

5. ENFORCEMENT MODES AND INSTITUTIONAL DESIGN

The adoption of new rules to improve transparency, competition or content moderation is an easy step. What will be really challenging in the platform economy is to enforce those rules effectively because platforms are complex, ever-changing, and global. There are three main modes to enforce rules in the platform economy: (i) by regulatory agencies (public enforcement); (ii) by private stakeholders, for instance, the users or competitors of the platforms (private enforcement); and (iii) by the technology itself when rules are directly embedded in the design of the services provided or within the algorithms applied (technological enforcement). The balance between these three modes of enforcement varies across jurisdictions, depending on their regulatory culture and endowment. For instance, the European Union tends to favour public enforcement, while the United States tends to prioritise private enforcement.

5.1 Enforcement Modes

The first mode of enforcement is centralised and relies on public regulatory agencies. For this mode to be effective**, regulatory agencies need to combine the features of a 'good regulator,'** on which there is growing international consensus as shown by the OECD (2014):[127]

- First, the regulator should have **sufficient investigative and sanctioning powers** to perform their tasks adequately and be credible. Section 2 already discussed the importance of investigative powers to reduce the massive information asymmetry between regulatory agencies and regulated platforms. It is equally important that the regulator can act on this information and have sanctioning power with sufficient deterrent effects to incentivise regulatory compliance.
- Second, the regulator should have **sufficient human and financial resources** to effectively use its investigative powers to design appropriate remedies and sanctions. In particular, the regulator should have the human and technical capability to analyse and interpret the enormous volumes and variety of data provided by regulated platforms.[128] In turn, this requires that the regulator sets up in-house dedicated teams of data analysis and Artificial Intelligence (AI) specialists.[129] Going one step further, regulators may also develop their own AI tools to process the data, which is often referred to as *Suptech* and *Regtech*.[130] In practice,

[127] Recommendation of the OECD Council of 23 March 2012 on Regulatory Policy and Governance.
[128] For instance, during the *Google Shopping* antitrust investigation, the Commission had to analyse very significant quantities of real-world data including 5.2 Terabytes of actual search results from Google (around 1.7 billion search queries): Commission Press Release of 27 June 2017.
[129] For instance, the French authorities have set up the Pôle d'expertise de la régulation numérique, which offers digital expertise to the French regulatory administrations, while the French Competition Authority has established a digital unit: https://fr.wikipedia.org/wiki/P%C3%B4le_d%27expertise_de_la_r%C3%A9gulation_num%C3%A9rique In the United Kingdom, the CMA has set up a Data, Technology and Analytics (DaTA) unit.
[130] On this topic, also see the Conference organised by the Club of Regulators in co-operation with the OECD Network of Economic Regulators, *RegTechs: Feedback from the First Experiments*, available at: http://chairgovreg.fondation-dauphine.fr/node/708

AI techniques are increasingly used by financial regulators and are starting to be used by competition agencies.[131] And

- Third, the regulator needs to be independent. A basic level of independence relates to the relationship between the agencies and the regulated firms. To alleviate obvious conflicts of interest, the agencies need to be independent of the regulated platforms. A more sophisticated level of independence applies to the relationship between the regulator, the government, and the Parliament. Regulatory literature and experience show that this second level of independence improves regulatory outcomes as it increases the quality and credibility of regulatory decisions.[132] While there is an international consensus that regulators should enjoy the first level of independence,[133] there is no consensus regarding the second level of independence.

Another condition for effective public enforcement is that regulatory agencies have the **ability and incentives to deal with global firms and contribute to solving global challenges**. To maximise those abilities and incentives, the regulatory function should be placed at the same level as the regulated firms. However, several platforms are global, yet a global regulator is not politically feasible at this stage in time and may not even be the best level of governance, given the heterogeneity of preferences across countries. Therefore, the best option is to place the regulatory function at the highest level of each jurisdiction. The European Union took this approach with the DMA and the DSA, which will be enforced by the European Commission (for additional rules that apply to the very large online platforms and search engines), and not by the regulators of individual Member States. [134] The United States and China made the same choice in their platform bills which will be enforced by federal and state administration agencies, respectively. In addition, those (federal and state administration) regulators should closely co-operate with each other at the global level in order to match the global reach of the regulated platforms.[135] Therefore, the existing international networks of regulators, such as the International Competition Network (ICN), International Consumer Protection Enforcement Network (ICPEN)[136] or the Global Privacy Enforcement Network (GPEN),[137] should establish specific workstreams on digital regulation, and as indicated above, if digital regulators are established, an international network of such regulators should also be created.

Moreover, effective public enforcement requires, as recently shown by the ICN,[138] that **regulatory agencies should have a holistic view of the effects of regulated platform conduct, by integrating**

[131] See ICN report of 2021 on digitalisation, innovation, and agency effectiveness: https://www.internationalcompetitionnetwork.org/portfolio/digitalisation-innovation-and-agency-effectiveness-2021/ also see Schrepel (2021).
[132] Decker (2014), at pp. 189-222.
[133] See for instance, the WTO Reference Paper on telecommunications services which provides at point 5 that: "The regulatory body is separate from, and not accountable to, any supplier of basic telecommunications services. The decisions of and the procedures used by regulators shall be impartial with respect to all market participants." The Recommendation of the OECD Council of 23 March 2012 on Regulatory Policy and Governance, at paragraph 7 recommends that States: "develop a consistent policy covering the role and functions of regulatory agencies in order to provide greater confidence that regulatory decisions are made on an objective, impartial and consistent basis, without conflict of interest, bias or improper influence."
[134] Larouche and de Streel (2021) show that this will be a major change of the regulatory design in the European Union.
[135] Recommendation of the OECD Council of 10 June 2022 on International Regulatory Co-operation to Tackle Global Challenges.
[136] See: https://icpen.org/
[137] See: https://www.privacyenforcement.net/
[138] See: https://www.internationalcompetitionnetwork.org/portfolio/intersection-project-issues-paper/

analysis from antitrust, consumer protection, and data protection laws. This requires co-operation between the agencies in charge of these different legal instruments. This new form of co-operation is starting to emerge in some countries; one of the most developed examples is the United Kingdom's 'Digital Regulation Cooperation Forum' (DRCF), which includes the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), Ofcom and the Financial Conduct Authority (FCA).[139] A more radical alternative consists of integrating different authorities into a new platforms agency. In the United States, this has been proposed by the Digital Platform Commission Bill. [140]

While this form of inter-field co-operation or integration may not be easy within a country, the real challenge is to do it internationally, and ideally globally, to match the global level of the regulated platforms. A first attempt will be made in the European Union with the DMA High Level group, which is composed of five different European Union networks of national regulators.[141] This is a sort of 'squared' co-operation as it involves an inter-field co-operation between intra-field regulatory networks. If this experiment does not end up being a bureaucratic and Kafkian nightmare, it could serve as an example of similar co-operation at the global level.

Finally, public authorities should not be left to act alone, **enforcement needs to be participatory,** and this has two dimensions:

- First, **public agencies should be supported by regulated platforms** while being mindful of the risks of regulatory capture. In order to do that, platforms should establish internal compliance mechanisms (officers, reports, and so on).[142] Also, to ensure compliance, many rules discussed in this report may be enforced by punitive measures: it is expected that penalties provide specific and general deterrence. However, this expectation may not always work, even studies in the field of antitrust law (where penalties could be very high) suggest that these have limited deterrent effects. There may be some differences in detail depending on the economic activities and risks being managed, however, the academic literature on responsive regulation suggests that the key element of this approach is, to begin with, the assumption that firms wish to comply with the rules, and from that perspective, implementing a legal framework that facilitates an *ex-ante* design of compliance pathways. Participatory enforcement also means that platforms will support the authorities in enforcing rules against their users.
- Second, **public agencies should be supported by the business and end users** of the platforms while being mindful of the risks of opportunistic requirements and regulatory

[139] See: https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum
[140] See: https://www.congress.gov/bill/117th-congress/senate-bill/4201/text?r=15&s=3 This proposal is based on a report by Wheeler et al., (2021). In the European Union, Monti and de Streel (2022), at pp. 57-60, have also analysed the possibility of establishing a European Platform Agency.
[141] European Union DMA, Article 40: Body of European Regulators for Electronic Communications (BEREC), European Data Protection Supervisor (EDPS), European Data Protection Board (EDPB), European Competition Network (ECN), Consumer Protection Cooperation Network and the European Regulatory Group of Audiovisual Media Regulators (ERGA).
[142] European Union DSA, Article 32, and European Union DMA, Article 28; Chinese draft platforms law, Article 5.

dependency. In order to do that, users should be able to complain, even confidentially, to the authorities. They should also be consulted on the design and monitoring of remedies.

The second form of enforcement is decentralised and relies on private actors, either the competitors of the regulated platforms or their users, complaining before a Court that the platform violates the rules. To reduce the costs of these complaints and maximise the use of private enforcement, several regulations impose the establishment of **out-of-court dispute resolution mechanisms** on platforms, which appear to be ideally online. [143]

A third, and more radical, enforcement mode consists of **by-passing (or supplementing) the regulatory oversight by "coding" legal requirements directly into the algorithms**. Thereby, the legislative code is replaced (or supplemented) by computer code.[144] This is an interesting avenue to pursue as the progress of AI technologies offers more opportunities for such a model of compliance by design. Currently, some platform laws already impose such a model. [145]

However, two important safeguards and cautions are in order. First, not every legal requirement can be coded into an algorithm, in particular, because the legislative rule is often open and subject to interpretation, while computer code should be closed and not flexible. Open norms are a feature of the legal system, but imprecise code is a bug in computer programming. Second, the rules must ultimately be decided by an elected legislator and not by privately owned and managed digital platforms. Thus, it is only the closed rules which have been decided by an elected legislative body that could be programmed in code or algorithms.

5.2 Regulatory Principles

Together with the modes of enforcement, good enforcement principles are also key to ensuring the effectiveness of rules. There is an international recognition that compliance and enforcement should support the principles of good regulation in fast-evolving technologies and markets. Those principles are: [146]

- **Effectiveness** implies that any regulatory intervention achieves its declared objectives; this should be demonstrated for every intervention and monitored *ex-post* after the interventions.
- **Proportionality and risk-based approach** imply that the content and form of regulatory interventions should not exceed what is necessary to achieve the objectives of the

[143] European Union DSA, Articles 17-18.
[144] In the words of Lawrence Lessig (1999), the East Coast rules (the Congress) are replaced by the West Coast code (the Silicon Valley platforms).
[145] GDPR, Article 25(1): "Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." See for more details the Guidelines 4/2019 of the European Data Protection Board of 20 October 2020 on Data Protection by Design and by Default.
[146] On those principles, see Baldwin, Cave and Lodge (2012); Brownsword, Scotford and Yeung (2017); World Economic Forum (2020). In the European Union, see: Commission Staff Working Document of 3 November 2021, Better Regulation Guidelines, SWD (2021) 305.

legislation. At the enforcement stage, this principle implies that regulatory agencies should adopt risk-based enforcement and tailor their interventions to the risks created by the services provided by the regulated platforms.

- **Experimentality and adaptiveness** imply that the regulatory agencies learn from their experience and, over time, minimise Type I (over-intervention) and Type II (under-intervention) errors.[147] Experimentation can be done *ex-ante* before the adoption of a regulatory decision by running A/B testing of different types and designs of the intervention.[148] Such A/B testing may take place in different manners. One possibility is that regulatory agencies require, when necessary and proportionate, the regulated platforms to test different product changes with their users and report the results to the regulators, for them to decide the best course of action. Another possibility is to allow the regulatory agencies to access algorithms to analyse the outcomes delivered by them from different courses of action.[149] And
- **Innovation harnessing** implies that the regulatory intervention provides support for innovations at the design, proof of concept, and testing stages, or for the further ongoing development of existing innovative products and services. To achieve this, lawmakers may directly provide innovation exemptions or experimentation clauses in laws. Another possibility is that regulatory agencies offer 'regulatory sandboxes' to innovators, allowing them to experiment with new products or services with a temporary exemption from regulation.[150]

Global Convergence Possibilities

There are **three main modes of enforcing regulation**: (i) public enforcement, based on regulatory agencies which should ideally be participatory; (ii) private enforcement, based on private stakeholders; and (iii) technological enforcement when the legislative code is embedded within programming code. Those three modes are not exclusive, but complementary to each other, and the ideal combination depends on the regulatory culture and endowment of each country. Thus, there **is no 'one size fits all' approach that should be imposed at the global level, but a global conversation on each of these modes will improve enforcement in every country and eventually, globally**.

Regarding **public enforcement**, experience shows that regulatory agencies should have a number of features (power, resources, and independence) to be effective. Moreover, agencies regulating the

[147] In this regard, NESTA, a United Kingdom innovation foundation, calls for an 'anticipatory regulation' stating that: "When regulators have to take on new functions for which they lack an established playbook, or need to deal with uncertain market developments, a flexible, iterative learning approach is needed rather than a 'solve-and-leave' mentality. Where regulations are being developed for a new area or introduce substantial changes, it is difficult to know exactly what the impacts will be. Utilising a more experimental, trial and error approach, at least at the beginning, rather than immediately creating definitive rules can help build evidence on what works to achieve the desired outcomes. Standards, testbeds/sandboxes, or exhorting best practice are different ways in which regulators can provide more flexible interventions." Armstrong et al., (March 2019), "Renewing regulation 'Anticipatory regulation' in an age of disruption", NESTA, at p.27.

[148] One of the advantages of digital technologies is that such experiments are less costly to run than before and indeed, online platforms now commonly run A/B testing before launching new products or services.

[149] Parker, Petropoulos, and Van Alstyne (2021).

[150] Recommendation of the OECD Council of 6 October 2021 for Agile Regulatory Governance to Harness Innovation.

same legal fields should co-operate at the international level to have sufficient abilities and incentives to deal with global platforms, and not try to solve global problems from a national lens. Thus, existing international networks of regulators should co-operate on the enforcement of platform regulation. Agencies should also co-operate across legal fields in order to have a holistic view and come up with holistic solutions to tackle platform power, which is multi-faceted. Finally, such enforcement should be participatory and public agencies should orchestrate an 'ecosystem of compliance and enforcement' which involves all stakeholders (consisting of regulated platforms, platform users, Non-Governmental Organisations, civil society, and so on).

Regarding **private enforcement**, a global dialogue could be organised to exchange best practices and facilitate cross-border private enforcement.

Finally, **technological enforcement** is only embryonic at this stage, but may develop as technologies, in particular AI, progress. International co-operation in research and the exchange of best practices could be very useful at this stage.

In addition, there is growing international recognition that compliance and enforcement should abide by a number of **good regulatory principles,** such as: effectiveness, proportional and risk-based approaches, being adaptive, and innovation friendly. Several of these principles are already part of the constitutional frameworks of many countries around the world. These **principles should be monitored and their implementation discussed by international organisations involved in platform regulation**. Moreover, any international agreements on platform regulation should comply with these principles.

REFERENCES

Australian Competition and Consumer Commission, (2019), *Digital Platforms Inquiry: Final Report*.

Alexiadis P. and de Streel A., (2020), 'Designing an EU Intervention Standard for Digital Platforms', EUI Working Paper-RSCAS 2020/14.

Baldwin R., M. Cave, M. Lodge, (2012), *Understanding Regulation: Theory, Strategy and Practice*, 2nd ed, Oxford University Press.

Baron J., J. Contreras, M. Husovec and P. Larouche, (2019), 'Making the Rules: The Governance of Standard Development Organizations and their Policies on Intellectual Property Rights', JRC Report.

Bietti E., (2021), A Genealogy of Digital Platform Regulation, available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3859487

Bourreau M., Krämer J. and M. Buiten, (2022), Interoperability in digital markets, CERRE Report available at: https://cerre.eu/publications/interoperability-in-digital-markets/

Bradford A., (2020), 'The Brussels Effect: How the European Union Rules the World', Oxford University Press.

Bronckers M. and P. Larouche, (1997), 'Telecommunications services and the WTO', *Journal of World Trade*, Vol. 31(3), pg. 5.

Brownsword R, E. Scotford and K. Yeung – eds, (2017), *The Oxford Handbook of Law, Regulation and Technology*, Oxford University Press.

Citron D. K., (2022), 'How to fix Section 230', University of Virginia School of Law: Public Law and Legal Theory Research Paper Series 2022-18.

Cusumano M.A., A. Gawer, D.B. Yoffie, (2021), 'Can Self-Regulation Save Digital Platforms?' *Industrial and Corporate Change* 30, pp. 1259–1285.

Cohen J., (2019), 'Between Truth and Power', Oxford University Press.

Crémer J., de Montjoye Y. A. and Schweitzer H., (2019), 'Competition Policy for the Digital Era', Report to the European Commission.

Decker C., (2014), *Modern Economic Regulation: An Introduction to Theory and Practice*, Cambridge University Press.

de Streel A. and M. Ledger, (2021), 'Regulating the Moderation of Illegal Online Content', in European Audiovisual Observatory, *Unravelling the Digital Services Act package*, Iris Special, pp. 20-40.

de Streel A. and M. Husovec, (2020), 'The e-Commerce Directive as the Cornerstone of the Internal Market', Study for the European Parliament.

Finck M., (2018), 'Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy', 43 European Law Review, pp. 47-68

Fletcher A., (2022), 'Pro-Competition Regulation of Digital Platform: Are Divergent Approaches Healthy Experimentation or Dangerous Fragmentation', Oxford Review of Economic Policy, forthcoming.

Furman J., D. Coyle, A. Fletcher, D. McAuley and P. Marsden, (2019), 'Unlocking Digital Competition', Report of the Digital Competition Expert Panel.

Galloway S., (2018), 'The Four: The Hidden DNA of Amazon, Apple, Facebook and Google', Corgi.

Grasser U. and W. Schulz, (2015), 'Governance of Online Intermediaries Observations From a Series of National Case Studies', Berkman Center Research Publication, 2015-5.

Internet & Jurisdiction Policy Network, (2019), 'Internet & Jurisdiction Global Status Report 2019'.

Jacobides M. G., C. Cennamo and A. Gawer, (2018), 'Towards a theory of ecosystems', Strategic Management Journal, Vol. 39, Issue 8, pp. 2225–2276.

Jenny F., (2021), 'Competition law and digital ecosystems: Learning to walk before we run', Industrial and Corporate Change, Vol. 30, Issue 5, pp. 1143–1167.

Keller D., (2021), 'Amplification and Its Discontents', Knight First Amendment Institute, Columbia University.

Krämer J. and Schnurr D., (2022), 'Big Data and Digital Markets Contestability: Theory of Harm and Data Access Remedies', Journal of Competition Law & Economics, Vol. 18, Issue 2, pp. 255–322.

Lancieri F. and Morita Sakowski P., (2021), 'Competition in Digital Markets: A Review of Expert Reports', Stanford Journal of Law, Business & Finance, Vol. 26, Issue 1, pp. 65-170.

Larouche P. and de Streel A., (2021), 'The European Digital Markets Act: A Revolution Grounded on Traditions', Journal of European Competition Law & Practice, Vol. 12, Issue 7, pp. 542–561.

Lessig L., (1999), 'Code and Other Laws of Cyberspace', Basic Books.

Marco Colino S., (2022), 'The Incursion of Antitrust into China's Platform Economy', Antitrust Bulletin Vol. 67, Issue 2, pp. 237– 258.

Mayer-Schonberger V. and T. Ramge, (2018), 'Re-inventing Capitalism in the Age of Big Data', John Murray.

Monti G. and de Streel A., (2022), 'Improving Institutional Design to Better Supervise Digital Platforms', CERRE Report.

OECD, (2014), 'The Governance of Regulators'. Available at: https://doi.org/10.1787/9789264209015-en

OECD, (2022), 'Handbook on Competition Policy in the Digital Age', available at: https://www.oecd.org/daf/competition-policy-in-the-digital-age/

Parker G., Van Alstyne M. and Choudary S.P., (2016), 'Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You', Norton and Company.

Parker G., Petropoulos, G., and Van Alstyne M., (2021), 'Platform Mergers and Antitrust', Industrial and Corporate Change, pg. 30.

Petit N., (2020), 'Big Tech and the Digital Economy: The Moligopoly Scenario'. Oxford University Press.

Riley C. and S. Ness, (2022), 'Modularity for International Internet Governance', available at: https://www.lawfareblog.com/modularity-international-internet-governance

Schnitzer M. *et al.,* (2021), 'International Coherence in Digital Platform Regulation: An economic perspective on the US and EU proposals', Yale Tobin Center of Economic Policy: Digital Regulation Project Policy, Discussion Paper 5.

Schrepel T., (2021), 'Computational Antitrust: An Introduction and Research Agenda', Computational Antitrust project at Stanford University, CodeX Centre (The Stanford Centre for Legal Informatics).

Scott Morton F., P. Bouvier, A. Ezrachi, B. Jullien, A. Katz, G. Kimmelman, D. Melamed, D. and J. Morgenstern, (2019), Committee for the Study of Digital Platforms: Market Structure and Antitrust Subcommittee, Stigler Center for the Study of the Economy and the State.

Scott Morton F. *et al.,* (2021), 'Equitable Interoperability: the "Super Tool" of Digital Platform Governance', Yale Tobin Center of Economic Policy: Digital Regulation Project, Policy Discussion Paper 4.

Teece D.J. and H.J. Kahwaty, (2021), 'Is the Proposed Digital Markets Act the Cure for Europe's Platform Ills? Evidence from the European Commission's Impact Assessment', Berkeley Research Group Institute.

US Congressional Research Service, (2021), 'Social Media: Misinformation and Content Moderation Issues for Congress'.

US House of Representatives, (2020), 'Investigation of Competition in Digital Markets: Majority Staff Report and Recommendations'.

Wheeler T., Ph. Verveer, Kimmelman G., (2021), 'New Digital Realities; New Oversight Solutions in the U.S.: The Case for a Digital Platform Agency and a New Approach to Regulatory Oversight', Harvard Kennedy School: Shorenstein Center Discussion Paper.

World Economic Forum, (2020), 'Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators'.

Wu T., (2018), 'The Curse of Bigness: Antitrust in the New Gilded Age', Columbia Global Reports.

Zhang A., (2022), 'Agility Over Stability: China's Great Reversal in Regulating the Platform Economy', Harvard International Law Journal, Vol. 63, Issue 2.

Zuboff S., (2019), 'The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power', Profile Books.

cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS

PROSPECTS FOR HARMONISATION OF GLOBAL DATA GOVERNANCE

JAN KRÄMER (editor)

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The academic workstream lead for this paper, Prof. Jan Kraemer, and his co-authors wish to thank the involvement and invaluable contribution to this paper of Mike Liu, Samuil Agranovich, Krissy Chapman, Grace Nyikes, Sadie O'Connor, Yaegy Park, and Jiaqi Tan.

cerre Centre on Regulation in Europe

01

RECOMMENDATIONS

Alice de Jonge
Anupam Chander
Moritz Hennemann
Jan Krämer
Mike Liu
Marcelo Thompson

1. INTRODUCTION

This report focuses on the convergence and divergence of international data flows, stressing that data is both an essential input for many industries, as well as a critical means for global communication and co-operation, and that major jurisdictions, such as the United States of America (USA), China, and the European Union (EU), have recently enacted or are in the process of enacting new data laws. The question arises whether there is a convergence between these laws, and if not, whether it is achievable or desirable, and where divergence will, and possibly should, prevail.

This report consists of four parts, in addition to this recommendation paper. In the first part, de Jonge (2022) conceptualises the issues emerging from the idea of a data commons across borders and jurisdictions and sets the scene for the three regulatory angles that are taken under consideration by the other parts. Secondly, Chander et al., (2022) consider convergence and divergence in personal data regulation across the jurisdictions, from the State of California, to the EU, and China. Thirdly, Hennemann (2022) addresses trade-offs and paths to convergence for non-personal data laws, an area for which convergence seems most promising from the outset because the flow of non-personal data is to date largely unregulated in these major jurisdictions. Lastly, Thompson (2022) considers the current scope and reasons for data sovereignty, as a central force that may counteract efforts for convergence and the free flow of data.

A number of policy recommendations emerge from this joint analysis, which are synthesised in this recommendations paper. In order to keep this paper concise, it cross-references the respective individual reports for a more detailed analysis and derivation of the conclusions which are presented herein. However, it largely refrains from cross-referencing other works (which are referenced in the individual reports). The recommendations are structured in four main areas. In Section 2, recommendations are made regarding data protection and privacy laws, and the global convergence of data protection and privacy regulation. In Section 3, recommendations are made on the free flow of non-personal data, and in Section 4, on ‘data sovereignty’. Finally, Section 5 considers institutional arrangements and fora at which convergence in data regulation can be discussed and advanced.

2. GLOBAL DATA PROTECTION AND PRIVACY LAW

As the workstream on digital trade observes (Low, 2022), the fracturing of co-operation which permits data flows reduces the benefits of digital trade. One key aspect of this fracturing is divergent personal data protection and privacy regimes.

A trend towards convergence among disparate jurisdictions in data protection and privacy regulation can be observed globally. For example, the laws of China, the European Union, and the State of California reveal—despite differences in personal scope and significant differences with regard to national security aspects—remarkable convergence (Chander et al., 2022). There is a significant core of shared legal norms across these leading jurisdictions. These include basic rights for individuals to access, correct, and delete personal information held by others, special protections for children and sensitive data, the right to data portability, data minimisation, data retention limitations, accountability for violations, and risk-based cybersecurity requirements (Chander et al., 2022). More study is nevertheless needed to understand what motivates the various greater and smaller divergences between data protection and data privacy laws across jurisdictions. Where some divergences may have cultural components—for example, the age of consent for children or the types of data considered "sensitive"—other divergences are more abstract and obscure and not readily ascribable to societal differences.

The global 'distribution' of data protection and privacy laws—as the *law in the books*—must also not overlook that it might not always be the *law in action*. Not every country enacting a Data Protection Law also installs an independent data protection agency—and generally, lacking enforcement is still a challenge in every part of the world—and the motivations for strict or less strict enforcement are manifold. More study is needed to evaluate and assess enforcement patterns across jurisdictions (for example, by the type of right that is alleged to be violated or by the kinds of violations that are most commonly enforced). It is an open question whether enforcement is typically focused on the failure of data security standards, excessive collection of information, use of information for improper purposes, the use of sensitive data, or restrictions on cross-border data flows. While many data protection authorities publish reports, including classification of enforcement actions by sectors and kinds of infringements, a more systematic study across jurisdictions would help inform global efforts for data privacy.

Nevertheless, against this background, two recommendations are made with respect to potential future instruments that may further facilitate the convergence of privacy laws.

Recommendation 1: International Agreement on (Minimum) Data Protection and Privacy Rules

> *An international agreement on (minimum) data protection and privacy rules is a medium-term goal that must be carefully evaluated with regard to a potential foreclosure of the 'market' for regulatory ideas.*

The existing convergence among disparate jurisdictions might be regarded as a basis for broader collaboration and interoperability—and might suggest there is a greater possibility for broad

international agreement on a minimum set of substantive and procedural data protection and privacy rules than what is commonly assumed (Chander et al., 2022).

In this regard, however, it must be noted that a great share of the existing convergence in data protection and data privacy law is linked to European regulation (EU Data Protection Directive (DPD) and EU General Data Protection Regulation (GDPR)). DPD- or GDPR-like laws can be spotted around the world (for examples see Hennemann, Lienemann & Spirkl, 2022). The first-mover advantage of the GDPR does not, however, necessarily mean that the GDPR is the most convincing data protection and privacy law to be followed in every setting. It must be noted that the GDPR might be an "easily transplantable regulatory model" (Schwartz, 2019), but it is not free of criticism from different angles (Gal & Aviv, 2020; Mannion, 2020). Despite its sensible aims, the GDPR model can indeed be linked to different conceptional shortcomings that should not be underestimated. It arguably starts with large entry gates (every processing of personal data) that lead to uncertainties (such as de-anonymisation) (Purtova, 2018). It comes along with large compliance burdens that are hard to bear—especially for smaller and medium-sized companies—and that rather favour bigger companies, which can more easily afford the compliance costs (Gal & Aviv, 2020). Generally, there is at least doubt as to its (negative) effects on an innovation environment. Further, conceptually it can be questioned whether a regulatory approach focussing on processing as such, is still practical and sensible with data flows being produced by every online user during every second. Risk-based and more targeted approaches might therefore be superior to broad input-based approaches.

Furthermore and because of this, other models of data protection and privacy regulation do exist and must be carefully evaluated (such as the Global Cross-Border Privacy Rules (CBPR) Declaration, the recent bipartisan draft of an American Data Privacy and Protection Act, and the United Kingdom's (UK) Data Protection Bill). To let the GDPR win the 'race' might also foreclose the market for regulatory innovations that might set a more risk-sensible and incentivising framework at the same time. This is more than necessary with a truly global view. And finally, and most importantly, the existing sets of data protections and privacy regulations do not always mirror the different cultural contexts and different social norms with regard to laws and rules, as well as to respective settings in the Global North, East, West, and South (Boshe, Hennemann & von Meding, 2022).

Recommendation 2: Model Law on Data Trusts

A model law on data trusts is a short-term goal to be pursued.

A model law on data trusts would seek to provide policymakers with a governance tool for the protection and responsible sharing of personal data. In so doing, it would address a blank spot to national approaches to data protection and privacy protection (de Jonge, 2022). The parties to the data trust would be the trustee, the data collector(s) and storers, and the beneficiaries—primarily the individuals whose personal data forms part of the data asset.

One prerequisite to EU participation in the establishment (or later acceptance) of a model law on data trusts would be modifying the GDPR to make room for the data trust model. The GDPR would need to be amended to empower the trustee to collect data from legitimate sources (in most cases the individual whose data is being collected). The trustee will also need powers to both use and empower

authorised third parties (not all of whom will be known at the time of data collection) to access and use the data. Other legal systems may also need consequential adjustments to existing laws before adopting a model law on data trusts.

Basic principles to be enshrined in a model law on data trusts would include (de Jonge, 2022): (1) The creation or appointment of a steward (trustee) to manage information and data (the trust asset) for specified purpose(s) to the benefit of beneficiaries; (2) principles governing de-identification of personal data and the protective measures built into data-collection software; (3) recognition of the changing nature of data and of the purposes for which it is used—this implies a recognition of the need for regular consultation and renegotiation of the trust terms; (4) rights of individuals who have contributed information to the data assets to be recognised as data beneficiaries and stakeholders—rights stemming from this recognition include the right to correct mistakes, the right to access personal data, the right to request deletion of personal data and the right to data portability, should an individual wish to transfer to or share custodianship of their data with a different trust; and (5) transparency in relation to users of de-identified personal data packages and the uses to which such data is put.

Data trusts are not a silver bullet, and there are forms and uses of personal data not suited to data trust arrangements. The model law recommended here is intended for adoption and adaptation, to specific national and regulatory contexts. It provides a useful public policy tool aimed at facilitating the sharing and transfer of data for specific public benefit uses (de Jonge, 2022). Examples include medical data trusts, aimed at facilitating research for promoting public health goals, environmental data trusts, aimed at promoting research collaborations with sustainable ecology goals, and public transport-use data, used for research into energy conservation and infrastructure-efficiency goals.

It is also noted that Recommendations 1 and 2 could be tackled jointly by policymakers: A global instrument on data privacy for personal information could include a section on data trusts which signatory states could opt out of if they are not ready for it, or if policymakers felt it was not suited to the domestic legal system.

3. PROSPECTS OF GLOBAL NON-PERSONAL DATA REGULATION AND HARMONISATION

Non-personal data regulation is underlying different parameters as personal data regulation. After a long period of no regulation specifically targeted at non-personal data, current regulatory activities mark a turning point in this regard (such as the EU Data Governance and Data Acts). Despite the current set of rules in many countries, one should, however, not (continue to) see non-personal data and personal data as two fundamental separate spheres. It is rather preferable to construct data regulation with regard to the respective ecosystems involved. National security data (either personal or non-personal) underlies fully different parameters than (personal or non-personal) data trade. Therefore, it must be stressed that it is of utmost importance to find the 'right' conceptual entry gate to data regulation—as the central pillars of data regulation shape any regulatory instrument built thereon (Hennemann, 2022).

Any non-personal data law instrument should define—in line with the G7 digital ministers—a trusted free flow of data as the conceptional starting point. It should be targeted at facilitating data use, promoting data markets, removing barriers to entry data markets, and countering (contractual) imbalances. Data law regulation should especially refrain from establishing an absolute right or an Intellectual Property (IP) right in non-personal data, to promote data sharing and data reuse on the one hand, and to avoid anti-competitive effects on the other hand (Hennemann, 2022). Data law should rather focus on building trust in data flows. A respective trust is only possible by a combination of a sensible institutional framework and a convincing substantial setting (Hennemann, 2022). With regard to the latter, the data economy is inconceivable without trusted actors as set out before (such as data intermediaries, data commons, and data trusts). Regarding substance, data law regulation must take transparent decisions about data monetisation and participation in data-generated value. Data regulation seems to be most convincing if it values the role of the person "producing" the data and should set incentives for enablers and users of data markets (Hennemann, 2022). Data law regulation should mirror the specific needs of small and medium-sized companies, especially the transaction and implementation costs that come along with regulation. Data regulation must carefully weigh the safeguards for fundamental rights against those for trade secrets, as well as consider the (anti-)competitive effects of proposed legislation (Hennemann, 2022).

Two potential future instruments will be presented against this background.

Recommendation 3: International Agreement or Soft Law on Non-Personal Data Contract Rules

> *A soft law on non-personal data contract rules should be a short-term goal to be pursued, while an international agreement on non-personal data contract rules should be a medium-term goal to be pursued.*

An international non-personal data law instrument should be considered a realistic goal. Non-personal data is not as 'culturally determined' as data protection and privacy laws. Unlike personal data, non-personal data is an informational good that is and can be traded between private parties without

fundamental constrains. Non-personal data should therefore be regulated mainly by means of 'enabling' contract law (Hennemann, 2022). Any exchange should—as a general rule—be linked to private-to-private interactions. Such interactions may be framed and incentivised by contract law instruments. In this regard, regulation should at least include non-binding standard terms for data contracts. Non-personal data law regulation might also consider contractual default rules for data contracts, mandatory standard terms and unfair contract terms *vis-à-vis* small and medium-sized enterprises and consumers, instruments boosting competitive data markets (such as access rights), data location and data transfer rules in specific cases, as well as specific rules regarding the access and use of specific research institutions and governmental actors (Hennemann, 2022). In addition, rules on data trusts and intermediaries facilitating data contracts, are also a road to follow in this regard (see above, as well as the EU Data Governance Act on data intermediaries).

Furthermore, before coming to an international agreement, a non-binding soft law instrument should be promoted (Hennemann, 2022). Different preparatory work for a respective instrument has already been done. Specifically, model laws and contract rules can serve as catalysts for data markets.

Recommendation 4: International Global (Framework) Agreement on Data Commons

> *A medium-term goal to be pursued, is an international global (framework) agreement on data commons.*

Furthermore, it is suggested to consider an instrument recognising global data commons as well as the nature of non-personal data as a non-rivalrous and non-exhaustive public good with multiple uses. Global commons typically embrace concepts of inclusive governance and equitable access as well as the promotion of the common good and sustainable economic development (de Jonge, 2022). These goals imply facilitating data flows and access to data by promoting different forms of public-private partnerships, data altruism, data-sharing, and data pooling arrangements —in line with the criteria set out above. Inevitably, where data sharing occurs across national boundaries, states are likely to raise security concerns and are likely to remain reluctant or unwilling to allow certain forms of data to be shared internationally. Existing global commons instruments (such as governing the high seas and outer space) recognise that sovereign actors have security interests that they wish to protect. An international instrument on data commons will most likely contain similar provisions, placing restrictions on data sharing and access arrangements (de Jonge, 2022; Thompson, 2022). Political negotiation will no doubt play a role in the final shape of any internationally negotiated balance between implementing the recommendations made above regarding data localisation and data transfers and realising the goals of a global data commons. Rules regarding transparency of local laws and participation in the global data commons will play an important role in reaching this balance.

It is noted that Recommendations 3 and 4 could also be pursued together in one global instrument, which could embrace concepts of a global data commons together with standards for access to and exchange of non-personal data.

4. DATA SOVEREIGNTY AND HUMAN RIGHTS

Institutional mechanisms must be conceived to enable agreement on how values stemming from different cultural traditions will find their way into the governance of global data flows (Thompson, 2022). While such mechanisms must provide avenues for the identification of evaluative perspectives deemed unacceptable, they must also recognise the diversity of acceptable ones and the role of nation states in affirming and furthering those of importance within their respective jurisdictions. Global data governance initiatives must recognise, in other words, the reality of digital sovereignty (Thompson, 2022; de Jonge, 2022).

Data localisation policies are one realm where such a recognition must take place. At the same time, it is also crucial to see that policies such as these are not arbitrarily implemented and, more broadly, that they comply with international commitments, as informed by the mechanisms proposed here, in the pursuit of values of national (or supranational) importance. Initiatives such as the European Gaia-X project and the International Data Spaces project, can be stressed as positive examples to establish a sovereign infrastructure for the sharing of data within different data spaces in the Digital Single Market. While data localisation initiatives often raise technical concerns, being associated with the demise of the Internet as we know it, initiatives such as these point to the possibility that data flows may be preserved in a way that enables sovereign values to be upheld (Thompson, 2022; compare also Hennemann, 2022). More specifically, these approaches avoid technological determinism in thinking about human values in the context of harmonisation processes. Harmonisation initiatives should reflect human values, rather than seek to assimilate human values to assumedly immutable configurations of technological processes (Thompson, 2022).

Recommendation 5: International Agreement on Human Rights Aspects Concerning Data Governance

> *A long-term goal to be pursued, is an international agreement on human rights aspects concerning data governance.*

On this basis and to fulfil this promise, an international agreement on human rights aspects concerning data governance should be considered. This proposal endorses and expands on existing ones in the literature, of a global privacy agreement under the WTO system—or, more broadly, of a new Digital Bretton Woods agreement. At the same time, however, it addresses a central challenge of data governance harmonisation initiatives, which is the indeterminacy of normative standards at the heart of data governance regimes—variations, that is, not only in relation to legal rights, but as to the zones of indeterminacy that characterise the boundaries of, and exceptions to those rights (Thompson, 2022). Around a right to data protection, one finds ideas of the adequacy of third-country data protection regimes, legitimacy of processing, and public interest in the processing, among others, which can be said to make up for hard cases in relation to the interpretation of the contours of a data protection right. If one places data governance regimes in the context of international trade agreements, other zones of indeterminacy emerge, in the form of general exceptions to obligations

agreed upon under such agreements—this is the case, for example, with the public morals exception in Article XX GATT and Article XIV GATS (Thompson, 2022).

These are questions profoundly related to debates on data sovereignty—they are, indeed, central to cases of such debates, since it is here that one can see at its strongest the endeavour of different global communities to identify and affirm the values upon which the authority of their political systems is founded. Yet, ideals of liberal neutrality around which trade regimes gravitate have difficulty in dealing with the substance of public morals questions (Thompson, 2022). Laudable though the goals of the international trade system certainly are, WTO dispute settlement bodies are just not the ideal fora to decide on the substance of questions that overlap so intensely with the value systems of different global communities (Thompson, 2022). In a way, the international trade system is a response precisely to the indeterminacy of questions concerning such value-systems, but a response that transforms such questions, if not fully into externalities, at least into exceptions to be thoroughly justified—whereas the international human rights system does the same, and with much more credibility given its guardianship of the coherence or integrity of rights of a fundamental nature, in relation to the international trade system.

This clash between necessities—the utilitarian necessity of unfettered trade and the deontological necessity of human rights—will only get accentuated as data governance questions unfold. There is just no way around it that does not involve urgent and cross-cultural dialogue around the boundaries of human rights commitments concerning international data flows (Thompson, 2022).

5. ALLIANCES AND INSTITUTIONAL MECHANISMS

Discourse platforms are necessary for the different dialogue processes to take place, as set out above.

Recommendation 6: International Instalment Agreement on Human Rights Aspects Concerning Data Governance

> *A multilateral human rights body on data sovereignty, ideally within the United Nations system, should be a short- to medium-term goal to be pursued and should be set on the basis of an instalment agreement (which should not be an agreement on the substance of different normative standards but should rather be a procedural agreement in scope).*

Decisions on human rights questions could be subjected to a multilateral body in the human rights realm, ideally within the United Nations system. A respective instalment agreement—to be acceptable and practical at this moment in time—should not be an agreement on the substance of different normative standards in data governance regimes but should be a procedural agreement in scope. It should be an agreement precisely to enable an earnest and open-minded engagement between different countries and traditions in seeking to ascertain the reasonable boundaries of their differences—the boundaries, that is, of what, while being socially acceptable in the context of a particular value system, cannot reasonably be accepted as a restrictive measure in an international context (Thompson, 2022).

Recommendation 7: Institutional Mechanism(s) to Facilitate Data Regulation

> *(An) institutional mechanism(s) aimed at facilitating data regulation, as well as cross-border learning and knowledge sharing, is a short-term goal to be pursued. This could include the establishment of a body of stakeholders and structural rules aimed at facilitating regional and other alliances (such as, the Global Committee, Alliance of Private Actors, an NGO-led forum, or a horizontal « Data 20 » (« D20 ») initiative).*

Further, institutional mechanisms aimed at protecting and facilitating data regulation, as well as cross border learning and knowledge sharing, could include the establishment of a body of stakeholders (sovereign, private and non-governmental non-profits) and structural rules aimed at facilitating regional and other alliances. Different options could be pursued (Hennemann, 2022) —either cumulatively or alternatively (such as, the Global Committee, Alliance of Private Actors, an NGO-led forum, or a horizontal « D20 » initiative).

Such an open forum could drive the development of data law regulations, models, and model laws with the objective to set minimum requirements and timelines (to enable all parties to embrace the framework). The quality of all instruments is highly dependent on the drafting process (Hennemann, 2022). In order to be accepted by all sides, it must be assured that instruments are drafted in a balanced way taking all sides and stakeholders into account. Clearly defined incentives will be essential to expedite the onboarding process for all actors (Hennemann, 2022).

REFERENCES

Boshe, P., Hennemann, M., von Meding, R. (2022). African Data Protection Laws – Current Regulatory Approaches, Policy Initiatives, and the Way Forward. 3(2) Global Privacy Law Review 56.

Chander, A., Agranovich, S., Chapman, K., Nyikes, G., O'Connor, S., Park, Y., & Tan, J. (2022). Convergence and Divergence In Global Data Privacy Law: Comparing The GDPR, PIPL, and CCPA. CERRE Policy Report.

de Jonge, A. (2022). Conceptualising Governance in the Digital Domain. CERRE Policy Report.

Gal, M., Aviv, O. (2020). The Competitive Effects of the GDPR. 16 Journal of Competition Law and Economics 349.

Hennemann, M. (2022). Non-Personal Data Governance: Facilitating Non-Personal Data Flows? CERRE Policy Report.

Hennemann, M., Lienemann, G., Spirkl, C. (eds.) (2022). Mapping Global Data Law. Part I: Data Protection Legislation. University of Passau Institute for Law of the Digital Society Research Paper Series No. 22-15.

Low, P. (2022). Building the Benefits of Digital Trade. CERRE Policy Report.

Mannion, C. (2020). Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets. 53 Vanderbilt Journal of Transnational Law 685.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. 10 Law, Innovation and Technology 81.

Schwartz, P. (2019). Global Data Privacy: The EU Way. 94 N.Y.U. Law Review 771.

Thompson, M. (2022). Digital Sovereignty and the Normativity of Data Governance. CERRE Policy Report.

cerre Centre on Regulation in Europe

02

CONCEPTUALISING GOVERNANCE IN THE DIGITAL DOMAIN

Alice de Jonge

1. INTRODUCTION

Data is a central resource of the 21st century, serving individual, collective, and commonwealth functions. Data and data ecosystems shape the competitiveness of commercial, non-commercial, and public actors alike. Relationships formed in the digital domain affect all our lives. Regulating such an ecosystem requires balancing the interests of stakeholders in the global data community. The term 'global data community' is used here to embrace all stakeholders in the data economy – including those (individuals and organisations) whose data is collected, actors engaged in the harvesting, storage, sharing or selling of that data, and those responsible for regulating the ways in which these activities are conducted.

Taking inspiration from Ostrom's framework for studying commons arrangements in the natural environment,[151] Frischmann et al., conceived of software sharing, data sharing, and other knowledge sharing environments as 'knowledge commons'; and developed a framework they called the Governing Knowledge Commons (GKC) framework for studying governance arrangements in these environments.[152] It is not within the intention or scope of this study to examine the GKC framework in detail. Rather, this report draws inspiration from the GKC framework's understanding of knowledge as a Commons. The global digital data ecosystem can be understood as one type of knowledge commons, embracing online and other ecosystems within which digital, creative, and other knowledge resources are shared.

All knowledge commons need governance arrangements - a demand which arises from the community's need to overcome various social dilemmas associated with producing, preserving, sharing, and using information, innovative technology, and creative works.

Knowledge commons governance institutions and rules interact with, and are shaped by, the knowledge resources being created and shared. Governance institutions are also necessarily socially embedded within different geographical, historical, cultural, and political contexts. The GKC framework is therefore built around three pillars – knowledge resources, community attributes, and governance 'rules in use', as further explained below.

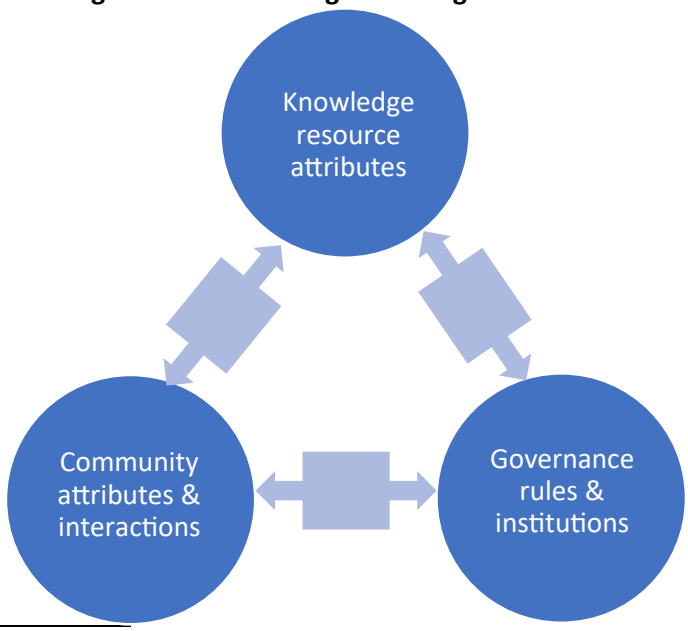
[151] Elinor Ostrom, *Governing the Commons: The evolution of institutions for collective action*. Cambridge University Press, (1990).

[152] Brett M. Frischmann, Katherine Jo Strandburg, Michael J. Madison (eds), *Governing Knowledge Commons*. (2014). United Kingdom: Oxford University Press. See also Michael J. Madison, Brett M. Frischmann, and Katherine J. Strandburg, Knowledge Commons, in Hudson, Blake, Rosenbloom, Jonathan, and Cole, Dan eds. *Routledge Handbook of the Study of the Commons* Abingdon, UK: Routledge. Schweik, Charles M. and Robert C. English. *Internet Success: A Study of Open-Source Software Commons*. MIT Press, Cambridge, MA (2012).

2. THE KNOWLEDGE COMMONS FRAMEWORK

This report begins by drawing inspiration from the Knowledge Commons Framework (KCF), developed by Frischmann et al.,[153] which in turn was inspired in part by pioneering Institutional Analysis and Development (IAD) approaches to studying commons arrangements developed by Ostrom and Hess.[154] 'Knowledge Commons' refers to an institutional approach (commons) to governing the production and management of a particular type of resource (data). The concept has been utilised to analyse online sharing in creative communities (Liu et al., 2014) and similar interactions in the digital environment.[155] The knowledge resources produced and managed within the global data knowledge commons include the information, science, creative works, data and so on, used and generated by the global digital and online community. The global data ecosystem can thus be conceptualised as built around three key pillars – knowledge resources, community attributes and governance rules and institutions. These three pillars are interrelated and contingent. Interactions throughout the knowledge commons action arena create new intellectual resources (new data), feeding back directly into resource characteristics, which in turn shape community attributes and governance. The analysis presented below incorporates considerations of the interests and influence of global digital stakeholders, including higher level governance institutions, intellectual property owners, and community members, including software and other creative works artists, those whose data is collected, as well as data harvesting, data storage and data sharing interests. It also expressly incorporates other frameworks for analysing regulatory endeavours in the digital realm – in particular, for digital marketplaces and digital sovereignty.

Figure 1: Diagram of a Governing Knowledge Commons Framework



[153] Brett M. Frischmann, Katherine Jo Strandburg, Michael J. Madison (eds), *Governing Knowledge Commons*. (2014). United Kingdom: Oxford University Press.
[154] Ostrom, Elinor. (2010). "Beyond Markets and States: Polycentric Governance of Complex Economic Systems." *American Economic Review*, 100 (3): 641-72. Charlotte Hess & Elinor Ostrom (eds), *Understanding Knowledge as a Commons: From theory to practice*. MIT Press, (2007).
[155] Liu, Chen-Chung; Lin, Chia-ching; Deng, Kuei-Yuan; Wu, Ying-Tien & Tsai, Chin-Chung. Online knowledge sharing experience with Creative Commons (2014) 38(5) *Online Information Review* 680-696.

3. THE DIGITAL DOMAIN AS A MARKETPLACE

The global data ecosystem can be conceptualised as a marketplace. A marketplace framework recognises the reality that data (whether personal or non-personal) is a valuable asset - a non-rival but de-facto limited access resource - that can be and often is recognised as property and can be traded. The need for a regulatory framework governing such trades has been recognised at national and international levels. The American Law Institute and the European Law Institute have proposed (soft law) principles for the data economy (2021), especially targeted at data contracts and data rights. Others have proposed that internationally recognised contract law principles codified in the Vienna Convention on Contracts for the International Sale of Goods could be extended to embrace trade in data (Hayward, 2021, Pts I & II).[156]

A marketplace and contract law framework for analysing the global data ecosystem, however, does not allow for adequate consideration of the rights of all stakeholders, including the rights of individuals whose data is harvested without reward, and the rights of NGOs and others excluded from the digital marketplace. These include the right to privacy, the right to informed consent before personal data can be collected, stored, and/or shared, and the right to have incorrect personal information rectified or deleted. These rights are now the subject of protective legislation at the national level in Europe, China[157] and elsewhere, with little or no attempt at international level to harmonise such efforts. Conceptualising the global data ecosystem as a knowledge-commons allows for consideration of a broader range of relationship types and interests than a 'marketplace' framework allows.

[156] Ben Hayward, To Boldly Go, Part I: Developing a specific legal framework for assessing the regulation of international data trade under the CISG. (2021) 44(3) *University of New South Wales Law Review*, 878. Ben Hayward, To Boldly Go, Part II: Data as the CISG's next (but probably not final) frontier. (2021) 44(4) *University of New South Wales Law Review*, 1482.

[157] Personal Information Protection Law of the PRC, 22 August 2021, effective 1 November 2021. https://www.secrss.com/articles/41748. For commentary, see What the PRC's new privacy law means for you. Lane Neave News. (2022). https://www.laneneave.co.nz/news-events/what-the-prcs-new-privacy-law-means-for-you/.

4. SOVEREIGNTY 2.0: THE DIGITAL DOMAIN AS A SOVEREIGN SPACE

Academics and news media have also sought to apply a sovereignty analysis to the digital ecosystem.[158] A digital sovereignty analysis recognises that assertions of data sovereignty are inevitable in a world order shaped by the ontology of the sovereign nation state. There are at least three motivations for national assertions of sovereignty in the digital domain:

> *"First, governments demand digital sovereignty to better protect their population – seeking, for example, to remove material deemed illegal under their laws or to protect the rights of citizens in the digital domain. This often takes the form of regulating foreign corporations that intermediate data flows for the local population. Second, governments seek digital sovereignty in an effort to grow their own digital economy, sometimes by displacing foreign corporations from fintech to social media. Third, governments seek digital sovereignty to better control their populations – to limit what they can say, read, or do".*[159]

This report recognises the reality that sovereign concerns (national interest considerations) will inevitably shape the formation of governance understandings reached in the digital domain. Co-operative efforts around the development of soft law guidelines and standards, the drafting of international model laws and binding instruments will require agreement from dominant members of the digital community - nation states and the global corporations that control the digital platforms that are a central feature of digital ecosystem infrastructure. At the same time, however, this report also makes use of the knowledge commons framework developed by Frischmann et al.,[160] to understand governance challenges in the digital ecosystem, and to overcome the limitations of an analytical framework bounded entirely by sovereign concerns.

Efforts now underway to establish co-operative governance understandings on regulating the digital realm all recognise that digital services must, to a greater or lesser extent still to be determined, be treated as a global public good. The WTO Joint Statement Initiative on E-commerce, for example, embraces global public interest concepts, recognising the need to close the digital divide, and ensure that developing and least-developed countries (LDCs) can access development opportunities offered by the digital economy.[161] The EU Vision for the Future of the Internet statement likewise incorporates respect for human rights as reflected in the Universal Declaration of Human Rights, and the need to 'ensure that all people of the world are able to benefit from the digital transformation'.[162] Both

---

[158] Anupam Chander & Haochen Sun, Sovereignty 2.0. https://scholarship.law.georgetown.edu/facpub/2404. https://ssrn.com.abstract=3904949/

[159] Anupam & Sun, Sovereignty 2.0, 8.

[160] Brett M. Frischmann, Katherine Jo Strandburg, Michael J. Madison (eds), *Governing Knowledge Commons*. (2014). United Kingdom: Oxford University Press.

[161] WTO Joint Statement Initiative on E-commerce: Statement by Ministers of Australia, Japan and Singapore (2021). Accessed at ji_ecom_minister_statement_e.pdf (wto.org)

[162] General Secretariat, Council of the European Union, Alliance for the Future of the Internet (AFI) revised Vision Statement, Working Document WK 1999/2022 REV 1. Brussels (2022). See also EU and international partners put forward a Declaration for the Future of the Internet. European Commission, Press Release, Brussels (28 April 2022). Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2695.

documents are nonetheless primarily shaped by a sovereignty framework built around the Charter of the United Nations, existing international fora, and the desire to 'affirm responsible state behaviour in cyberspace'. While global initiatives to facilitate harmonisation of cyberspace have often been framed by sovereignty concerns, they have not been confined by such concerns. Indeed, the data commons idea has also emerged at the recent ITU AI for Good Summit and the World Government Summit.[163]

A knowledge commons approach to conceptualising the digital ecosystem enables policy makers to recognise that governance cannot only be structural, it must also be relational. It renders visible actors and relationships in the digital realm that are neither sovereign nor necessarily recognised within sovereign legal systems.[164] It facilitates an understanding of (and respect for) local contexts, including sub-national contexts and local contexts that transcend, or are not recognised by sovereign legal systems. A knowledge-commons approach also encourages investigation of the often unintended and consequences of interactions between different parts of the global governance ecosystem shaping the digital realm. It facilitates multi-stakeholder participation in governance, which can be supported by (financial and possibly other) resources held by a dedicated global trust.

In June 2019, a report of the UN High-Level Panel on Digital Co-operation presented a vision for strengthening multilateralism and diversification of voices in digital co-operation. The report identified three potential governance frameworks for global digital co-operation – an Internet Governance Forum Plus, a distributed co-governance architecture, and a digital commons architecture. While norm-making and governance in digital technologies pose different challenges, the UN Panel recognised that aspects of the digital realm do share characteristics with other global commons spaces requiring responsible and multi-stakeholder stewardship. The Panel's proposed 'Digital Commons Architecture' would comprise multi-stakeholder tracks to create dialogue and initiate projects around emerging issues, and co-ordinate aggregation of lessons from use-cases and problems for use in soft-law or more binding approaches in appropriate forums. Each track could be owned by a lead organisation with participation governed by principles designed to ensure inclusiveness and broad representation.

The process of ongoing engagement and dialogue established within such a structure could be used to facilitate harmonisation projects on particular areas of law. One downside may be that the energies and resources expended in establishing and maintaining a multi-stakeholder architecture could detract from specific law-reform projects. More importantly, establishing top-heavy architecture could effectively replace efforts to facilitate the kind of bottom-up feed-in mechanisms that can be so valuable, but are all-too-often neglected in multilateral governance initiatives.

[163] See: https://news.itu.int/roadmap-zero-to-ai-and-data-commons/ and https://the-levant.com/use-world-leader-ai-global-data-data-commons-roundtable.

[164] The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital Technologies. Mark Leiser & Andrew Murray in *The Oxford Handbook of Law, Regulation and Technology*
Edited by Roger Brownsword, Eloise Scotford, and Karen Yeung (2017) DOI: 10.1093/oxfordhb/9780199680832.013.28

5. RECOGNISING INTERACTIONS AND RELATIONSHIPS: GLOBAL DATA GOVERNANCE AND THE WIDER REGULATORY ECOSYSTEM

Efforts to regulate transborder data flows go back to the 1970s.[165] Early efforts include the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[166] and the Council of Europe's *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*.[167] From the start, potential for conflict between free trade principles and privacy protection was recognised. By the time the Uruguay round began work on drafting a General Agreement on Trade in Services (GATS), the United States and other nations, urged on by global financial platforms including American Express (Amex), were openly expressing concern that disparities in national privacy legislation 'could hamper the free flow of personal data across frontiers … caus[ing] serious disruption in important sectors of the economy, such as banking and insurance'.[168] What finally emerged was an attempt to balance the priorities of nations (including India and the Nordic countries) concerned to 'preserve sovereignty, national security, and … the privacy of individuals', with those of nations keen to ensure the global free flow of data essential to their domestic business interests. The compromise was a limited privacy 'carve out' to the free-trade principles of GATS found in Article XIV(c)(ii):

> *"Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures … necessary to secure compliance with laws or regulations … including those relating to: the protection of the privacy of individuals in relation to the processing and dissemination of personal data …"*

By allowing signatory nations to protect privacy so long as such action is both 'necessary' and not unduly restrictive of trade, this carve-out has resulted in a proliferation of divergent national privacy rules applied inconsistently. Jurisdictions have sought to determine the 'adequacy' of privacy protection for data transfers by asking whether the level of protection offered in the third country is 'essentially equivalent' to local standards. The regulatory thicket and splintering of national standards for determining 'adequacy' have resulted in 'harm to small and medium enterprises (SMEs), especially in less developed countries, and a boon to large companies, especially those in the West. 'The promise of an internet that would permit workers in the Global South to provide services and goods to consumers and businesses in the Global North' has been broken.[169] As Chander & Schwartz explain:

---

[165] Anupam Chander & Paul Schwartz, Privacy and/or Trade. (2023) 90 *University Chicago Law Review*. Forthcoming. Accessed at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531

[166] OECD Doc. C(80) (58) final (1980).

[167] 28 January 1981, E.T.S. 108.

[168] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Preface. Accessed at https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#preface

[169] Anupam Chander & Paul Schwartz, Privacy and/or Trade. (2023) 90 *University Chicago Law Review*. Forthcoming. Accessed at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531, 5.

> *"Many of the largest tech enterprises are in the United States, and … have [the resources to] invest heavily in the process of privacy compliance. [These firms also]… begin with a significant global advantage due to their extensive customer base. By having this existing relationship with millions or even billions of customers throughout the world, it is easier for these enterprises to craft processes to comply with changing legal requirements while also maintaining data-rich relationships with their current users. These connections provide a major head start …"*

While the signatories to the GATS declared their desire to, "facilitate the increasing participation of developing countries in trade in services and the expansion of their service exports including, inter alia, through the strengthening of their domestic services capacity and its efficiency and competitiveness",[170] the opposite has occurred. Instead, the outcomes of existing interactions between the regulatory regime for data privacy, and the regulatory structures which perpetuate oligopolistic ownership structures in the digital marketplace are highly undemocratic. The irony is that both privacy and trade share important democratic values. Trade rules were always meant to promote the global democratisation of opportunity,[171] while the values of privacy include self-determination and democratic community.[172]

Another example of regulatory interactions in the global digital ecosystem having undemocratic consequences relates to the interaction of ownership structures in the global digital (platform-based) marketplace, and global anti-money laundering (AML) rules. Global AML rules, as enshrined in the Financial Action Task Force Recommendations, now embrace the combatting of terrorist financing (CTF) amongst their aims. The nature and impact of the interactions between these two aspects of the digital ecosystem were highlighted by the President of Barbados, Mia Mottley, delivering the Inaugural WTO Presidential Lecture[173] in March 2022. She began by noting that the geography of digital commerce is shaped by a high concentration of corporate ownership and control. In particular, the digital realm is dominated by nine digital platforms controlled by nine multinational corporations: Alibaba, Amazon, Apple, Baidu, Facebook (Meta), Google, IBM, Microsoft and Tencent. Six of these firms are based in the United States and three are based in China. The business model upon which this digital oligopoly (Mottley's term) is based on, centres around the provision of free access to internet services, in exchange for free use of data harvested from the users of those services. This data is then assembled into valuable digital products which are then sold on. The business model is one which relies on economies of scale and is dependent upon the regulatory infrastructure which allows those economies of scale to be exploited for profit.

Because of these features of the digital ecosystem, access to the benefits of global trade is increasingly dependent upon the ability of consumers and producers to access at least one of the nine dominant digital platforms which in turn requires agreeing to the terms of use dictated by their powerful

[170] General Agreement on Trade in Services (1994), Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M.
[171] See eg. the Agreement establishing the WTO preamble, recognising the 'need … to ensure that developing countries, and especially the least developed among them, secure a share in the growth in international trade commensurate with the needs of their economic development'.
[172] Privacy and/or Trade, 6.
[173] 23 March 2022, available on Youtube at https://www.youtube.com/watch?v=Vhb8afdue1s

corporate owners. The space and opportunity for consumers and producers to remain outside of these digital platforms is rapidly shrinking. This has particularly inequitable consequences for suppliers and consumers in smaller, developing, and least developed economies.

One important reason for the inequitable consequences of digital platform oligopolies stems from the ways in which this feature of the digital realm, and the regulatory framework which enables it, interacts with the regulatory framework established since 2001 to combat money laundering. The Financial Action Task Force Anti-Money Laundering/Combatting Terrorist Financing (AML/CFT) Recommendations impose regulatory standards for financial regulation that have effectively been globally adopted by developed and developing countries alike.[174] Jurisdictions deemed to have flaunted international AML/CFT rules, notably small and/or least developed economies on the periphery of global financial markets, are punished severely as they are cut off from global financial circulation.[175] Isolation from global financial flows occurs either indirectly, through 'blacklisting' by other governments, which leads to financial market players adjusting their risk profiles for blacklisted jurisdictions, or directly, as investors withdraw their money, fearing the devaluation or confiscation of their assets.[176] One effect of this dynamic has been that retail banking services have gradually withdrawn from and abandoned these peripheral jurisdictions.

Consumers and producers in nations affected by this dynamic, nations which include Myanmar, Vanuatu, and Barbados, are effectively cut off from the benefits of financial transfer systems, such as the SWIFT regime accessible through retail banking networks. It also means that financial regulation has long since ceased to be a domestic concern. Instead, those seeking to transfer funds into or out of these jurisdictions must rely upon the dominant financial platform providers Amex, Mastercard and/or Visa, and must opt into the globalised terms offered. These terms reinforce a global structure for financial flows that is advantageous to, and profitable for, dominant platforms and service providers, rather than for users.

Efforts have been made to demonopolise the Internet. Sir Tim Berners-Lee, for example, envisioned a way of giving users an option to store their data on a private server using solid open-source technology. If a dominant platform company, such as Facebook (Meta), does not store a person's data, it becomes significantly easier for that individual to control which parts of their digital lives they are sharing with the company. Looking for a legal framework to support Berners-Lee innovation, Jack Balkin and Jonathan Zittrain came up with the concept of information fiduciaries. Treating tech companies that have access to personal or potentially sensitive information about their clients as fiduciaries would, imposing legal obligations upon them to act in the best interests of those clients. Yet the concept of information fiduciaries has been criticised for putting too much trust in the platform companies.

---

[174] FATF (2012-2019), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html

[175] Hameiri, S. & Jones, L. (2015), 'Governing transnational crime: securitisation and the global anti-money laundering regime', in Hameiri & Jones, *Governing Borderless Threats: Non-traditional Security & the Politics of State Transformation* (CUP).

[176] Shahar Hameiri & Lee Jones, Governing Borderless Threats: Non-traditional security and the Politics of States Transformation. Cambridge University Press, (2015), Chapter 5, p. 162.

6. DATA TRUSTS AS A TOOL FOR USE IN GOVERNANCE STRATEGY

Drawing upon the concept of information fiduciaries, Sylvie Delacroix and Neil Lawrence argued that a variety of independent data stewards are needed to mediate the relations between individuals and communities on the one hand, and tech companies on the other.[177] Sean Macdonald has explored the historical evolution and practical considerations surrounding the concept of civic data trusts. A data trust is a steward that manages someone's data on their behalf. The data trustee owes fiduciary obligations to act in the best interests of trust beneficiaries. A distinction needs to be recognised between trusts that store data and those that manage individual and collective rights of access to the data. Anna Artyushina draws an analogy between data trusts and digital libraries (such as, JSTOR) that likewise serve a designated community and protect data (digital texts) from unauthorised access.

In the UK, trust law is widely applied to manage access to public and common resources. It is not surprising then that the British government was the first to embrace data trusts as a legal framework for data access. The University of Cambridge' Data Trust Initiative, the Open Data Institute (ODI) and the Ada Lovelace Institute have all examined data trusts as a possible legal framework for data stewardship in the UK and abroad. The European Commission's Data Governance Strategy and the AI Roadmap propose an industry of professional data stewards charged with custody and management of public pools of personal and non-personal information collected from European residents. Canada's Bill C-11 (Digital Charter Implementation Act) proposes establishing public data trusts as a means of managing de-identified data for 'socially beneficial purposes.' Australia's data stewardship policies announced in 2020 likewise seek to treat pools of de-identified data collected from individuals, firms and collectives as 'knowledge commons' that should be managed for the benefit of all.

One issue potentially confronting these initiatives and developments in national jurisdictions is the extent to which data should be treated as property. As noted in this report's chapter on 'Non-Personal Data Governance: Facilitating Non-Personal Data Flows', non-personal data *as such* is not usually captured by traditional IP rights, nor is a 'property-like' right to data provided by major legal systems.[178] Attempts to facilitate the free flow of data have treated this lack as a barrier to be overcome, and have sought to fit data within the framework of existing legal instruments – such as compulsory data license agreements (as proposed in the EU Data Act) or some form of 'data property' or 'data IP rights'.[179]

[177] Sylvie Delacroix and Neil D. Lawrence, Bottom-up data Trusts: disturbing the 'one-size-fits all' approach to data governance (2019) 9(4) *International Data Privacy Law* 236-252.
[178] Cf. in this regard, Amstutz, Dateneigentum, AcP 218 (2018), 438-551; Drexl et al., Data Access and Data Ownership: Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate (Max Planck Institute for Innovation and Competition Research Paper No. 16-10), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165 Kerber, Governance of Data: Exclusive Property vs. Access, International Review of Intellectual Property and Competition Law (2016), 759-762.
[179] Zech, Building a European Data Economy – The European Commission's Proposal for a Data Producer's Right, 9 Zeitschrift für Geistiges Eigentum (2017), 317-330

The non-fungible nature of data has also been seen as a barrier to establishing legal avenues for data trusts. A legal framework report entitled 'Data Trusts: legal and governance considerations' (commissioned by the Open Data Institute) for example, concluded that 'data is not capable of constituting property in the legal trust sense, and thus cannot form the basis of a legal trust in any of the legal systems which have a concept of trust law'.[180] Delacroix and Lawrence convincingly argue that this argument misunderstands the nature of data. The nature of data, its collection, processing, storage and transfer means that data rarely exists for long in the same form. Discrete pieces of data only have value in so far as they are bundled, packaged, accessed, and used. This value can change according to the size and nature of the data set, and the use to which it is put. Data itself is not subject to valuation, only the use to which it is being, or is to be, put can be valued. It is not surprising then that existing legal frameworks for data privacy and fiduciary principles of accountability, when data is transferred internationally, avoid the language of property rights (rights in *rem*) and instead speak of the need to protect personal and contractual rights (rights in *personam*). In other words, data trusts may well provide a tool for facilitating data flows, without necessarily turning to concepts derived from the law of property and/or IP licensing.

Companies are becoming increasingly aware of the value of sharing data with industry peers and/or across industries. Typical use cases for data sharing are fraud detection in financial services firms or combining genetics, insurance data, and patient data to develop new digital health solutions and insights. Data trusts provide a tool for data sharing while at the same time minimising the regulatory, financial, and reputational risks that companies can be exposed to when sharing sensitive company (including customer) data. Data trust trustees will represent the rights and interests (including privacy rights) of data providers, when negotiating and contracting access to their data for use by data consumers, such as other companies and organisations.

Data trusts are a means of ensuring the ethical and compliant governance of data – for example, by ensuring that individuals have provided the required consent to various uses of their data, de-identifying personal data and removing data bias). They can also encourage data interoperability. By adopting technologies such as federated machine learning, homomorphic encryption, and distributed ledger technology, a data trust can facilitate transparency in data sharing, as well as the auditing of who is using the data at what time and for what purposes (for example, tracking chains of custody for data).

[180] Reed, BPE Solicitors, and Pinsent Masons, 'Data Trusts: legal and governance considerations' (2019), https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf

7. THE PUBLIC TRUST CONCEPT AND EMERGING DATA TRUST PRACTICE

The public trust doctrine has been explored and discussed for its potential application to other 'global commons', including Antarctica, the high seas,[181] outer space,[182] and natural resource commons.[183] The special nature of data - its variegated and dispersed nature, and its unique relationship with individual, corporate, and sovereign interests - however, means that a different model is emerging. There is a need to recognise the reality of top-down regulatory constraints, at the national and regional levels (including those of the GDPR). The 'bottom-up' data Trust model envisioned by Delacroix and Lawrence, which is being adopted and adapted by lawyers, is 'resolutely' complementary to these sovereign regimes. It also allows for the emergence of a wide variety of data Trusts, each designed to balance data risks and responsibilities in the way best suited to the aims, needs, and interests of participants.

Examples of specific use data trusts include medical data trusts, which can be designed to protect data subjects' (patients) rights by encouraging them to think about their sharing preferences before possibly being placed in a vulnerable position. Such trusts can also remove obstacles to research by making anonymised data accessible to health project researchers, for so long as research projects aim to make on-going access desirable. Given the contested nature of limits to medical research objectives and ethical boundaries, medical data trustees may play a more active and significant role in monitoring compliance and ensuring 'best practices' within particular research studies. Genetic data trusts are another specialised trust which might be designed to facilitate 'bottom up' societal debate about complex issues such as the right balance between the interests of current and future generations.

Data Trust structures could also be used to overcome some of the existing power imbalances in the use of social media data. When individuals exercise 'choice' about how data from their social media feed is shared when they interact with different online sites the extensive nature of the conditions, they are asked to agree to makes it unrealistic for most to actually read, understand and exercise active choices. Additionally, when terms and conditions are changed, users are unlikely to weigh the benefits of access with the costs of those changes before agreeing to the change. Data Trusts could be used to step in and ameliorate the resulting power imbalances by pooling together social media data rights. Individuals could join a data Trust on the basis of a pre-determined set of guidelines for handling negotiations with social media platforms on their behalf. Instead of having to agree to predetermined conditions, users would name the data Trust they belong to, and their data would then be dealt with accordingly.

[181] Sarah Cinquemani, Can the Public Trust Doctrine Save the High Seas? (2019) 31(3) *Environmental Claims Journal* 218-238.
[182] Hope M. Babcock, The Public Trust Doctrine, Outer Space, and the Global Commons: Time to Call Home ET (2019) 69(2) *Syracuse Law Review* 191.
[183] Joseph Orangias, Towards global public trust doctrines: an analysis of the transnationalisation of state stewardship duties (2021) 12(4) *Transnational Legal Theory* 550-586.

The evolution of such a network of different types of trust implies the development of an ecosystem of Trusts. According to Delacroix and Lawrence, two conditions must be met for such an ecosystem to thrive. First, entry barriers should be low – the creation of new Trusts must be relatively straightforward. Second, the data subjects' data must be secure. This second condition may mean relying upon the expertise of commercial providers of secure computational and storage infrastructure, leaving the Trust itself free to focus on collectively setting the terms according to which the settlors' data should be stored and made available for processing and usage.

An ecosystem of data Trusts implies a system of data exchange between Trusts and consumers of the data (companies, research labs, and so on). Data exchange may occur within or between the borders of national (or regional) regulatory systems. Such a data exchange system requires that data Trusts, and the rights they are set up to protect, are recognised across and between different regulatory systems. In addition, computational and storage systems must be able to store and manage different types of personal data from different sources. As well as being portable between different computer systems, an individual's data (so far as remains possible in the case of anonymised data sets) must be erasable from any particular system. Existing legal provisions in different regulatory systems may require amendment if a fully flourishing data Trust ecosystem is to be facilitated. Delacroix and Lawrence give the example of Article 17 of the GDPR which grants a right to have personal data erased in certain circumstances only, rather than allowing the data provider to determine (negotiate) the terms on which data erasure can be demanded.

Mutual recognition of different data Trust models from foreign regulatory systems would be for each jurisdiction to determine but could be facilitated by the development of a UNCITRAL-style Model Law. Since the 1980s, UNCITRAL has been developing a suite of legislative instruments aimed at facilitating commercial transactions by electronic means. In 1985 the Recommendations to Governments and international organisations concerning the legal value of computer records was published. The UNCITRAL Model Law on Electronic Commerce (1996) has become the most widely enacted text, along with the UNCITRAL Model Law on Electronic Signatures (2001), it helped to lay the path towards a UN Convention on the Use of Electronic Communications in International Contracts (2005). Most recently, the UNCITRAL Model Law on Electronic Transferable Records (2017) applies the same principles to enable and facilitate the exchange of legal documents and transferable instruments in electronic form. The same or similar approach could be taken to develop a Model Law on international data exchange, including provisions for mutual recognition of computer system security standards and fiduciary law principles applicable to data Trusts. As a result, more than one Model Law instrument may emerge.

Trusts and fiduciary law, more broadly, are common law innovations, meaning that they do not exist in a large part of the world. While a growing number of countries have developed fiduciary and trust adaptations, there are no globally recognised principles in domestic systems. Yet principles applicable to global commons are well recognised in international law and could form the basis for a globally recognised Model Law on global data Trusts for adoption (and adaptation) in domestic systems. The three major digital markets – the United States, the EU and China – have taken divergent approaches to internet and data governance, with the United States, EU and their allies favouring a rules-based global cyberspace within which data flows freely between nations, while China and its Shanghai Co-

operation Organisation allies would prefer a greater role for national authorities in defining and governing the network's frontiers through domestic regulation. Agreement on a Model Law setting out basic fiduciary principles for national regulation of data Trusts provides a first step towards bringing together important parts of a currently fragmented regulatory landscape for privacy protection and data localisation. The consequent harmonisation of domestic laws governing global data commons would improve predictability for businesses, reduce barriers to trade and innovation, and prevent a technological rupture in a duopolistic or monopolistic global economy dominated by United States' and Chinese interests. Forum shopping would also be minimised by incorporating mutual recognition rules between the Model Law member jurisdictions.

UNCITRAL and/or the WTO are not the only fora within which harmonisation initiatives are taking place. At the June 2019 G20 summit in Osaka, then-Japanese Prime Minister Abe Shinzo declared the launch of the Osaka track, a policy dialogue aimed at building international rulemaking on the digital economy. By strengthening data and privacy protection, intellectual property rights, and cybersecurity norms, the Data Free Flow with Trust (DFFT) initiative, pursued through the Osaka Track, seeks to reinforce consumer and business trust, establish interoperability, and enable free data flows to harness digital economy opportunities.

Data trusts are not a silver bullet for governing the global digital commons. There are many issues of data governance that cannot be solved through the application of fiduciary principles, including challenges of international relations and power-imbalances between stakeholders. Yet, to the extent that they are a useful tool for representing concerns of data subjects, for solving challenges of balancing rights and interests in local situations, and for achieving specific aims, they are a useful tool that should be available to individuals, companies, and collectives. The job of sovereign governments is to put in place regulatory systems that facilitate easy and cheap access to data Trusts as a legal structure for managing data in which they have an interest.

cerre Centre on Regulation in Europe

03

CONVERGENCE AND DIVERGENCE IN GLOBAL DATA PRIVACY LAW: COMPARING THE GDPR, PIPL, AND CCPA

Co-ordinated by Anupam Chander

1. INTRODUCTION

It is conventional wisdom that divergent approaches to data privacy across the world make any global agreement on data privacy unlikely. But precisely how different are those approaches? Is there a core agreement upon which to build? This study compares and contrasts the data privacy laws in three jurisdictions—the European Union, China, and the State of California. The three are chosen because of their leading role in international economic law—the EU, as the global leader in data privacy regulation; China, with an economy that is central to international trade; and the State of California, with the world's largest internet enterprises and the first comprehensive data privacy law in the United States. While the three jurisdictions represent different levels of political organisation, the focus here is on the convergences and divergences among the substantive data privacy norms that each jurisdiction offers.

The European Union's General Data Protection Regulation (GDPR), China's Private Information Protection Law (PIPL), and the California Consumer Privacy Act (CCPA) all regulate the collection, processing, and transfer of personal data. While the GDPR regulates both public and private parties, the PIPL and the CCPA focus on personal data held and processed by private parties alone. This study summarises key areas of convergence, as well as key differences between the various laws.

A panoramic view of the three jurisdictions reveals that, while drafted in diverse contexts, these laws offer a significant core of overlapping rights and duties. They all provide broad coverage over the processing and use of personal data which cuts across economic sectors, though the CCPA excludes some areas already governed by federal privacy law. With the recent amendment of the California Privacy Rights Act (CPRA), all three bodies of law now establish an independent data privacy regulatory authority, charged with investigation and enforcement.

The GDPR and its predecessor, the Data Protection Directive, have proven remarkably influential across the world, both through their *de facto* adoption by multinational businesses as global standards, and through their *de jure* adoption by governments. The Chinese law draws heavily on the European approach, and thus the two share a familial resemblance. In fact, seven of the PIPLs eight chapters – excluding the chapter on special provisions – directly correspond with a chapter of the GDPR, though the details within these chapters differ.[184] While both the PIPL and the CCPA have adopted some structural and substantive features of the GDPR, the PIPL has gone further and directly modelled its laws on concepts in the GDPR. However, unlike the GDPR, the PIPL often frames its rules in broad terms, which require elaboration to ease compliance. While all of these laws share roots in the Fair Information Practices developed in the 1970s, the CCPA is not modelled on the European data protection model.

[184]Jet Deng & Ken Dai, *The Comparison Between China's PIPL and EU's GDPR: Practitioners' Perspective*, Dentons (Oct. 8, 2021), https://www.dentons.com/en/insights/articles/2021/october/8/the-comparison-between-chinas-pipl-and-eus-gdpr

While the three laws often employ different terminology, their terms generally refer to the same subject matter and use similar definitions. The CCPA, PIPL, and GDPR all give residents within their respective jurisdictions personal rights to their data.[185] Under each law, the covered data is determined using similar definitions. The party that determines the purposes and methods for processing personal information is called the "data controller" in the GDPR, and the "personal information handler" in the PIPL.[186] While four terms in the PIPL (personal information handlers, automated decision-making, de-identification, and anonymisation) have direct counterparts and similar definitions in the GDPR, the GDPR defines another 21 terms that are not in the PIPL.[187]

Overall, all three laws feature provisions that address consumer rights of access, portability, data deletion, purpose limitations, notice, accountability, data security, enforcement, privacy impact assessments, and consent in relation to individuals' data. Although these provisions are not the same in each law, they mark major areas where the CCPA, PIPL, and GDPR align on core data privacy rights. With the recent passage of the CPRA, most of which is scheduled to come into effect in 2023, the State of California followed the European Union in establishing a data privacy authority, the California Privacy Protection Agency. While many of the substantive obligations of the CPRA will not take effect until 2023, the California Privacy Protection Agency was already established in 2020.

The State of California law offers a narrower set of data privacy rights than those available under the European and Chinese laws, but the overlap of rights is still substantial. The State of California's law has catalysed data privacy laws in multiple states and may lead to a national data privacy law in the United States.[188] Large companies operating in this jurisdiction must now comply with this law to continue serving the largest market within it. While the U.S. Congress is considering enacting the country's first comprehensive privacy law, the State of California's law currently stands as the most well-elaborated of all the state laws.

Each of these three laws exists within a broader framework of statutes, institutions, procedures, and practices that must be examined to gain a fuller understanding of the effects of these rules. Thus, a comparison of these three statutes themselves is only one part of understanding the similarities and differences between them. Both enforcement priorities and capacities are likely to vary, though each of the selected jurisdictions has formidable regulatory authorities, with a significant record of enforcement in respect of data privacy. The United States Federal Trade Commission, for example, cited GeoCities for privacy failures as early as 1998.[189] While this study confines itself to law on the

[185] *See* Cal. Civ. Code §§ 1798.105(a); 1798.140(g); Cal. Code Regs. tit. 18, § 17014; GDPR Art. 4(1); PIPL Arts. 1-2.

[186] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 4(1), OJ 2016 L 119/1; PIPL Art. 4; Xu Ke Et Al., *Analyzing China's PIPL and How it Compares to the EU's GDPR*, IAPP (2021), https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/

[187] GDPR Art. 4; Creemers, Rogier, and Graham Webster. *"Translation: Personal Information Protection Law of the People's Republic of China."* DIGICHINA (2021), https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

[188] Anupam Chander, Margot E. Kaminski, and William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1737 (2021).

[189] *FTC, GeoCities Settle on Privacy*, CNET (Aug. 13, 1998), https://www.cnet.com/tech/services-and-software/ftc-geocities-settle-on-privacy/ [https://perma.cc/Y2AG-B78N] (archived Jan. 9, 2022) GeoCities, 127 F.T.C. 94 (1999) (cited in Anupam Chander & Haochen Sun, Sovereignty 2.0, 54 VAND. J. TRANSNAT'L L. (2022)).

books, differences in contexts, institutions, and practices are also likely to prove critical to the real meaning of these laws.

2. RECOMMENDATIONS

> *An international agreement on (minimum) data protection and privacy rules is a medium-term goal that must be carefully evaluated with regard to a potential foreclosure of the 'market' for regulatory ideas.*

As the workstream on digital trade observes, the fracturing of co-operation-permitting data flows reduces the benefits of digital trade. One key aspect of this fracturing is divergent personal data privacy regimes. This study's comparison between three principal data privacy regimes helps to show both the extent of the divergence, and also the significant convergence that is emerging.

The existing convergence among disparate jurisdictions might be regarded as a basis for broader collaboration and interoperability—and might suggest that there is a greater possibility for broader international agreement on a minimum set of substantive and procedural data protection and privacy rules, than is commonly assumed.

A detailed comparison between the privacy laws of China, the European Union, and the State of California reveals significant convergence that can be a basis for broader collaboration and interoperability. There is a significant core of shared legal norms across these leading jurisdictions. These include the basic rights to access, correct, and delete personal information, special protections for children and sensitive data, the right to data portability, data minimisation, data retention limitations, accountability for violations, and risk-based cybersecurity requirements. As such, there is more that unites these laws than divides them. This convergence among these disparate jurisdictions suggests that there is a greater possibility for broad international agreement on a minimum set of substantive and procedural privacy rules, than is commonly assumed.

More study is needed to understand what motivates the various divergences between privacy laws across jurisdictions. Where some divergences may have cultural components—for example, the age of consent for children or the types of data considered 'sensitive'—other divergences are more abstract and obscure, and not readily ascribable to societal differences.

It would be useful to compare enforcement patterns across jurisdictions by the type of right that is alleged to be violated. What are the kinds of violations that are most commonly enforced? For example, is enforcement typically focused on the failure of data security standards, excessive collection of information, use of information for improper purposes, the use of sensitive data, or restrictions on cross-border data flows?

3. CONVERGENCE AND DIVERGENCE IN THE GDPR, PIPL, AND CCPA

	GDPR	PIPL	CCPA
What is protected?	Covers "personal data," meaning any information relating to an identified or identifiable natural person, with special rules for sensitive data, but not when processed for "purely personal or household activity." Arts. 2(2), 4 (1), 9(1)	Covers "personal information" which is defined as information related to an identified or identifiable natural person, with special provisions for sensitive data, but not when processed for "personal or family affairs. " Arts. 4, 28-32, 72	Covers "personal information" which is defined broadly to include information that is capable of being associated with a particular consumer or household, with special provisions for sensitive data added by the CPRA. It excludes data that is made publicly available by the government, and explicitly excludes de-identified or aggregate consumer information. §§ 1798.140(o)(1), 1798.121
Who is regulated?	The GDPR regulates all data controllers and data processors, both public and private entities. Art. 3	The PIPL regulates personal information handlers, which are organisations or individuals who decide how personal information is to be processed, for what purposes, and in what way. It covers both public and private entities. Art. 73	The CCPA regulates any for-profit entity doing business in the State of California that meets certain conditions. Parts of the CCPA apply specifically to service providers and third parties. §1798.140(c)
Where does the law apply?	Applies within the European Union. Applies extraterritorially to personal information controllers and processors processing personal data of European Union subjects when they are targeting the European Union's market or when they are monitoring European Union residents. Art. 3	Applies within the People's Republic of China. Applies extraterritorially to entities processing personal information of Chinese residents. Art. 3	Applies within the State of California. Applies extraterritorially to businesses that are operating in the state and meet specific threshold requirements (at least USD $ 25 million in annual revenue; data collection on at least 50,000 Californians; or at least half of revenue derived from data sales). § 1798.140(c)

Notice	The controller must notify in clear language the data subject of the identity of the controller, the contact details of the data protection officer and data controller, the purposes and legal basis of the processing, categories of personal data concerned, how long the data will be stored, recipients of the data, the existence of any automated decision-making, and the other rights the GDPR grants them. Arts. 12 (1), 13 (1), 13(2), 14, and 90	The individual must be conveniently notified in clear language before their personal information is processed. The notification tells them the name and contact of the handler, the purpose and legal ground of the handling, types of personal information processed, retention period, and the rights the PIPL grants them. There is an exemption to notify when the personal information is confidential. Arts. 17 and 18	Businesses must inform individuals regarding the categories of personal information collected and its intended use, and third parties with which information is shared. Requires further notice for collection of additional categories of data or use of data for unrelated purposes. § 1798.100(b)
Right of Access	Provides an individual's right to obtain their own personal information. Art. 15 (1)	Provides an individual's right to obtain their own personal information. Art. 45	Provides an individual's right to obtain their own personal information. § 1798.110
Right to Deletion/ Erasure	Individual may request erasure of their personal information in certain circumstances, such as if the data is no longer necessary or was obtained unlawfully. Arts. 17 (1)	Individual may request erasure of their personal information in certain circumstances, such as if the data is no longer necessary or was obtained unlawfully. If the retention period has not passed, handlers may hold onto the information but "shall cease personal information handling except for storage and taking necessary security protective measures." Art. 47	Californian residents have the right to request a business to delete their personal information that has been collected, subject to exceptions. The business must also direct their service providers to delete the information. § 1798.105
Right to Correct	A data subject has the right to correct personal data that is inaccurate or incomplete. Arts. 16 and 19	An individual can correct personal information that is inaccurate or incomplete. Information handlers must verify the personal information prior to correction. Art. 46	A business that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate information. § 1798.106

Right to Object/ Restrict Processing	The data subject can refuse or limit the handling of their information, and withdraw their consent at any time. Allows data subjects to prevent their personal data from being used for direct marketing. Arts. 21	The data subject can refuse or limit the handling of their information, and withdraw their consent at any time. Allows individuals to prevent their personal information from being used for direct marketing. Arts. 24 and 44	Limited to opting-out of the sale (defined broadly) of data, though can be supplemented with an action for unfair and deceptive practices if a business violates the disclosed purposes for data collection and processing. Businesses must enable and comply with a consumer's request to opt-out of the sale of personal information to third parties, where "sale" is defined very broadly. The CPRA provides an additional right to limit the use and disclosure of sensitive personal information. §§ 1798.120, 1798.121, 1798.135
Automated Decision-Making	Data subjects have a right to an explanation, and to not be subject to, decisions based solely on automated processing that significantly affect them. Art. 22 (1), Recital 71	Individuals can seek an explanation for, and object to, decisions based solely on automated processing that have a significant impact on the rights and interests of the individual. Arts. 24	The CPRA empowers the CPPA to establish rules related to automated decision-making, including opt-out rights and meaningful information about the logic involved. § 1798.185(a)(16)
Right to Data Portability	A data subject must be able to transfer their personal data in a commonly used and machine-readable format from one controller to another as long as the processing is based on consent and is automated. Art. 20 (1)	An individual must be able to transfer their personal information from one handler to another as long as they meet the conditions of the Cyberspace Administration of China (CAC). Art. 45	All personal information must be portable in readily usable format upon request. §§ 1798.100(d), 1798.130(a)(2)
Privacy by Design	Data controllers must implement privacy by design. Art. 25	While there is no explicit requirement for privacy by design, a number of other requirements suggest a	While there is no explicit requirement for privacy by design in the CCPA, the CPRA adds data minimisation and

		similar principle, including data minimisation and limitations on data retention. Arts. 5-6, 19	limitations on data retention. § 1798.100(c)
Data Minimisation	Personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" Art. 5(c)	"Collection of personal information shall be limited to the minimum scope for the purpose of processing and shall not be excessively collected." Art. 6	The CPRA adds a requirement that data use should be "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed." § 1798.100(c)
Data Retention	Data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, except for scientific, historical, or statistical purposes. Art. 5 (e)	"The retention period of personal information shall be the minimum period necessary for achieving the purpose of processing, except for where the retention period of personal information is otherwise provided for in laws and administrative regulations." Art. 19	The CPRA adds a requirement that businesses shall not retain personal information "for longer than is reasonably necessary for that disclosed purpose." § 1798.100(a)(3)
Data Security	Data controllers and data processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In the event of a breach, data controllers must report it to the relevant authorities within 72 hours. There is no requirement to inform the affected individuals if protection measures to effectively avoid the harms created by the breach are subsequently adopted. Data processors must notify their data controller	Personal information handlers must ensure that handling activities comply with the law and prevent unauthorised access, disclosure, tampering with, or loss of personal information. In the event of a breach, personal information handlers must immediately adopt remedial measures, and notify the departments responsible. There is no requirement to inform the affected individuals if protection measures to effectively avoid the harms created by the breach are subsequently adopted. Arts. 9, 51	As mentioned above, businesses have a "duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information." § 1798.150(a)(1)

	if the processor becomes aware of a breach. Arts. 32 (1), 33 (1), and 34 (3)		
Data Protection Impact Assessment	Impact assessments must be carried out prior to a special category of data being processed or other high-risk data processing activities. The assessment must ascertain the necessity and proportionality of the processing operations in relation to the purposes as well as the risks to the rights and freedoms of data subjects. Arts. 35 (1-3) and 35 (7)	Impact assessments must be carried out prior to sensitive personal information being handled; or prior to a legally binding evaluation based on automated data processing. The assessment must ascertain whether the handling and the protective measures undertaken are legal, effective, and suitable to the degree of risk, as well as the impact on individual's rights. Impact assessment reports and treatment records should be kept for at least three years. Arts. 55 and 56	While the CCPA does not require impact assessments, the CPRA will require impact assessments for activities with significant risk to privacy or security. § 1798.185(a)(15)
Record-keeping	Data controllers and data processors must maintain a record of all their processing activities. Art. 30 (1)	Information handlers must record the handling of sensitive personal information, personal information used in automated decision-making, transfers of personal information to other handlers or abroad, and other "personal information handling activities with a major influence on individuals." Art. 55	Regulations implementing the CCPA require businesses to keep records for at least two years of customer data requests. § 1798.199.40(b), California Consumer Privacy Act Regulations § 999.317.

Data Protection Authority	Mandates each member state of the European Union to create its own independent enforcement authority called the Data Protection Authority (DPA).	Charges the Cyberspace Administration of China (CAC) for comprehensive planning and co-ordination, empowers departments of the State Council to enforce the PIPL in their respective industries, and gives personal information protection duties to certain departments at the county level and higher.	Creates the California Privacy Protection Agency (CPPA), which is vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. § 1798.199.10
Accountability/ Enforcement	The DPA may levy fines up to a maximum of €20 million or 4% of *global annual revenue*, whichever is higher. The DPA may also carry out investigations, issue warnings, order controllers or processors to adopt measures to correct infringements, and impose temporary or permanent bans on processing. Individuals have a right to compensation for "material and immaterial" damages suffered. Class actions only through representative actions. Arts. 51 (1), 58 (1-2), 79, 82, and 83 (5)	The CAC may levy fines with a maximum of ¥50 million or not more than *5% of annual revenue*, and up to 1 million Yuan against a directly responsible person. The CAC may also carry out investigations, issue warnings, order controllers/handlers to adopt measures to correct any infringements, and impose temporary or permanent bans on processing/handling. Creates a private cause of action for violations. Arts. 50, 60, 66, 69, and 70	Civil penalties up to $2,500 per violation or up to $7,500 per intentional violation. Individuals may sue for data breaches in certain cases. § 1798.150(a)(1), §1798.155(a), (b)
Representative	Controllers and processors who are covered by Art. 3(2), but do not have an EU establishment, must designate a representative in the EU, except when the processing is occasional or they are a public authority or body. Art. 27	Processors outside China must designate a representative within the country. Art. 53	No requirement.

Children	The default age for consent is 16, but EU member states can lower the age (but not below 13). Requires parental consent for a child below the age of consent. Children must receive an age-appropriate privacy notice; the personal data of children has heightened security requirements. Art. 8(1)	Data of children under the age of 14 is treated as sensitive data. Art. 31	The CCPA prohibits selling personal information of a minor (under 16) without consent. Children ages 13 to 16 can provide consent, but children younger than 13 require parental consent. The federal Children's Online Privacy Protection Act (COPPA) still applies in addition to CCPA requirements. § 1798.120(c)-(d)

3.1 What Information is Protected?

All three systems protect the personal information of natural persons. They each use different terms to refer to similar concepts: "data subjects" under the GDPR, "natural persons" or "individuals" under the PIPL, and "consumers" under the CCPA.

The type of information protected is similar under the three systems. The GDPR defines personal data as "information concerning a person which makes them directly or indirectly identifiable," the PIPL defines it as "information … related to identified or identifiable natural persons," and the CCPA defines it as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked…with a particular consumer or household."[190] However, the CCPA excludes data that is publicly available.[191] It also seems to borrow the definition of "processing" directly from the GDPR, even retaining the GDPRs use of the term "personal data", rather than the CCPAs preferred term "personal information" in the definition. Indeed, the definitions for data "processing" (or as the PIPL calls it, "handling") are also largely the same between the GDPR, CCPA, and PIPL; however, the GDPR and PIPL both include non-comprehensive examples.[192]

The GDPR imposes additional constraints on the processing of special categories of personal data determined to be sensitive. These categories include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.[193] The PIPL, too, contains special protections for sensitive data, which includes "information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location

[190]GDPR 4(1); PIPL Art. 4.; Cal. Civ. Code § 1798.140(v)(1).
[191]Cal. Civ. Code §§ 1798.140(v)(2).
[192]GDPR Art. 4(2); PIPL Art. 4.; Cal. Civ. Code § 1798.140(y).
[193]GDPR Art. 9(1).

tracking, and personal information of minors under the age of 14."[194] The CPRA adds special protections for sensitive data, which is defined to include a broad array of information providing precise geolocation, racial or ethnic origin, religious or philosophical beliefs, union membership, genetic data, sex life, sexual orientation, and also includes provisions to add additional categories through rule-making.[195]

Both the GDPR and the PIPL exempt data that has been anonymised or pseudonymised, such that the data subject can no longer be identified.[196] The GDPR and the PIPL also exempt the handling of personal data for "purely personal or household activity" (GDPR) or "personal or family affairs" (PIPL).[197] The CCPA implicitly exempts the purely personal or household use of data, because it focuses only on commercial businesses operating at a large scale.[198]

3.2 Who is Regulated?

The GDPR regulates both data controllers and data processors, including public and private entities, regardless of size. What the GDPR calls "processors," the PIPL calls either "processors" or "entrusted parties," although the PIPL does not define the latter term.[199] The PIPL regulates the "handling" of personal information, "where 'handling' includes the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information."[200] The CCPA targets the collection of information by for-profit businesses, and limits the definition of "business" to those undertakings that meet one of three thresholds: (1) they have annual gross revenues in excess of twenty-five million dollars ($25,000,000); (2) they annually transact for commercial purposes in the personal information of 50,000 or more Californian consumers, households, or devices; or (3) they derive 50 percent or more of their annual revenues from selling consumers' personal information.[201]

The CCPA also applies to any entity that either controls, or is controlled by, a covered business or shares common branding with a covered business, such as a trademark.[202] Parts of the law apply specifically to service providers and third parties.[203]

Where the GDPR uses the concept of a "processor" to refer to a party processing data on behalf of the controller, the PIPL uses the term "entrusted party." The GDPR provides more detailed obligations for the data processor.

---

[194]PIPL Art. 28.
[195]Cal. Civ. Code §§ 1798.121, 1798.140(ae).
[196]GDPR Recital 26; GDPR Art. 4(5); PIPL Art. 4, 73(4) (calling the use of pseudonyms "de-identification").
[197]GDPR Art. 2(2); PIPL Art. 72.
[198]*See* Cal. Civ. Code § 1798.140(c).
[199]GDPR Art. 4(1); PIPL Art. 4; Xu Ke, *supra* note 9.
[200]Sullivan and Cromwell, *Personal Information Protection Law of the People's Republic of China—Overview* (Oct. 27, 2021) at 2.
[201]Cal. Civ. Code §§ 1798.100, 1798.140; CCPA and GDPR Comparison Chart, BakerHosteler LLP (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf
[202]Cal. Civ. Code § 1798.140(c).
[203]*See* Cal. Civ. Code § 1798.100.

3.3 Extraterritoriality

All three regimes have extraterritorial applications. The GDPR applies to controllers and processors that are either (1) established in the EU or (2) are not established in the EU, but process EU residents' personal data in connection with offering goods or services in the EU, or monitor the behaviour of EU residents.[204] The PIPL adopts a nearly identical approach. It regulates the handling of the personal information of natural persons from outside of China when that handling: (1) has the purpose of providing products or services to natural persons within China; (2) involves analysing activities of natural persons inside China; or (3) as otherwise provided under other laws or regulations.[205] The CCPA focuses on companies that are doing business in the State of California, whether or not they have a physical presence there or elsewhere in the United States, as long as they meet one of the three quantitative thresholds specified above.[206]

3.4 Legal Basis for Processing

For a controller to lawfully process personal data under the GDPR or the PIPL, it must either obtain consent from the data subject, or have an alternative legitimate legal ground for the processing.[207] The CCPA does not require a legal ground for processing as such, but rather requires that the processing follows the other provided rules, including notice, purpose specification, data minimisation, and rights to opt out. The CCPA presumes that personal data as a default may be collected, shared, and used unless there is a specific legal rule that inhibits such activities.[208]

Consent is defined similarly in each law. Under the GDPR and CCPA, consent is "any freely given, specific, informed and unambiguous indication" of the data subject's wishes, while in the PIPL consent must be "under the precondition of full knowledge, and in a voluntary and explicit statement".[209] Both the GDPR and the PIPL permit the individual to rescind consent, but the withdrawal of consent will not affect the legality of processing carried out prior to consent being withdrawn.[210] The PIPL obligates personal information handlers to attain separate consent whenever "the purpose, manner, and type of handling changes," or when processing sensitive data.[211]

In the absence of consent, personal data can still legally be processed if one of the other legal grounds enumerated in the GDPR or PIPL is available.[212] The common legal grounds between the GDPR and PIPL are those where processing is required in performing a contract in which the data subject is a party, when processing is necessary to comply with a statutory obligation to which the controller is subject, for journalistic purposes, or when processing is necessary to protect certain private and public

[204]GDPR Art. 3.
[205]PIPL, Art. 3.
[206]Cal. Civ. Code § 1798.140(c).
[207]*Comparison: CCPA vs. GDPR*, Clarip https://www.clarip.com/data-privacy/california-consumer-privacy-act-gdpr-comparison/ (last visited June 4, 2022); PIPL Art. 13.
[208]Chander, Kaminski, & McGeveran, *supra* note 5, at 1747.
[209]GDPR Art. 4(11); PIPL Art. 14; Cal. Civ. Code § 1798.140(h).
[210]GDPR Art. 7(3); PIPL Art. 14.
[211]PIPL Art. 14; Laird, *GDPR vs China's PIPL*.
[212]GDPR Art. 6(1); PIPL Art. 13.

interests.[213] Of course, the interpretation of public interests may differ between the EU and China. Specifically, the PIPL permits processing "where necessary to respond to sudden public health incidents or protect natural persons' lives and health or the security of their property, under emergency conditions," while the GDPR splits the justification into "necessary in order to protect the vital interests" of a natural person and "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".[214]

3.5 Notice Requirements

Individuals have a right to know about the uses and collection of their data under the CCPA, the PIPL, and the GDPR, although the specific information and delivery methods differ.[215] Individuals must be notified of the name and contact information of their data controller, the purpose and legal ground for the processing, and information regarding the other rights they have, and how they can exercise them.[216] This information must be conveyed in simple intelligible language.[217] Under the GDPR, data controllers must also give detailed information regarding the collection and processing, including whether it was collected directly or through a third party.[218] The GDPR requires data controllers to provide information such as contact information, the contact details of the data protection officers, the purposes of the processing and its legal basis, and, where applicable, the fact that the personal data will be transferred to a third party.[219] The PIPLs notice requirements are generally similar to the GDPRs. The CCPA requires businesses to notify individuals of the categories of personal information collected, the intended use for each category, and further notice for any collection of additional categories of personal information or use of personal information for unrelated purposes.[220] The PIPL provides an exemption to the requirement to notify when personal data must remain confidential, and the GDPR permits member states to set out rules for professional secrecy.[221]

3.6 Right of Access

The CCPA, the PIPL, and the GDPR each offer individuals a right of access, also known as a right of disclosure, to their personal information from business entities processing or handling their personal information. Under the CCPA, consumers may request disclosure of their personal information and "receive additional details regarding the personal information a business collects and its commercial purposes, including any third parties with which it shares or sells information".[222] Under the GDPR, consumers may request a copy of their information and obtain information on how their data is being

[213]GDPR Art. 85(1); PIPL Art. 13(5).
[214]See footnote above.
[215]Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart,* Thomson Reuters (2018); PIPL Art. 17.
[216]GDPR Art. 13(1); PIPL Art. 17.
[217]GDPR Art. 12(1); PIPL Art. 17.
[218]GDPR Art. 13-14.
[219]GDPR Art. 13.
[220]Cal. Civ. Code §§ 1798.100(a)-(b), 1798.105(b), 1798.110, 1798.115, 1798.120(b), 1798.130, and 1798.135; *CCPA and GDPR Comparison Chart*, BakerHosteler LLP (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf
[221]GDPR Art. 90; PIPL Art. 18.
[222]*CCPA and GDPR Comparison Chart*, BakerHosteler LLP (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf *see* Cal. Civ. Code §§ 1798.100(d), 1798.110, 1798.115.

processed.[223] A response to an access request under the GDPR must be done without "undue delay and in any event within one month [but up to three if necessary] of receipt of the request," while the PIPL only states the information should be provided "in a timely manner".[224] The CCPA gives businesses 45 days to respond to a consumer request for access, extendible for another 45 days upon notice to the consumer.[225]

3.7 Right to Deletion/Erasure

Each of the laws permits individuals to request their data to be deleted by a controller under certain circumstances. While the time frame and procedure of this right differ across these three laws, the legal grounds for invoking this right are similar.[226] The GDPR and the PIPL grant a deletion right in certain enumerated circumstances (six and five such circumstances, respectively), while the CCPAs deletion right can be exercised at any time, but may be refused by a business (on one of eight grounds).[227] Under all these laws, a requested party can refuse the request in order to protect freedom of expression, comply with legal obligations, establish legal claims, or use the information to further the public interest.

3.8 Right to Correction

The right to correction, found in all three laws, allows citizens to correct or complete their personal information which is inaccurate or incomplete.[228] The PIPL goes further to require personal information handlers to verify the personal information prior to correcting it.[229]

3.9 Right to Object to, or Restrict, Processing

Under the right to restrict processing, citizens may refuse the handling of their personal information, limit the use of their personal information, and withdraw consent at any time. Under the GDPR, a data subject's objection "must be on grounds relating to [their] particular situation".[230] Under the PIPL, individuals may object to their personal information being handled upon notification of handling, unless the law or regulations provide for such processing.[231] Under the GDPR, individuals may also object to their personal data being used for direct marketing purposes. The PIPL requires businesses to provide options not based on an individual's personal characteristics for marketing or algorithmic recommendations.

The CCPA does not provide an enumerated right to restrict processing, but it requires companies to allow individuals to opt-out of the "sale" of personal information, where "sale" is defined broadly to

[223]GDPR Art. 15.
[224]GDPR Art. 12(3); PIPL Art. 45(2).
[225]Cal. Civ. Code § 1798.130(a)(2).
[226]*See* GDPR Art. 17; PIPL Art. 47; Cal. Civ. Code § 1798.105.
[227]Cal. Civ. Code § 1798.105(d).
[228]GDPR Art. 16, 19; PIPL Art. 46; Cal. Civ. Code § 1768.106.
[229]*See footnote above.*
[230]GDPR Art. 21(1).
[231]PIPL Art. 44.

include disclosing for valuable consideration.[232] Businesses must offer a "Do Not Sell My Personal Information" link in a clear and conspicuous location on the business website homepage.[233] The CPRA adds the right to opt-out of the use and disclosure of sensitive information.[234] The CCPAs requirement that a business must disclose the purpose for which it is collecting personal information, can lay the foundation for a claim for "unfair or deceptive acts or practices" under the Federal Trade Commission Act, if the business uses it for non-specified purposes.[235]

3.10 Automated Decision-Making

Under the GDPR, data subjects have the right to not be subjected to automated decision-making including profiling, which produces legal effects concerning them or significantly affects them, unless the decision: (1) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (2) is authorised by Union or member state law; or (3) is based on the data subject's explicit consent.[236]

The PIPL requires a personal information protection impact assessment prior to using personal information to make automated decisions.[237] It also requires that such automated decision-making "shall not impose unreasonable differential treatment on individuals in terms of transaction price and other transaction conditions," and that the results must ensure "fairness and justice".[238] Where automatic decision-making has "a significant impact on individual's rights and interests," the individual can demand an explanation and also reject the use of solely-automated decision-making.[239]

While the CCPA has no special provisions on automated decision-making, the CPRA authorises regulations allowing consumers to opt out of the use of automated decision-making, including profiling, and allowing consumers to request "meaningful information about the logic involved in those decision-making processes".[240]

3.11 Right to Data Portability

The CCPA, PIPL, and GDPR all give individuals the right to request their personal information in a format that allows it to be moved from one data controller to another. Under the GDPR, data subjects have the right to receive their personal data from a data controller in a "structured, commonly used, and machine-readable format".[241] The PIPL gives individuals the right to "request that their personal information be transferred to a personal information handler they designate, meeting conditions of

[232]Cal. Civ. Code §§ 1798.135, 1798.140(ad).
[233]Cal. Civ. Code § 1798.135.
[234]Cal. Civ. Code §§ 1798.120, 1798.121.
[235]*See* 15 U.S.C. § 45(a)(1).
[236]GDPR Art. 22.
[237]PIPL Art. 55.
[238]PIPL Art. 24.
[239]*See footnote above.*
[240]Cal. Civ. Code § 1798.185(a)(16).
[241]GDPR Art. 20; *CCPA and GDPR Comparison Chart*, BakerHosteler LLP (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf

the [Cyberspace Authority of China]".[242] The CCPA requires businesses to provide the requested information in a usable format so that consumers can transmit the information without any hindrance.[243]

3.12 Privacy by Design, Data Minimisation, and Data Retention

The GDPR adopts "privacy by design," requiring organisations to design their systems to minimise data and implement other data protection principles.[244] The GDPR adopts the principle of data minimisation, requiring that personal data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".[245] Under the GDPR, data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, except for scientific, historical, or statistical purposes.[246]

Neither the PIPL, nor the CCPA requires privacy by design explicitly. However, various principles in both the PIPL and the CCPA (as revised by the CPRA) support key aspects of such an approach. The PIPL requires collection to be "limited to the minimum scope for the purpose of processing".[247] Under the PIPL, "The retention period of personal information shall be the minimum period necessary for achieving the purpose of processing, except for where the retention period of personal information is otherwise provided for in laws and administrative regulations".[248]

While the CCPA did not mandate data minimisation, the CPRA prohibits businesses from collecting more personal information than "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed . . . ". [249] The CPRA also prohibits businesses from retaining "a consumer's personal information or sensitive personal information . . . for longer than is reasonably necessary" for the purpose for which it was collected.[250]

3.13 Cybersecurity and Data Security

The GDPR requires data controllers and processors to take "appropriate technical and organisational measures" to establish security that is appropriate to the risk of the data processing.[251] The PIPL broadly mandates that processors "take necessary measures to ensure their security".[252] The CCPA implicitly mandates security by authorising individuals to sue businesses when their "nonencrypted or nonredacted personal information ... is subject to an unauthorised … disclosure as a result of the

[242]GDPR Art. 20.
[243]Cal. Civ. Code §§ 1798.100(d); 1798.130(a)(2).
[244]GDPR Art. 25.
[245]GDPR Art. 5(c).
[246]GDPR Art. 5(1)(e).
[247]PIPL Art. 6.
[248]PIPL Art. 19.
[249]Cal. Civ. Code § 1798.100(c).
[250]Cal. Civ. Code § 1798.100(a)(3).
[251]GDPR Art. 24(1).
[252]PIPL Art. 9.

business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information".[253] The CCPA provides both a private right of action and statutory penalties of USD $100 to $750 per incident for such data breaches.[254] The CPRA will require businesses whose processing of personal information presents significant risk to privacy and security, to conduct annual cybersecurity audits.[255]

In the event of a breach, all three jurisdictions mandate that the business reports the breach to the relevant authorities.[256] The GDPR requires this report to occur within 72 hours, unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons," in which case they do not have to report it at all. The PIPL requires handlers to "immediately adopt remedial measures, and notify the departments responsible."[257] There is no requirement to notify affected individuals of a breach under either the GDPR or the PIPL if data controllers subsequently adopt protection measures to effectively avoid the harms created by the breach.[258] The GDPR states that data processors must notify their data controller if the processor becomes aware of a breach, but the PIPL is silent on what an entrusted party must do in such a situation.

3.14 Data Protection Impact Assessments

The GDPR and PIPL both require impact assessments before sensitive information or a special category of data can be processed, or a legally binding evaluation of a natural person based on automatic processing can be made, or other high-risk data processing activities.[259] These assessments include a description of the purpose and manner of the processing, an analysis of the necessity and proportionality of the processing in relation to the purpose, and an appraisal of the processing's impacts and risks to the data subject's rights, freedoms, and interests.[260] The GDPRs assessments require a description of risk-addressing measures, while the PIPLs require an assessment of whether the "protective measures undertaken are legal, effective, and suitable to the degree of risk, and impact assessments reports and treatment records should be kept for at least three years".[261]

While the CCPA does not require data protection impact assessments, the CPRA will require businesses to conduct "regular" risk assessments if the business's "processing of consumers' personal information presents significant risk to consumers' privacy or security".[262]

[253]Cal. Civ. Code § 1798.150.
[254]*See footnote above.*
[255]Cal. Civ. Code § 1798.185(a)(15).
[256]GDPR Art. 33(1); PIPL Art. 57.
[257]*See footnote above.*
[258]GDPR Art. 34(3); PIPL Art. 57.
[259]GDPR Art. 35(1-3); PIPL Art. 55.
[260]GDPR Art. 35(7); PIPL Art. 56.
[261]*See footnote above.*
[262]Cal. Civ. Code § 1798.185(a)(15).

3.15 Record Keeping

While the GDPR requires data controllers and processors to maintain a record of all their processing activity, the PIPL requires personal information handlers to record the handling of sensitive personal information, personal information used in automated decision-making, transfers of personal information to other handlers or abroad, and other "personal information handling activities with a major influence on individuals". [263] Regulations implementing the CCPA require businesses to keep records for at least two years of customer data requests. [264]

3.16 Enforcement

All three laws assign accountability to the data controllers and empower enforcement authorities to ensure their compliance. The GDPR explicitly states that controllers are responsible for and must demonstrate compliance with GDPR Article 5(1), which enumerates, *inter alia*, principles of lawfulness, fairness, and transparency.[265] Under the GDPR, fines may be imposed up to 20 million Euro, or four percent of a company's annual worldwide revenue, whichever is higher.[266] The GDPR permits individuals to receive compensation for both material and immaterial damages from data protection violations. While class actions are not common in Europe, the GDPR authorises representative actions brought by non-profit bodies, and member states are introducing such mechanisms.[267]

Similarly, the PIPL states that information handlers "shall bear responsibility for their personal information handling activities and adopt the necessary measures to safeguard the security of the personal information they handle".[268] The PIPL authorises fines of up to ¥50 million or five percent of annual turnover, though it does not specify if this is with respect to national or global turnover, or how to choose between these two parameters for the upper limit.[269] The PIPL also authorises authorities to suspend a business or revoke its license to operate, and to fine individual corporate officers as well.[270] Violations of the PIPL can be entered into credit files and published.[271]

The CCPA authorises civil penalties of up to USD $2,500 per violation or up to USD $7,500 per intentional violation, which can quickly add up to hundreds of millions or even billions.[272] In the United States there is no private right of action for affected individuals to enforce most elements of the CCPA, though privacy class actions can be maintained for security breaches under the CCPA and on the basis of violations of other laws or contractual obligations.[273]

---

[263]GDPR Art. 30(1); PIPL Art. 55.
[264]California Consumer Privacy Act Regulations § 999.317.
[265]GDPR Art. 5(1)-(2).
[266]GDPR Art. 83(5).
[267]*Privacy, GDPR and class actions: recent developments in the Netherlands*, LOYENS LOEFF (Dec. 15, 2021), https://www.loyensloeff.com/insights/news--events/news/privacy-gdpr-and-class-actions-recent-developments-in-the-netherlands/
[268]PIPL Art. 9.
[269]PIPL, Art. 66.
[270]PIPL Art. 66(1)-(2).
[271]*See* PIPL Art. 67.
[272]Cal. Civ. Code § 1798.155.
[273]Cal. Civ. Code § 1798.150.

The GDPR, CCPA, and PIPL all empower enforcement authorities to ensure compliance. The GDPR relies on independent Data Protection Authorities (DPAs) established by each member state, as well as a European Data Protection Board and European Data Protection Supervisor.[274] The PIPL empowers the CAC for comprehensive planning and co-ordination, and departments of the State Council to enforce the PIPL for various industries, and also empowers relevant departments at the county and regional level to perform personal information protection duties.[275] The CCPA establishes the California Privacy Protection Agency (CPPA), which has administrative power, authority, and jurisdiction to implement and enforce the CCPA.[276] As indicated above, the three agencies have the power to levy large fines for non-compliance.[277] Each agency may also carry out investigations, issue warnings, order controllers or handlers to adopt measures to correct any infringements, and impose temporary or permanent bans on processing.[278]

3.17 Representative

The GDPR requires data controllers and processors to designate in writing a representative in the European Union if the controller or processor is established outside the EU, unless the processing activity is occasional, or the controller or processor is a public authority or body. The PIPL also requires that extraterritorial personal information handlers designate a representative in China and notify the relevant department of their contact information. There is no such requirement in the CCPA.

3.18 Data Protection Officers

The GDPR requires controllers and processors processing personal information at a 'large scale' to name a Data Protection Officer.[279] The PIPL similarly requires processors that process a high quantity of information to appoint a Personal Information Protection Officer responsible for supervising data protection, with that quantity threshold to be specified by the Cyberspace Administration of China.[280] The CCPA does not require the naming of a data protection officer.

3.19 Children's Personal Information

All three bodies of law provide special protections for the personal information of children. The GDPR requires parental consent for the processing of children's data, as does the PIPL. The CCPA relies on a federal statute, the Children's Online Privacy Protection Act (COPPA), to impose a parental consent requirement, but supplements that with respect to the sale of children's personal information.[281]

---

[274]GDPR Art. 51(1).
[275]PIPL Art. 60; Ken Dai and Jet Deng, *The Comparison Between China's PIPL and EU's GDPR: Practitioner's Perspective*, JDSupra (2021), https://www.jdsupra.com/legalnews/the-comparison-between-china-s-pipl-and-2189482/
[276]Cal. Civ. Code § 1768.155.
[277]GDPR Art. 82, 83(5); PIPL Art. 66; Cal. Civ. Code §§ 1798.199.75, 1798.155.
[278]GDPR Art. 58(1)-(2); PIPL Arts. 61, 64, 66; Cal. Civ. Code § 1798.199.40.
[279]GDPR Art. 37(1) (stating a controller or processor is required to appoint a DPO when processing operations "require regular and systematic monitoring of data subjects on a large scale").
[280]PIPL Art. 52 (stating an information handler is required to appoint a PIPO when controllers handle personal information "reaching quantities provided by the CAC").
[281]*See* Cal. Civ. Code § 1798.120.

Under the GDPR, children must receive an age-appropriate privacy notice and their personal data is subject to heightened security measures.[282]

Each of the bodies of law defines the age of consent for data privacy differently. The GDPR allows member states to choose a range from 13 to 16.[283] The PIPL sets the age at 14. The CCPA requires a parent or guardian to affirmatively authorise the sale of personal information of a child under 13 years of age, and for children between 13 and 16, requires that the child must affirmatively authorise the sale of their personal information.[284]

3.20 Cross Border Data Flows

Both the GDPR and the PIPL provide significant conditions on the flow of personal data outside the country. The CCPA contains no restrictions on cross-border data flows.

The GDPR provides an extensive set of regulations for the transfer of personal data for processing outside the country. Organisations can only transfer data on the basis of one of a number of mechanisms provided by the GDPR. The simplest basis for transfer is an adequacy decision by the European Commission, declaring a foreign country's data protection law and practice as essentially equivalent to that of the European Union. But only a handful of countries have received such a ruling, so most organisations rely on alternative mechanisms. The most popular such mechanism is the use of standard contractual clauses, model clauses approved by the European Commission by which the transferring parties agree to protect the data under EU standards. A second popular mechanism is binding corporate rules, which permit transfers within a corporate group upon approval of a data protection authority. The GDPR also provides additional alternatives through certifications and codes of conduct. Finally, the GDPR permits transfers based on "derogations" from the rules, but these are intended to be limited.

The PIPL offers a variety of mechanisms to permit data exports.[285] First, the Cyberspace Administration of China (CAC) may have cleared the transfer after a security assessment. Second, the exporter has been certified for data protection under the CAC regulations. Third, the exporter enters into a contract with standard contractual terms promulgated by the CAC. Lastly, laws or regulations may authorise additional circumstances for such transfers. Critical Information Infrastructure Operators (CIIO) and personal information handlers handling large quantities of personal information, however, face stricter regulations.[286] These rules reveal the "cyber-sovereignty" and national security goals implicit in the PIPL.[287]

[282]GDPR Art. 8(1).
[283] GDPR Art. 8.
[284]Cal. Civ. Code § 1798.120.
[285]PIPL Art. 38.
[286]PIPL Art. 40.
[287]Adam Segal, *When China Rules the Web: Technology in Service of the State*, FOREIGN AFF., Sept.-Oct. 2018, at 11-12.

cerre Centre on Regulation in Europe

04

NON-PERSONAL DATA GOVERNANCE: FACILITATING NON-PERSONAL DATA FLOWS?

Moritz Hennemann

Data – as codified information – is a strategic resource for private actors and state actors alike in the 21st century; it defines competitiveness. While the governance of personal data is very much determined by data protection law(s), non-personal data governance ranges from enabling to limiting the use of data – and the routes and calibrations taken, are of utmost importance for a free flow of data for open, competitive, and potentially global data markets, and – last, but not least – data law harmonisation.

EXECUTIVE SUMMARY

Non-personal data regulation is underpinned by different parameters than personal data regulation. After a long period of non-regulation of non-personal data, current regulatory activities mark a turning point in this regard. Despite the current set of rules in many countries, one should, however, not (continue to) see non-personal data and personal data as two fundamentally separate spheres. It is rather preferable to construct data regulation regarding the respective ecosystems involved. National security data (may it be personal or non-personal) is underpinned by fully different parameters than (personal or non-personal) data trade. Therefore, it must be stressed that it is of utmost importance to find the 'right' conceptual entry gate to data regulation, as the central pillars of data regulation shape any regulatory instrument built thereon.

Any data law instrument should define, in line with the G7 digital ministers, a trusted free flow of data as the conceptional starting point. It should be aimed at facilitating data use, promoting data markets, removing barriers to entry in data markets, and countering (contractual) imbalances. Data regulation should especially – with the aim of enabling (more) data sharing and data re-use – refrain from establishing an absolute or IP right to data. Data law should rather focus on building trust in data flows. Trust is only possible through a combination of a sensible institutional framework and a convincing substantial setting. Regarding the latter, the data economy is inconceivable without trusted actors (such as, data intermediaries, data commons, or data trusts). With regard to substance, data law regulation must make transparent decisions about data monetisation and participation in data-generated value. Data regulation seems to be most convincing if it values the role of the person "producing" the data and should set incentives for enablers and users of data markets. Data regulation should mirror the specific needs of small and medium-sized companies, especially the transaction and implementation costs coming along with regulation and, it must carefully weigh safeguards for fundamental rights and trade secrets and consider any (anti-)competitive effects of the proposed legislation.

An international non-personal data law instrument can be considered a realistic goal. Non-personal data is not as 'culturally determined' as data protection and data privacy law. Unlike personal data, non-personal data is an informational good that is, and can be, traded between private parties without fundamental constrains. Non-personal data is therefore currently regulated mainly by means of contract law – and should ideally be regulated by an 'enabling' and 'trust-building' contract law. Any exchange should, as a general rule, be linked to private-to-private interactions. Such interactions may be framed and incentivised by contract law instruments. In this regard, regulation should at least include non-binding standard terms for data contracts. Non-personal data law regulation might also consider contractual default rules for data contracts, mandatory standard, or unfair contract terms

vis-à-vis small and medium-sized enterprises and/or consumers, instruments boosting competitive data markets (access rights, for instance), data localisation rules, and data transfer rules. It might also be accompanied by specific rules regarding access, or use, of specific research institutions and governmental actors. In addition, rules on data trusts, or data intermediaries, facilitating data contracts are another road to follow.

In the meantime, before coming to an international agreement, a non-binding soft law instrument should be promoted. Different preparatory work for a respective instrument has already been done. Especially, model laws or model contract rules can serve as a catalyst for data markets.

1. THE STATUS QUO

Data – as codified information – is a strategic resource for private actors and state actors alike in the 21st century. Countries and businesses are competing and co-operating with respect to different kinds of data. Data defines competitiveness.[288]

> A CERRE stakeholder points to the fact that data flows play an invisible, but structural role in how global and domestic communications and digital transactions function. because of how the global internet was built and has evolved, cross border data flows occur as part of almost every online communication or activity, often including those which are wholly domestic.[289]

The *governance* of data, therefore, ranges from enabling to limiting the use of data. The routes and calibrations taken from policy decisions are of utmost importance – constantly having the need to bear individual, economic, industry-related, and societal effects, as well as security and the common good in mind.

The different regional perspectives create variance and complexity in adopting a common framework or sharing the practices across the world – where lead indicators are the cultural context, social norms regarding laws and rules, the stage of development in the respective setting between the Global North, East, West, and South, as well as the legislation systems in each country or region.

1.1 Data Regulation

With regard to personal data, we have seen a rising awareness of data protection and data privacy issues at the global level. As a consequence, a worldwide trend of regulation and a clear pattern of instruments can be identified – leading to data protection and data privacy regulation in more than three-quarters of the world's countries to date.[290] Intertwined with infrastructural decisions, countries are using different regulatory approaches.[291] However, the European Union must be – for "good and bad"[292] – regarded as a trendsetter with its General Data Protection Regulation (GDPR), in this 'race to the top' (or even to the 'GDPR').[293] Furthermore, the global convergence of data and privacy regulation has triggered respective harmonisation prospects.[294]

---

[288] Cf. e.g. Liu, The Rise of Data Politics: Digital China and the World, 54 Studies in Comparative International Development (2021), 45-63.
[289] The statements of CERRE's stakeholders referred to in this paper are either direct, indirect and / or reformulated quotations handed in by stakeholders in response to a questionnaire dealing with issues of Global Governance for the Digital Ecosystems.
[290] Cf. Greenleaf, Global Tables of Data Privacy Laws and Bills, 7th ed. (2021) and the Research Centre for Law and DIgitalisation (ed.), Global Data Law Maps by Continent, https://www.jura.uni-passau.de/en/faculty/institutes-and-centres/fredi/global-data-law/
[291] Cf. Chander/Kaminski/McGeveran, Catalyzing Privacy Laws, 105 Minnesota Law Review (2021), 1733-1802; Erie/Streinz, The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance, 54 NYU Journal of International Law and Politics (2021), 1-92; Bygrave, The 'Strasbourg Effect' on data protection in light of the 'Brussels Effect': Logic, mechanics and prospects, 40 Computer Law & Security Review (2021), 105460, https://www.sciencedirect.com/science/article/pii/S0267364920300650
[292] Cf. Mannion, Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets, 53 Vanderbilt Journal of Transnational Law (2020), 685-711.
[293] Cf. Schwartz, Global Data Privacy: The EU Way, 94 NYU Law Review (2019), 771-818; Hennemann, Wettbewerb der Datenschutzrechtsordnungen – Zur Rezeption der Datenschutz-Grundverordung, 84 RabelsZ (2020), 864; Schwartz/Peifer, Transatlantic Data Privacy Law, 106 Georgetown Law Journal (2017), 115-179; Gstrein/Zwitter, Extraterritorial application of the GDPR: promoting European values or power?, (2021) 10(3) Internet Policy Review, https://policyreview.info/pdf/policyreview-2021-3-1576.pdf.
[294] Cf. the WP 2 on the (potential) global convergence of data protection / data privacy rules.

Non-personal data has not gained similar regulatory attention in the last decades. Its enormous value and relevance, however, is undisputed. Examples of non-personal data are countless – as representative of this, one might point to machine data (an engine, for instance)[295], weather data, or agricultural data. Traditionally, non-personal data was not specifically regulated – based on the correct notion that non-personal data must be grounded in other parameters than personal data.

> Consequently, a CERRE stakeholder points to the fact that non-personal data does not pose the level of risk that warrants (…) regulatory intervention (as data protection law), and regulation should encourage more use of such data.

Rather, non-personal data generation and exchange were (and are) captured by contractual agreements between private parties (data license agreements).[296] To some extent, Trade Secret Law played an accompanying role in this regard offering an additional layer of protection. Non-personal data *as such* was (and is), however, not captured by traditional IP rights. An absolute right and/or a 'property-like' right to data is not provided for (the status quo that is favoured by most).[297] In addition, competition law rules on information exchange might form another barrier – but are not specifically targeted at non-personal data.[298] Next to *hard law*, *soft law* instruments with respect to data contracts or data rights, have only been developed recently.[299]

1.2 The Current Major Limitations

Despite the low level of regulatory boundaries, non-personal data sharing has, by far, not unleashed its potential.[300] It is assumed that data does not flow as 'smoothly' as possible.

> A CERRE stakeholder points to the issues in question: the risk of the misuse of non-personal data, fostering innovation through encouraging more non-personal data use and protection for investments, or industrial policy which seeks to facilitate the sharing of non-personal data across the digital ecosystem.

[295] If not linked to an individual.
[296] Cf. Schur, Die Lizenzierung von Daten – Der Datenhandel auf Grundlage von vertraglichen Zugangs- und Nutzungsrechten als rechtspolitische Perspektive, GRUR (2020), 1142-1152; Hennemann, Datenlizenzverträge, RDi 2021, 61-70; Czychowski/Winzek, Rechtliche Struktur und Inhalt von Datennutzungsverträgen – Datenwirtschaftsrecht III: Der Vertrag über ein neues Elementarteilchen?, ZD (2022), 81-90.
[297] Cf. in this regard, Amstutz, Dateneigentum, AcP 218 (2018), 438-551; Drexl et al., Data Access and Data Ownership: Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate (Max Planck Institute for Innovation and Competition Research Paper No. 16-10), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165; Kerber, Governance of Data: Exclusive Property vs. Access, International Review of Intellectual Property and Competition Law (2016), 759-762.
[298] Cf. generally Crémer/Montjoye/Schweitzer, Competition policy for the digital era: Final report (European Commission, 2019), https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf
[299] American Law Institute and European Law Institute (eds), 'ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights' (ALI-ELI Principles), https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf
[300] Cf. the Explanatpory Memorandum by the European Commission, Proposal for a Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, 1 et seq.

Several reasons for limits to the flow of data are given.[301] It is easy to copy and hard to control. It is therefore observed that companies are unwilling to share their data with specific parties, as it includes an inherent risk of disclosure to third parties.

This was also underlined by a CERRE stakeholder pointing to the lack of control which goes along with a respective sharing of data.

The EU Commission, for example, points to "[b]arriers to data sharing[,] lack of incentives for data holders to enter voluntarily into data sharing agreements, uncertainty about rights and obligations in relation to data, costs of contracting and implementing technical interfaces, the high level of fragmentation of information in data silos, poor metadata management, the absence of standards for semantic and technical interoperability, bottlenecks impeding data access, a lack of common data sharing practices and abuse of contractual imbalances with regards to data access and use."[302] Furthermore, data sets are hard to value, especially for small and medium-sized companies, and, additionally, legal uncertainties exist.

It is, however, partly uncertain whether this current state is a consequence of a market failure (especially not offering respective (trusted) services), or whether the existing regulatory framework hinders a functioning market for non-personal data exchanges. The European Union assumes the first, many others point to the latter.[303] In favour of the latter, it is widely highlighted that, in particular, the "blurry" lines between non-personal and personal data[304] also lead to significant uncertainty with respect to non-personal data trade.

A CERRE stakeholder points to the fact data protection authorities have construed the concept of personal data and anonymisation in an absolute manner; therefore, there is actually very little information where consumer-facing organisations may have the certainty that they are not personal data.

A legally certain 'way out' from data protection law (through anonymisation, for example) is rather difficult to find. Also, taking into account the significant fines for data protection breaches (compare Article 83 GDPR), companies in doubt, apply the data protection law regime to their data (self-limiting exchange and trade options). This effect is even stronger for small and medium-sized companies which are, relatively speaking, hit harder by the regulatory compliance costs of horizontal regulation, such as the GDPR.[305]

[301] Cf. in detail and with further references, Hennemann/v. Ditfurth, Datenintermediäre und Data Governance Act, NJW (2022), 1905-1910.
[302] European Commission, Proposal for a Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final, 17.
[303] Cf. Hennemann/v. Ditfurth, Datenintermediäre und Data Governance Act, NJW 2022, 1905-1910.
[304] Purtova, The law of everything. Broad concept of personal data and future of EU data protection law, 10 Law, Innovation and Technology (2018), 40-81.
[305] Cf Gal/Aviv, The Competitive Effects of the GDPR, 16 Journal of Competition Law and Economics (2020), 349-391.

This situation was also highlighted by a CERRE stakeholder pointing to the fact that small and medium-sized companies are not always able to meet the high, multiple, and manifold regulatory burdens in data transfer scenarios.

In the future, however, Articles 4 (1) and (5), 5 (6) and (7) of the European Union's Data Act, might actually "force" data holders to take a stand on the question of whether personal data or non-personal data is at stake in order to avoid the (further) fines on the basis of Article 33 of the Data Act. The norm obliges member states to enact fining rules regarding violations of the Data Act. For a variety of violations and within their area of competence, data protection authorities might fine entities up to a sum possible under the GDPR (Article 83) (Article 33 (3) Data Act).

1.3 Setting A New Tone: The European Union Data Strategy

The long period of non-regulation of non-personal data has come to an end with the strategic efforts of the European Union in the last few years. Especially (but obviously not only), the European Union has pursued an extensive data regulation agenda since 2017.[306] First and foremost, its goals were set out in the 2020 European Data Strategy.[307] In that strategy, the European Union points to a multi-field regulatory approach. Different instruments – partly linked to specific fields of law, partly setting out rules independently of a specific field of law – have been presented (at least as drafts) since then[308]: (1) Data Governance Act (DGA)[309]; (2) Digital Markets Act[310]; (3) Digital Services Act[311]; and (4) Data Act (DA).[312] The first three were presented as first drafts in 2020 – the first of which has just been enacted, while the second and third are close to being passed. The Data Act has just been presented recently and negotiations (and debates) are on-going. With its regulatory advancement, the European

[306] European Commission, Building a European Data Economy, COM (2017) 9 final.
[307] European Commission, A European Strategy for Data, COM (2020) 66 final.
[308] Cf Picht/Richter, EU Digital Regulation (2022): Data Desiderata, GRUR Int. (2022), forthcoming.
[309] Final version: Regulation (EU) 2022/868 of the European Parliament and the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act); compare, for an analysis, Hennemann/v. Ditfurth, Datenintermediäre und Data Governance Act, NJW 2022, 1905-1910. Draft version: European Commission, Proposal for a Regulation of the European Parliament and the Council on European data governance (Data Governance Act), COM/2020/767 final and European Parliament legislative resolution of 6 April 2022 on the proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) (COM(2020)0767 – C9-0377/2020 – 2020/0340(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2022-0111_EN.html compare, for an analysis, Graef, I. and Gellert, R. (2021), 'The European Commission's Proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing', https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3814721 Richter, Europäisches Datenprivatrecht: Lehren aus dem Kommissionsvorschlag für eine „Verordnung über europäische Daten-Governance", ZEuP 2021, 634-666.
[310] European Commission, Proposal for a Regulation of the European Parliament and the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.
[311] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A277%3ATOC; compare, for an analysis, Cauffman, C. and Goanta, C. (2021), 'A New Order: The Digital Services Act and Consumer Protection' 12 *European Journal of Risk Regulation* 758-774.
[312] European Commission, Proposal for a Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final; compare, for a first analysis, Bomhard, D. and Merkle, M. (2022) 'Der Entwurf eines Data Acts: Neue Spielregeln für die Data Economy' *Recht Digital* 168-176; Hennemann/Steinrötter, Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?, NJW 2022, 1481-1486.

Union is aiming for a coherent and all-embracing data regulation – enabling and setting the boundaries for data flows and different European Data Spaces.[313]
Whilst the DMA must be classified as a Competition Law instrument in the broader sense, and the DSA can be seen as an update to the eCommerce-Directive 2000/31/EC[314] (and therefore an extended intermediary regulation), it is important to note that the Data Act and the Data Governance Act, form new central pillars of the emerging field of data economy law.[315] Both instruments must be considered together as they are intertwined in a different way, and it must be regarded as rather unfortunate that the Data Act is still in the legislative process whilst the Data Governance Act is already final. The Data Act, as well as the Data Governance Act, aim at facilitating (more) data use. This goal is first and foremost pursued by new (compulsory) data access rights of users of data-generating Internet of Things-products, also to the benefit of third parties.[316] What is remarkable, is that both instruments do not – from the outset – differentiate between non-personal and personal data. The Data Act, as well as the Data Governance Act, set general rules with respect to data and data-related actors.

1.4 Scope of this Paper

Against this background, this paper analyses prospects of facilitation of data flows by (non-personal) data regulation. To this end, fundamental strategic decisions are mapped – and set into context, also – with respect to the consequences of (more) regulation and/or bundles of regulation.

The following focal points of (current) regulatory approaches – and their contribution to facilitating data flows – shall be examined: (1) the attribution of data by contractual means (by compulsory data license agreements, for example), (2) legal incentives as well as duties to share data (by compulsory data access rights and FRAND conditions for data access, for instance), and (3) actor-specific regulation (such as by creating a specific framework for data intermediaries[317]). The assessment, thereby, focusses on specific data law instruments – especially the current EU proposal of a Data Act and the recently enacted Data Governance Act – and excludes concurring legal fields, such as, competition law developments.[318]

In addition, the role of soft law instruments shall be examined, as well as the extent to which these might serve as catalysts for non-personal data law harmonisation – and thereby also to data flows. To this end, central pillars and institutional options of a (harmonised) data law regulation are also presented.

---

[313] European Commission, Commission Staff Working Document on Common European Data Spaces, SWD(2022) 45 final. Cf also the proposal for the European Health Data Space, see https://ec.europa.eu/health/publications/proposal-regulation-european-health-data-space_en
[314] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178 (17.7.2000), 1–16.
[315] Cf Streinz, The Evolution of European Data Law, in: Craig/de Búrca (eds), The Evolution of EU Law, 3rd ed. (2021), 902-936; Steinrötter, Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts, RDi 2021, 480-486.
[316] The notion of access to data (instead of an absolute right to data) is a mainstream line in data law; compare with Drexl, Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz – Teil 1 und 2, NZKart (2017), 339-344 and 415-421; Hartl/Ludin, Recht der Datenzugänge, MMR (2021), 534-538.
[317] Cf Richter/Slowinski, The Data Sharing Economy: On the Emergence of New Intermediaries, IIC (2019), 4-29.
[318] Cf in this regard, Crémer/Montjoye/Schweitzer, Competition policy for the digital era: Final report (European Commission, 2019), https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

2. THE GOAL: (WHICH) FREE FLOW OF DATA?

Entry point to the assessment shall be a reiteration of the goals to pursue. It is generally accepted – and not doubted here – that data carries an enormous potential that is currently not fully exploited. It can be used in different scenarios and by many users or applications at the same time. Data is a multiple-use good with unique economic characteristics. Consequently, a *(trusted) free flow of data* is a commonly favoured and discussed strategic goal[319] that was recently and prominently highlighted by the G7 Digital Ministers,[320] as well as by the Declaration for the Future of the Internet.[321]

A CERRE stakeholder is of the opinion that data localisation requirements undermine economic rights by eroding the ability of consumers and businesses to benefit from access to both knowledge and international markets, and by restricting data transfers and giving governments greater access to, or control over, locally stored information. Preventing cross-border data flows inhibits countries from benefiting from the research and knowledge base of other countries, as well as opportunities for foreign direct investment, and the ability for local firms to expand their customer bases in foreign markets.

However, this goal goes along with different challenges (and not only if personal data is at stake where data protection law draws boundaries for the flow). These challenges also mirror regulatory instruments to which we will turn afterwards.

2.1 Level 1 - Non-Binding

First, if free flow of data is only understood as the general possibility to exchange non-personal data with others, typically only public (security) laws draw limiting lines (such as, with regard to national security), a specific non-personal data regulation – and a respective harmonisation – would not be needed.

2.2 Level 2 - Model and/or Default Rules

Second, if the *free flow of data*, however, is understood as a process to be intensified by private actors, facilitating the exchange of data becomes a regulatory goal. Specific non-personal data law regulation might include non-binding standard terms or contractual default rules for data contracts, thereby offering a 'legal infrastructure' to facilitate private decisions to exchange data. Harmonising respective

[319] Cf World Economic Forum, Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flow (White Paper, May 2020), https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data_Flows_2020.pdf Ducuing, Beyond the data flow paradigm: governing data requires to look beyond data, Technology and Regulation (2020) 57-64, https://techreg.org/article/view/10995/11969 Le Chapelle / Porciuncula, We need to talk about data: Framing the debate around free flow of data and data sovereignty (Internet & Jurisdiction Policy Network, April 2021), https://www.internetjurisdiction.net/uploads/pdfs/We-Need-to-Talk-About-Data-Framing-the-Debate-Around-the-Free-Flow-of-Data-and-Data-Sovereignty-Report-2021.pdf

[320] https://www.bmvi.de/SharedDocs/DE/Anlage/K/g7-praesidentschaft-final-declaration-annex-1.pdf?__blob=publicationFile.

[321] https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet

standards might be regarded as a fruitful and non-interventionist approach for which, inter alia, the work of the American Law Institute and the European Law Institute might serve as a starting point.[322]

2.3 Level 3 - Actor-Specific or Mandatory Rules

Third, if the *free flow of data* is also understood as being limited by structural challenges, especially the market participants' trust in specific actors, guaranteeing this trust becomes a goal of regulation, and might be pursued by regulating specific actors (as it is done for data intermediaries by the Data Governance Act of the European Union), or by mandatory standard terms and/or Contract Law rules (as it is proposed by the European Union through the Data Act).[323]

2.4 Level 4 - Attribution of Data

Fourth, if the *free flow of data* is also seen as being limited by an adequate legal attribution of data to a specific entity or person – attributing information is a challenge! – one might consider respective legal instruments reaching from compulsory data license agreements (as it is proposed in the Data Act by European Union) to some kind of 'data property' or 'data IP rights'[324].

2.5 Level 5 - Compulsory Access Rules

Fifth, if having a *free flow of data* is also regarded as an objective to achieve and a goal to further, even independently of contractual agreements (as it is regarded by many – including the European Union in its Data Act proposal), *compulsory access* to data comes into play.[325] Access rights are then granted on specific terms for competitors, non-competitors, and/or consumers. As data is *valuable* to many, but often only in the hands of some, respective compulsory data access, at least in private-to-private scenarios, bears an inherent and obvious tension with the data holder's legitimate interest of protecting its data as (potential) trade secrets.

2.6 Level 6 - Location Rules

Sixth, if data is seen as a unique production factor of a state and/or within a specific territory, geographical parameters to (or better: against) a *free flow of data* will be considered in the following three ways:[326] (1) the location where data has to be stored (data localisation)[327]; (2) to which extent a

---

[322] Cf American Law Institute and European Law Institute (eds), 'ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights' (ALI-ELI Principles), https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf.

[323] Cf also Grünbeger, Data access rules: The role of contractual unfairness of (consumer) contracts, in: BMJV / MPIIC (eds), Data Access, Consumer Interests and Public Welfare, (2021), 253-286

[324] Zech, Building a European Data Economy – The European Commission's Proposal for a Data Producer's Right, 9 Zeitschrift für Geistiges Eigentum (2017), 317-330

[325] Ducuing, Mandating Data Sharing to Establish Data as an Infrastructural Resource, 21 Network Industries Quarterly (2019), 21-25. Cf also Specht-Riemenschneider, Data access rights – A comparative perspective, in: BMJV / MPIIC (eds), Data Access, Consumer Interests and Public Welfare, (2021), 401-438

[326] Cf generally Chander/Lê, Data Nationalism, 64 Emory Law Journal (2015), 676-739.

[327] Svantesson, Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines (OECD Digital Economy Papers No. 301, December 2020), https://www.oecd-ilibrary.org/docserver/7fbaed62-en.pdf?expires=1647463200&id=id&accname=guest&checksum=FFCA9BE79F45C3292A48D204C46A3A33

data transfer is allowed[328]; and (3) to which extent foreign actors – may it be businesses or state authorities – might request access to the data in question.[329] It must be noted that especially demands for data localisation are partly an outcome of protectionist policies, but may also – next to security concerns – derive from the desire to oppose an "exploitation" of data by foreign actors. Generally, however, respective approaches can come along with anti-competitive effects.[330]

[328] Cf Art. 44 et seq. GDPR.
[329] Cf Art. 27 Data Act.
[330] Cf Cory/Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, ITIF (2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

3. FACILITATING DATA FLOWS BY REGULATION? SELECTED INSTRUMENTS

Along these lines, regulators have to decide which levels of data regulation are activated and combined. Central structural choices are to be taken. Inter alia, it must be decided whether the regulation covers only non-personal data or applies to personal and non-personal data alike. From a strategic level – and with an effects-based approach – it also has to be evaluated whether regulation is practically suitable and/or capable of being understood and whether the amount of regulation and/or the bundle of different types of regulation, is bearable by those obliged by the regulation (especially by small and medium-sized companies). The practical consequences of regulation are often underestimated.

This notion is also underlined by a CERRE stakeholder pointing to the need to draft regulation in a way that mirrors the actual realities of modern complex datasets, and that can also be understood and applied by non-experts.

On this basis, selected instruments of non-personal data regulation shall be evaluated. These following instruments form not only the most fundamental decisions to take, but also mirror the aforementioned central fields of regulation (independent of a specific territory): actors, data, data contracts, and data access. It shall be assessed whether and to what extent, respective instruments might facilitate (more) data flows. Practical examples of these instruments are derived from the recent EU data regulation proposals.

3.1 Facilitating Data Flows by Attributing Non-Personal Data?

The increased value of data as a resource and the perception of data as a tradable good has – probably not surprisingly – led to the desire of attribution of data to both people and specific entities. Such attribution is, however, far from easy: first, does one attribute the data as such (syncretic level) or the information codified (semantic level)?; second, how is it defined to whom the data is attributed (producer or owner of a product or machine, or the user, and so on)?; and third, in what way is such an attribute effectuated (through IP, contract, or other ways)?[331]

3.1.1 Absolute data rights

It is by now generally accepted that an absolute right to data is not favourable. Such an absolute right would potentially not facilitate data flows. The notion of an absolute right to data is contrary to the specific characteristics of data (non-rival and non-consumable), as well as to the general non-proprietary nature of information. It is furthermore assumed that a respective absolute right would rather manifest the strong position of those actors producing data or (*de facto*) controlling data.

[331] This is not to say the other legal fields might add layers of protection, e. g. trade secret law.

A potential alternative to an absolute right of data is the extension of existing IP rights, especially the database right.[332] This does, however, echo similar objections to the ones mentioned above and seems not to be – being a helpful indication – an approach favoured by the European Union. The Data Act proposal stipulates in Article 35:

> *"In order not to hinder the exercise of the right of users to access and use such data in accordance with Article 4 of this Regulation or of the right to share such data with third parties in accordance with Article 5 of this Regulation, the sui generis right provided for in Article 7 of Directive 96/9/EC does not apply to databases containing data obtained from or generated by the use of a product or a related service."*

The Data Act generally does not seek to introduce a respective absolute right. Recital 5 reads:

> *"This Regulation should not be interpreted as recognising or creating any legal basis for the data holder to hold, have access to, or process data, or as conferring any new right on the data holder to use data generated by the use of a product or related service. Instead, it takes as its starting point the control that the data holder effectively enjoys, de facto or de jure, over data generated by products or related services."*

However, Article 2 No. 6 of the Data Act defines the data holder as:

> *"a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data".*

Thereby, the Data Act underlines the *de facto*-power of (often) the manufacturer of the product to access data or make it available.[333] It is important to note that this definition of data holder might be considered counter-intuitive, as the actual user (defined by Article 2 No. 5 as "a natural or legal person that owns, rents or leases a product or receives a services") could also have been regarded as the one holding the data, especially as he or she (often) physically controls the (Internet of Things) product.

3.1.2 (Compulsory) Data license agreements

The Data Act, however, actually accepts the access of the data holder and stipulates the requirement of a compulsory data licence agreement as a (potentially or at least in theory) counter-balancing instrument. One might argue that this leads (contrary) to a *de facto*-attribution of non-personal data. The data holder willing to use the data must conclude a contract with the respective person specified by law (the 'user', for instance). The recent proposal of the Data Act introduces a respective compulsory data license agreement like this. Article 4 (6) of the proposal reads: "The data holder shall

[332] Cf Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors (May 2022), https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf
[333] Cf Specht-Riemenschneider, Der Entwurf des Data Act: Ein großer Wurf in die falsche Richtung?, GRUR (2022), 937-938.

only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user." This requirement leads to a *de facto*-attribution of non-personal data (which is on this basis – at least conceptually – even more protected than personal data).[334]

This approach goes along with fundamental difficulties. First and foremost, it must be determined which kind of data is "generated by its use". Second, the contractual partner, or user, must be defined. According to Article 2 (5) of the proposal, 'user' refers to "a natural or legal person that owns, rents or leases a product or receives a service". It is unclear, however, how to determine the user if more than one person is at stake (for example, the owner, regular driver, and a spontaneous driver of a smart car might all be different persons). Therefore, this proposal must be carefully evaluated. The potential economic consequences coming along with the requirement of a data licence agreement are not to be underestimated.

A CERRE stakeholder points to the fact that contract law, as well as intellectual property law, should underpin the relationship between contracting parties in the provision of services or the conditions of transfer or use of non-personal data and IP rights associated thereto. Policymakers may – according to the stakeholder – also look to foster the use of existing data licensing agreements, such as the Community Data License Agreement (CDLA) and other best practices. These might usefully draw from experience and working methods established in other communities, such as the open-source community. Community-led efforts in drafting and gathering feedback (for instance via the Linux Foundation, Apache Foundation and Eclipse Foundation) and central administration of the licenses by the Open Source Initiative, which have resulted in a set of tried and trusted licenses that are widely used.

3.1.3 Free use of non-personal data

Both aspects (3.1.1 and 3.1.2) stem from the notion that the role of the person "producing" the data (such as, the one who generates the data by its use) is valued, may it be by contractual requirements or by (opt-out)options, re-use and monetisation, and so on. The status quo does not follow this route but leaves the different actors without a special attribution. Non-personal data can be used by those having (legally) gained access to the data (for example by 'production' or contractual access rights) without the need to conclude a respective contract – a setting (only) serving those with access to large amounts of data.

[334] Hennemann/Steinrötter, Data Act – Fundament des neuen EU-Datenwirtschaftsrechts?, NJW (2022), 1481-1486.

3.2 Facilitating Data Flows by Fostering Co-operation?

Data flows might be facilitated by compulsory elements of data regulation.

3.2.1 Compulsory data access rights

The most intrusive instrument to enable a flow of data is compulsory access rights. As indicated above, such a compulsory instrument goes along with compliance efforts for those obliged.

> Consequently, one CERRE stakeholder indicated that mandatory data sharing should be (or stay) voluntary. Another one pointed to a significant increase in compliance costs, whilst at the same time, it was doubted whether users enjoy commensurate benefits in terms of meaningful transparency.

Nevertheless, a respective right offers non-data holding companies, especially small and medium-sized companies, but also consumers, the perspective of access to data from larger data holders, and thereby a monetisation option.

> One CERRE stakeholder acknowledges that in the data economy, large amounts of data are typically collected and processed by large and incumbent industry players. Smaller players generally (but not always) struggle to compete as barriers to entry are high.
>
> Another CERRE stakeholder argues that industrial policy should facilitate incentives and certainty regarding the safeguards that shall apply to sharing data, and should create the space for innovators in the digital economy, be they local champions or multinational companies with significant investments in the EU, to engage in that sharing in a way that makes sense for their business, innovation, investments, and the interests of the people who rely on their services.

Data access rights have been widely promoted on these lines – and it is, at this moment in time, the path the Data Act is pursuing data generated by the use of Internet of Things-products. Article 4 (1) of the proposal reads:

> *"Where data cannot be directly accessed by the user from the product, the data holder shall make available to the user the data generated by its use of a product or related service without undue delay, free of charge and, where applicable, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible."*

In addition, Article 5 (1) of the proposal offers the user the possibility to request access to the benefit of a third party – making Articles 4 (1) and 5 (1) a set of portability rights for non-personal and personal data, complementing Article 20 of the GDPR.

A CERRE stakeholder points to the fact that data portability can help promote online competition and encourage the emergence of new services, and that regulation should guarantee portability, and they also added that clear rules – mirroring practical needs – are needed.

3.2.2 Fairness tests

Compulsory access rights can, but do not have to, be accompanied by safeguards for data access on a contractual basis. Article 8 of the Data Act stipulates in this regard: "Where a data holder is obliged to make data available to a data recipient under Article 5 (…), it shall do so under fair, reasonable and non-discriminatory terms and in a transparent manner (…)." Even stronger is the protection of small and medium-sized companies (and one might extend this to consumers):

> *"A contractual term, concerning the access to and use of data or the liability and remedies for the breach or the termination of data related obligations which has been unilaterally imposed by an enterprise on a micro, small or medium-sized enterprise (…) shall not be binding on the latter enterprise if it is unfair. A contractual term is unfair if it is of such a nature that its use grossly deviates from good commercial practice in data access and use, contrary to good faith and fair dealing." (Article 13 (1) and (2)).*

Respective requirements are two-fold as, on the one hand, they might incentivise data recipients and small and medium-sized companies as well as, on the other hand, de-incentivise companies to act as data holders in the first place.

Consequently, one CERRE stakeholder indicated that data exchange should be pursued on a value-metric.

3.2.3 Data altruism

An additional option to strengthen data flows is to incentivise altruistic data sharing (such as, for research purposes). The Data Governance Act pursues this approach explicitly and offers the possibility to become registered as a data altruistic organisation (Article 16 and what follows). These organisations are explicitly supported by the Data Governance Act as the Act stipulates in Article 15 with regard to the various obligations of data intermediaries (compare in detail sub-section 3.3.2 below):

> *"This Chapter shall not apply to recognised data altruism organisations or other not-for-profit entities insofar as their activities consist of seeking to collect data for objectives of general interest, made available by natural or legal persons on the basis of data altruism unless those organisations and entities aim to establish commercial relationships between an undetermined number of data subjects and data holders on the one hand and data users on the other."*

3.3 Facilitating Data Flows by Boosting Specific Data Actors?

Data flows might also be facilitated by activating or boosting specific data actors.

3.3.1 Data users

One option is to activate the user of a specific product and/or related service for the sharing of data for instance, by passing data on to third parties, allowing direct access to the uses, and/or third parties. The Data Act generally follows this approach – and puts the user (next to the data license agreement) in a conceptionally rather strong position by letting him decide whether or not a third party (data recipient) shall get indirect or direct access to data, compare this to Article 5 (1) of the proposal:

> *"Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available the data generated by the use of a product or related service to a third party, without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time."*

It must be noted that at least the experiences with user activation so far do not indicate a strong push for data sharing. Empirical evidence regarding the right to (personal) data portability according to Article 20 of the GDPR, indicates that users are not aware of their right and/or do not exercise it to a notable extent.[335] However, this right is only granted to natural persons, whereas the data access right by the Data Act is also open to commercial users, which will not only (more likely) be aware of their right, but might exercise it with a clear-cut commercial incentive.

3.3.2 Data Intermediaries

Another actor-specific activation is pursued by the Data Governance Act. The European Union is of the opinion that data sharing is not pursued due to a lack of trust in the market. By establishing far-reaching and tight rules for data intermediaries (Article 10 and what follows) the European Union seeks to build this much needed trust. It seems, however, rather unlikely at this moment in time that the duties only-approach of the Data Governance Act will fulfil its set goal.[336] The Act does not actually incentivise the activity of a data intermediary (for example, by establishing exceptions from the GDPR or from Competition Law). The Act is therefore still yet to demonstrate its suitability 'in practice'.

[335] Lusza, Datenportabilität: Bedeutungsvoll, aber kaum bekannt, bidt Blog, https://www.bidt.digital/blog-datenportabilitaet/.
[336] In detail Hennemann/v. Ditfurth, Datenintermediäre und Data Governance Act, NJW (2022), forthcoming.

A CERRE stakeholder is of the opinion that it is too early to assess whether the Data Governance Act is setting a standard that should be followed in countries outside the EU; and that once it is applicable, one will see if it works in practice, if it hampers or boosts innovations and its effects on the economy in general. For any data sharing model to work – when personal data is involved – it is indispensable according to the stakeholder – to address the GDPR impact on how the data would be collected by the data intermediary for subsequent data sharing and purposes.

A sensible regulatory framework, therefore, must value the eminently useful role of data intermediaries (such as data platforms).

4. PROSPECTS OF HARMONISATION

Finally, the prospects for non-personal data law harmonisation shall be considered.

A CERRE stakeholder highlights in this regard that co-regulation on data governance is a valuable, indeed critical, tool to address data-related issues.

4.1 International Law

At least for non-personal data (which does not seem to be as 'culturally determined' as data protection or data privacy law), it is not unimaginable that an international law instrument is designed and concluded. Different preparatory work for a respective instrument has already been done by different actors. First and foremost, the existing sets of regulation might serve as one (but only one) option for a potential international instrument. Second, existing and future model laws serve as a catalyst for a respective instrument (compare with section 4.2 below).

4.2 Model Laws

Model laws can be used as a source of inspiration for legislations, contract drafters, and non-state actors alike. A *menu* of data rights, data sharing rights, and data access rights is, for example, offered by the ALI-ELI Principles for a Data Economy.[337] Potentially, further institutions (for instance, UNCITRAL, UNIDROIT) might develop similar instruments.

4.2.1 General advantages

Respective soft law instruments also often serve harmonisation purposes and processes, offering legislators the option to copy the model law in its entirety, or in parts. If many countries have already taken a respective route, that might also lead to a 'legislative network effect' (where countries do not want to 'bother' their enterprises with double or too many standards). Furthermore, respective rules might be used by private parties as either a blueprint or starting point for contractual agreements (as model clauses like the Community Data License Agreement) or – depending on the respective conflicts of law, civil procedural law, and the law of arbitration – they might even serve as applicable law for non-personal data contracts. As non-binding rules, however, one should not overestimate the role of these instruments. They are often not enforceable in courts or by arbitration as law, but only as contractual clauses, if so chosen (and with respect to the applicable mandatory contract law).

4.2.2 Drafting process

Generally, it is worth noting that the quality of the proposals is highly dependent on the drafting process. In order to be accepted by all sides, it must be assured that the model laws are drafted in a balanced and co-operative way – taking into account all sides – from industry to consumers and from

[337] American Law Institute and European Law Institute (eds), 'ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights' (ALI-ELI Principles), https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf

governmental to non-governmental actors. In this regard, and to guarantee a relevant outcome, it is of utmost importance that the instruments are drafted by experts representing a variety of perspectives and stakeholders: traditional and tech industries, small and medium-sized enterpises, start-ups, consumers, NGOs, goverments, legislators, data regulators, competition authorities, and ICT regulators.

4.3 Parameters for Substantial Non-Personal Data Regulation

In substance, these instruments face the difficult task to decide on the goals with respect to non-personal data set out above (compare section 2). All instruments will likely share the notion that data carries an enormous potential that is currently not fully exploited and that it is a multiple-use good with unique economic characteristics. Beyond this understanding, one must consider and value the different cultural contexts, different social norms with regard to laws and rules, the stage of development in the respective setting in the Global North, East, West, and South, as well as the legislation systems in each country or region.

A CERRE stakeholder highlights the need to incentivise the use of more non-personal data over personal data, and enhance the environment for the use of privacy enhancing technologies, like a reasonable standard of anonymisation. Over-regulation of non-personal datasets—like subjecting non-personal data to similar obligations as for personal data—will have, according to the stakeholder, a chilling effect on data sharing.

It is also of utmost importance to evaluate the amount and/or density of regulation in general and whether, and to what extent, cumulative (and partly contradicting) sets of norms are practically capable of being handled.

A CERRE stakeholder is of the opinion that it is concerning how many obligations companies have and need to comply with. It is getting difficult to operate, which could in turn end up hampering innovation.

It is, at this moment, in time not foreseeable whether the EU model of data regulation (as set out by the EU Data Strategy) presents a model that takes the lead globally (as the GDPR did). Doubts are undeniable regarding the different shortcomings of current proposals.

A CERRE stakeholder is of the opinion that the EU model of data regulation is rapidly transforming from one that has been grounded in principles and taken a proportionate, risk-based approach, to one which is overly protectionist, prescriptive and revisionist. This shift from a globalist perspective to one based on open strategic autonomy, marks a pivot from shoring up the global digital economy where innovation delivers for society and people based on the ability to invest in research and collaboration across borders, to a more isolationist approach with punitive regulation for companies that have invested in the market. The stakeholder therefore asserts that the new model of EU data regulation is not the vehicle for achieving a more harmonised regulatory landscape globally.

4.4 Recommended Pillars of Non-Personal Data Regulation

On the basis of the toolboxes set out in sections 2 and 3 above, as well as with regard to the parameters set out under 4.3, the following pillars of non-personal data regulation should be considered.

4.4.1 Fundamentals

- Non-personal data regulation should be aimed at data as (structurally) codified information;
- Any non-personal data law instrument should define a trusted free flow of non-personal data as the conceptional starting point, whilst taking into account public (security) and IP laws as limiting lines;
- Non-personal data law regulation should be aimed at facilitating non-personal data use, promoting data markets, removing barriers to entry to data markets, and countering (contractual) imbalances;
- Non-personal data law regulation should refrain from establishing an absolute right or IP right in non-personal data, in order to promote data sharing and data reuse on the one hand, and to avoid anti-competitive effects on the other hand;
- Non-personal data law regulation should, however, value the role of the person 'producing' the data (that is, the one who generates it by their use) for example through requirements of a contractual agreement, (opt-out-)options, re-use and monetisation, and so on; and
- Non-personal data law regulation should regulate non-personal data (mainly) by means of contract law.

4.4.2 Minimum Instruments

- Non-personal data law regulation should at least include non-binding standard terms for data contracts;
- Non-personal data law regulation should set incentives for enablers of data markets (especially data intermediaries); and

- Non-personal data law regulation should calibrate the personal scope of obligations set in such a way, that small and medium-sized companies are not confronted with a disproportionate amount of regulatory transaction and implementation costs.

4.4.3 Optional instruments

- Ideally, non-personal data law regulation does include contractual default rules for data contracts;
- Ideally, non-personal data law regulation should include mandatory standard terms and unfair contract term rules vis-à-vis small and medium-sized enterprises, as well as vis-à-vis consumers;
- Ideally, non-personal data law regulation should pave the way for competitive data markets, for example, by granting access rights on distinct terms for competitors, non-competitors, and/or consumers, while bearing the legitimate interest of protecting trade secrets in mind.
- Non-personal data law regulation might consider – not as a rule, but as an exception – data location rules in specified cases, but must also bear its anti-competitive effects in mind, and must consider and balance those carefully against other goals pursued;
- Non-personal data law regulation might consider reciprocal rules on (required levels for) data transfer;
- Non-personal data law regulation might consider specific rules for non-personal data access or use, to the benefit of (independent) research institutions and under the condition that this type of data is only used for its specified purposes; and
- Non-personal data law regulation might consider specific rules for non-personal data access or use by governmental actors, especially with regard to clearly defined cases of an exceptional need.

4.5 Institutional Setting

In order to discuss and/or boost (harmonised) rules on non-personal data, different institutional settings might be considered to serve as an open forum for an exchange of ideas and models. Recent developments with regard to global co-ordination in the fields of data protection and data privacy might serve as an example in this respect.[338] In spring 2022, the Global Cross-Border Privacy Rules Forum was established.[339] The United States and EU also reached a Trans-Atlantic Data Privacy Framework[340] and a EU-United States Trade and Technology Council was established.

[338] Cf. also Chander/Schwartz, Privacy and/or Trade (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4038531
[339] See: https://www.commerce.gov/news/press-releases/2022/04/statement-commerce-secretary-raimondo-establishment-global-cross-border
[340] See: https://ec.europa.eu/commission/presscorner/detail/es/ip_22_2087

Against this background, one might consider the establishment of an International Governance Body to ensure cross-border learning and knowledge sharing within all stakeholders. Different options could be pursued – either cumulatively or alternatively:

4.5.1 Global committee / «Data 20» («D20») initiative

First, a committee at global level could be considered to facilitate the learning and sharing, and provide consultative roles to different stakeholders who requires the knowledge to establish non-personal data framework for instance, the establishment of a Global Non-Personal Data Alliance or a horizontal « Data 20 » (« D20 ») initiative.

4.5.2 Alliance of private actors

Second, an alliance of private actors could be considered. A respective alliance could develop models of practice; big, medium, and small, as well as local, national, and multinational corporations (in addition to non-commercial private actors) might serve as an indicator as to the need for regulation. It is however important to note that any proposal of such an alliance might have the disadvantage that consumer and societal interests might not be mirrored if non-commercial private actors are not involved. A respective initiative could therefore sensibly only cover a field without any (direct) consumer-relevance; especially in countries of the Global South, where consideration must be given to the role of local enterprises and the share of foreign company activity and investment.

4.5.3 NGO-led forum

Thrid, NGOs could be encouraged to tackle non-personal data governance. NGOs could promote the awareness of private acors for different options or frameworks regarding personal data (critically important to small and medium-sized enterprises). Furthermore, states, legislators, and societies could be balanced and provide inclusive insights and assistance on non-personal data governance.

SUMMARISED RECOMMENDATIONS

1. An international non-personal data law instrument should be the long-term and realistic goal as non-personal data does not seem to be as "culturally determined" as data protection or privacy laws.
2. In the meantime, a (non-binding) soft law instrument should be promoted. Different preparatory work for a respective instrument has already been done. Model laws or contract terms can especially serve as a catalyst for data markets.
3. The quality of respective instruments is highly dependent on the drafting process. In order to be accepted by all sides, it must be assured that the model laws are drafted in a balanced way – taking all sides and stakeholders into account.
4. Potential instruments must consider and value the different cultural contexts, different social norms with regard to laws and rules, the state of (economic) development in the respective settings in the Global North, East, West, and South, as well as the legislative systems in each country or region.
5. Against this background, fundamental, minimum, and optional pillars of non-personal data regulation – serving this purpose – have been stipulated.[341]
6. Any non-personal data law instrument should define a trusted free flow of non-personal data as the conceptual starting point. It should be aimed at facilitating non-personal data use, promoting data markets, removing barriers to entry to data markets, and countering (contractual) imbalances.
7. Non-personal data law regulation should refrain from establishing an absolute right or an IP right in non-personal data, but should regulate non-personal data (mainly) by means of contract law. Therefore, any regulation should at least include non-binding standard terms for data contracts.
8. Non-personal data law regulation should value the role of the person "producing" the data and should set incentives for enablers of data markets. Non-personal data law regulation should mirror the specific needs of small and medium-sized companies, especially the transaction and implementation costs coming along with regulation.
9. Non-personal data law regulation might also consider contractual default rules for data contracts, mandatory standard terms and unfair contract terms vis-à-vis small and medium-sized enterprises and/or consumers, instruments boosting competitive data markets (access rights, for example), data localisation rules, data transfer rules, as well as specific rules re access/use of research institutions and governmental actors.

[341] Cf Sec. 4.4.

10. One might consider an open forum for the exchange of ideas and models on data law regulation to ensure learning and knowledge sharing within all stakeholders across the board. Different options could be pursued – either cumulatively or alternatively (such as, the Global Committee, Alliance of Private Actors, a NGO-led forum, or a horizontal « Data 20 » (« D20 ») initiative).
11. Such an open forum could drive the development of non-personal data law regulation and models with the objective to set minimum requirements and timelines (to enable all parties to embrace the framework).
12. Clearly defined incentives will be essential to expedite the onboarding process for all actors.

cerre Centre on Regulation in Europe

05

DIGITAL SOVEREIGNTY AND THE NORMATIVITY OF DATA GOVERNANCE

Marcelo Thompson

1. INTRODUCTION

Harmonisation approaches to data governance suggested in earlier papers of this workstream resonate with recent proposals in the scholarly literature advocating for a global data privacy agreement — either as an agreement anchored in the WTO system,[342] or as an expression of a new Digital Bretton Woods agreement.[343] These proposals respond to difficulties in reconciling differences between global data privacy regimes, as well as between the more substantive regimes among them, and the principles that inform the international trade system. They speak of ideals of *universality* that the networks of technology and trade are taken to reflect, given the equalising potential of such networks, as enablers of "development of human capital" and "democratisation of opportunity throughout the world". As Plato gestured in "The School of Athens", these proposals point up.

These are met, however, with a global proliferation of initiatives that — from data localisation to the regulation of online harms — highlight the *embeddedness* of global data flows in political communities through which such flows pass. This embeddedness of data flows traverses realms from the purely distributive — revealing the fact that equality of opportunity is but an illusion, and instead what unfettered data flows really enable are the network effects at the heart of surveillance capitalism — to the more broadly normative. Here, in the views of such communities, development is not true development if their conceptions of how arguably universal values should be interpreted, in light of material circumstances and cultural traditions that define them, are not taken into account. Conversely, as Aristotle did in the famous painting by Raphael, such communities gesture down.[344] Earlier parts of this workstream have focused on the legal dimension of harmonisation initiatives and pointed to possibilities of convergence in the legal realm. This paper focuses instead on the interplay between legal and *extra-legal,* or otherwise *political*[345] ideals, which, wittingly or not, are at the heart of contemporary discussions on data governance and *sovereignty*. What will be observed here is the myriad of ways in which extra-legal considerations pervade data governance debates and challenge the prospects of harmonisation initiatives that treat such considerations as *exceptions* to what is

[342] See, e.g., Anupam Chander and Paul M. Schwartz, *Privacy and/or Trade*, 90:1 U. CHI. L. REV. (forthcoming 2023).
[343] See, e.g., Douglas W. Arner, Giuliano G. Castellano, and Erik Selgas, *The Transnational Data Governance Problem*, 36 Berkeley Tech. L. J. (forthcoming 2023).
[344] Such communities' views of justice, as will be noted shortly, reflect a comprehensive conception of the political within which the state is seen to have a role in promoting the good. With Aristotle as well, they can hold that "while the state came about as a means of securing life itself, it continues in being to secure *the good life*". Aristotle, The Politics bk. I, at 59 (T.A. Sinclair ed., T.J. Saunders trans., Penguin Press rev. ed. 1992) (c. 350 B.C.E.). In fact, even from a purely distributive perspective, one can hardly think of a contemporary community that does not reflect principles of *redistribution*–for instance, through taxation and public services—going beyond what unfettered market ideals would enable.
[345] All ideals with which this paper is concerned are, in a way, political. They concern the foundational values of different political communities, and conceptions prone to confrontation—and hopefully reconciliation— between these communities. More broadly than political ideals, however, they are *moral* ideals. Here we adopt Ronald Dworkin's understanding that "law is a branch of political morality, which is itself a branch of a more general personal morality, which is in turn a branch of a yet more general theory of what it is to live well"—of ethics, that is (see, Ronald Dworkin, Justice for Hedgehogs 5 (2011). For Dworkin, the unifying problem that concerns ethics, and thus all such branches into which it is divided, is the problem of what makes up a *good life*. As law itself exists within such a broader political, moral, and ethical universe, when we speak of the extra-legal here, we are speaking of portions of the political that transcend the objective determinacy of legal rules—the province, that is, of legal positivism. These are realms where law opens itself to the broader universes to which it belongs, where evaluative questions spring, unadorned by the certainties of the rule of law, into the universe of interpretation—and, indeed, of responsibility for interpretation (*id.* at 99-122) as a dimension of authoring common life that is as good as it can be. This is the realm where we now stand.

otherwise portrayed as the *rule* — and thus the importance that such considerations be taken seriously.

As a corollary of such an observation, this part makes two recommendations. The first is that a trade agreement in the realm of data governance — which, without question, would be a most important development — be coupled with *another agreement*, under the United Nations System, on the *human rights* aspects of data governance. Such an agreement would work as a platform for cross-cultural dialogue, enabling different interpretations of the relations between human rights in the realm of data governance — and between the underlying values that define these interpretations – to come into contact with one another. In the first instance, this would be a procedural agreement, whose objective would be the pursuit, not so much of a common denominator, but instead of a common understanding, of the reasonable *differences to be had* within and between each country's margins of appreciation concerning human rights involved in data governance questions. Such levels of understanding are something one can scarcely find in the realm of trade alone.

The second recommendation takes an initiative in development within the EU — the Gaia-X project, a cloud-based data infrastructure to "allow for the secure, open, and sovereign use of data"[346] — as an example of how technological systems can be designed to reflect human values, here values reflecting sovereignty, rather than the other way around. While data localisation initiatives often raise technical concerns and are often associated with the demise of the Internet as we know it, the second recommendation is to avoid technological determinism when thinking about human values in the context of harmonisation processes.

In other words, harmonisation initiatives should reflect human values rather than seek to assimilate human values to assumedly immutable configurations of technological artefacts. Despite all the good the Internet has brought about, there is no reason to think its configurations should remain unchanged, particularly where the lack of granularity in such configurations operates to the detriment of otherwise valuable goals whose pursuit it disables.[347]

The structure of this paper proceeds as follows: part 2 introduces the general problem of legal indeterminacy at the heart of digital sovereignty questions; part 3 demonstrates how this problem expresses itself in the major jurisdictions this workstream has so far focused on, pointing to concrete ways in which data governance regimes in these jurisdictions invite forms of normative evaluation that contrast with the ideals of neutrality these jurisdictions are typically thought to reflect; part 4 demonstrates how such jurisdictions pursue data localisation initiatives as guarantees of the application of values of sovereign importance, but also points to models within such initiatives that

[346] *FAQ*, GAIA-X: A Federated Secure Data Infrastructure, https://gaia-x.eu/faq/ (last visited Sep. 29, 2022).
[347] The literature speaks here of an idea of plasticity. See e.g. Lawrence Lessig, Code Version 2.0 61 (2006). The point has been made in the literature on the philosophy of technology that technological artefacts have a dual dimension, as both material and normative/teleological constructs. Designers bear responsibility for finding the best justification for how both dimensions interact. Thus, function ascription is generally a highly normative affair, and this is no different in relation to the Internet. See, e.g., Peter Kroes and Anthonie Meijers, *The Dual Nature of Technical Artefacts*, 37 Studies in History and Philosophy of Science 1-4 (2006) and Wybo Houkes, Knowledge of Artefact Functions, 37 Studies in History and Philosophy of Science 102-113 (2006).

seek to address the technical difficulties that data localisation is usually associated with. Finally, while important contributions in recent scholarly literature suggest the adoption of a trade-based approach to data governance, part 5 explains how challenges of indeterminacy *also* affect such approaches, and puts forward concrete institutional solutions, within the realm of human rights, to address such challenges, in relation to the international trade system and beyond. Part 6 contains the conclusions.

2. SOVEREIGNTY AND LEGAL INDETERMINACY

Harmonisation challenges and opportunities in relation to personal and non-personal data flows depend as much on the language of the law as on the law's pauses — on the interstices and zones of penumbra that invite one to make sense of the open texture of legal categories.[348] It is here, in these realms of indeterminacy, that one confronts ideas such as *harm*, *fairness*, *legitimacy*, *national security*, *public morals*, and, uniting them all, *the public interest*, which are to be found all over the frameworks concerning different forms of regulation of online data flows.

Making sense of these ideas naturally requires forms of normative evaluation extending beyond the strictly legal. As a result, legal indeterminacy is also a profoundly *culturally relative* affair. It requires that the character of different forms of intervention on information flows be assessed against the backdrop of the values, and indeed of the *value-systems*, that such interventions seek to enable or uphold. This is so because decisions concerning such forms of normative evaluation are a manifestation of both legal and *political* power that characterises relations of *sovereignty*[349] — a power founded upon the relations between the institutional offices of the state and *the people* who are the repository of their authority.[350] Such decisions concern ideals that, while not impervious to evolution through mutual and self-understanding, are not alienable ideals either, susceptible to being reframed on demand at the behest of other cultures.

Hence, while earlier papers in this workstream have pointed to domains where the harmonisation of global rules concerning online data flows may appear more promising, due to the objectivity of legal frameworks that increasingly start to look more like each other — which is specifically the case with general data protection regimes around the world — the present part points to tensions that, left unattended, tend to preclude rather than to enable harmonisation. It also points to the elusive nature of forms of progress that overlook such tensions and the values they mobilise.

Indeed, no real progress towards harmonisation will be possible without an open-minded and determined endeavour to reach a common understanding in realms of greater normative indeterminacy, and without the understanding as well that these *are* realms where it is legitimate that countries make decisions in accordance with the value-systems that underpin their societies. All countries *do* so, even where these are obfuscated by the apparent neutrality and objectivity of rule-of-law ideals. In the domain of international trade, for example, WTO panels and the Appellate Body have recognised in different technology-related cases that the public morals exception to trading

---

[348] See Hla Hart, The Concept of Law 124ff (1994) (discussing the idea of open texture in law).

[349] See Martin Loughlin, *Ten Tenets of Sovereignty*, in Sovereignty in Transition 55, 79 (Neil Walker ed., 2006) (noting, e.g.: "Law plays a critical role in explicating in the form of rules, regulations, rights and responsibilities the character of sovereign authority. But if we are to take seriously the nature of public law, it must be recognised that, notwithstanding certain rhetorical flourishes about the appeal to 'higher', 'fundamental' or even 'natural' law, the determination of the limits to sovereign authority, even when articulated by courts, must be political").

[350] *See footnote above*, at pp. 63-67 (noting, e.g.: "As Arendt explains, the term authority (*auctoritas*) is derived from the verb *augere* (to augment) and 'what . . . those in authority constantly augment is the foundation'. Authority therefore 'has its roots in the past'; the question of authority 'is fundamentally a question of tradition' and 'the question of tradition is inextricably related to the question of the people'". *See footnote above*, at p. 66).

rights under the General Agreement on Tariffs and Trade,[351] and the General Agreement on Trade in Services,[352] reflect "standards of right and wrong conduct maintained by or on behalf of a community or nation",[353] and thus that their content for Members "can vary in time and space, depending upon a range of factors, including prevailing social, cultural, ethical and religious values".[354] In the privacy domain, likewise, courts have spoken of an expectation of privacy being *reasonable* when "*society accepts*" certain information "should remain out of the state's hands",[355] or when such an expectation is of a kind "that *society is prepared to recognise* as reasonable".[356] Inquiring upon such standards thus necessarily entails examining the values prevailing in that society at a particular point in time.

To say so does not necessarily entail the reduction of normative values to how they find themselves materially exemplified at a particular point.[357] As concerns ensuing from network effects and relationships of dominance on the Internet illustrate very well, it is often the case that how such relationships end up instantiated is neither how they *ought* to be, nor how people would *wish* them to be so.[358] To note this is merely to recognise that, at the foundations of modern accounts of sovereignty lies the idea of the state as a device — indeed a technology[359] — for augmenting the power of citizens to uphold the values embedded in an original or hypothetical relational bond.[360] The key for our discussions here is understanding that different traditions deal with this relational foundation in different ways — and that tending to such differences is not extraneous to discussions on regulations of online data flow. Rather, it is of the essence of these discussions.

[351] General Agreement on Tariffs and Trade, (Oct. 30, 1947), 61 Stat. A-11, 55 U.N.T.S. 194 [hereinafter GATT].
[352] General Agreement on Trade in Services, (Apr. 15, 1994), Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994) [hereinafter GATS].
[353] Panel Report, *China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, ¶5.11, WTO Doc WT/DS363/R (adopted Jan. 19, 2010) [hereinafter 'China — Audiovisuals'].
[354] Panel Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶6.461, WTO Doc. WT/DS285/R (adopted Nov. 10, 2004) [hereinafter 'US — Gambling'].
[355] R. v. Gomboc, 2010 SCC 55, (2010) 3 SCR 211, para. 34 (Can.) and adopting the Court's understanding in R. v. Tessling (2004 SCC 67, [2004] 3 S.C.R. 432, para. 42 (Can.)), that reasonable "[e]xpectation of privacy is a normative rather than a descriptive standard"). *See footnote above*., paras. 34, 115.
[356] Katz v. United States, 389 U.S. 347, 361 (1967).
[357] It does not need to commit us, in other words, to views that reduce the essence of constitutions to the "actual relations of force" in place in a given society (Ferdinand Lassalle, *On the Essence of Constitutions*, 3(1) Fourth International (1942)), or in contemporary views that reduce the normativity of law to the materiality of networks (See, e.g., Bruno Latour, An Inquiry into Modes of Existence: An Anthropology of the Moderns (2013) and Kyle McGee, *On Devices and Logics of Legal Sense: Toward Socio-technical Legal Analysis*, in LATOUR AND THE PASSAGE OF LAW 61 (2015.). But compare, Marco Goldoni, The Materiality of the Legal Order (2022). For Loughlin, sovereignty has a dual dimension as both a sovereignty of capacity, which is ultimately a matter of power, and thus a matter of fact, and a sovereignty of competence, which points to the institutions of public law as indeed the great political contribution of modernity (Loughlin, *supra* note 199, at 78).
[358] Courts in the common law make a distinction between what the *public is* merely *interested in knowing* and what is genuinely *in the public interest to be known* (British Steel v. Granada Television (1981) A.C. 1096, 1168). And courts arrogate to themselves the role of identifying what truly the public interest is (Mosley v. News Group Newspapers Ltd. [2008] EWHC 1777 (QB), 135).
[359] See Carl Schmitt, The Leviathan in the State Theory of Thomas Hobbes 45 (George Schwab and Erna Hilfstein trans., Greenwood Press 1996) (noting: "[T]he idea of the state as a technically completed, manmade magnum-artificium, a machine that realizes "right" and "truth" only in itself—namely, in its performance and function—was first grasped by Hobbes and systematically constructed by him into a clear concept").
[360] See Loughlin, *supra* note 199, at 66. As noted above, Loughlin, with support in Arendt, refers to the etymology of authority (from the Latin *augere*), to make the point that what the social contract augments is the relational foundation that precedes state authority.

3. DATA GOVERNANCE BEYOND NEUTRALITY

It is important to observe, however, that differences between political traditions increasingly revolve around their self-image and conceptual representations, rather than around the reality of how they regulate data online. Ongoing debates in the United Kingdom on the regulation of online harms, for example, illustrate this well, as the proposed Online Safety Bill admits the need that platforms to tackle content that, while being legal, is nevertheless harmful.[361] In the European Union, likewise, the proposal for a new Digital Services Act[362], while avoiding obligations toward outright removal of harmful yet not necessarily illegal content, does seek to address the problem of harm in different ways. Several of the proposal's recitals and provisions recognise concerns with the publication or amplification, not only of unlawful, but also of "otherwise harmful" information and activities,[363] and establish corresponding obligations for very large online platforms.[364] They grant powers to newly created Digital Services Co-ordinators, to be established in each Member State, to request the data necessary to assess possible harms brought about by online platforms and take measures to avoid the risk of serious harm.[365] Most consequential, as well, are provisions concerning the drawing up and application of Codes of Conduct in relation to harms and systemic social risks caused by misleading information.[366]

Both the UK and EU proposals mark a departure, which has been building up throughout the last decade, not only from anarchical regulatory approaches that characterised the early days of the commercial Internet, but also from ideals of liberal neutrality that characterised subsequent, rights-based regulatory interventions at the turn of the century. Indeed, the second half of the 1990s and the beginning of the 2000s saw a proliferation of regulatory initiatives in a whole range of areas, from data protection to digital copyright, to cybercrime, which were distinctively based on the language of individual rights. Yet, such initiatives were also based on an enduring expectation that the state would not move beyond the strictly necessary for the protection of such rights.[367]

---

[361] Online Safety Bill, Bill 2022-23, HL Bill [121] (UK).

[362] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A277%3ATOC

[363] See, e.g., *id.*, recitals 5 and 52.

[364] See, e.g., *id.*, arts. 26 and 27.

[365] See, id., arts. 39 and 41. They speak of the need for "effective regulation and enforcement" that effectively identifies and mitigates "societal and economic harm" that very large online platforms can cause (recital 56), of the provision—to Digital Services Coordinators or to the Commission—of data necessary to assess "possible harms brought about by the platforms systems" (recital 64), and of the application of codes of conduct in relation to harms and systemic risks on society and democracy caused by misleading information (recital 68). Digital Services Coordinators, as noted, are empowered "to adopt interim measures to avoid the risk of serious harm" (art. 41(2)(e)).

[366] See, id., recital 68 and art. 35. The proposal for an 'Artificial Intelligence Act', also currently under deliberation, is likewise forged on a harms-based approach, where not only impacts on fundamental rights, but also harms to public interests generally, including harms that the deployment of subliminal AI-based techniques may cause to a person's physical or psychological safety—beyond, thus, a rights-based realm—are covered by the Act. Is it not a natural corollary of such an approach that, for example, the induced urge to engage in activities perceived as less socially desirable would count as harm, whereas the urge to engage in those perceived as more socially desirable would not so count? One can hardly imagine the compulsion to reading the classics of literature, subliminally induced though it might be, counting as a form of harm. See *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021)206 final (Apr. 21, 2021)., e.g., at recital 1, and arts. 5 and 67.

[367] The paradigmatic articulation of these ideals is found in the (just now 25-year-old) Clinton Framework For Global Electronic Commerce, which epitomised the affirmation of the twin ideals of technological neutrality and regulatory minimalism (e.g., defending "minimal government involvement or intervention" in the provision of Internet services, noting that "government attempts to regulate are likely to

Regulatory approaches at the turn of the century were marked by an emphasis on market liberties and a "market-based approach to structuring political and social participation"—which Julie Cohen aptly notes reflects a neoliberal governmentality.[368] More helpful for our purposes here, however, is to note how such models are based on a distinction, central to many liberal accounts, between rights and conceptions of the good, and on an enjoinment to the state to only act out of concern for rights, remaining thus neutral towards the good.[369] Within such accounts, it would be unthinkable, for example, that states could regulate content out of moral considerations or that, in matters concerning the background culture of society, they would invoke upon themselves the power to tell what is false from what is true.

The relentless development of the Internet, however—and above all the platformisation of contemporary societies[370] — have shattered the assumptions on which such accounts are based. Not only moral and otherwise evaluative considerations are enduringly and consequentially articulated everywhere in the information environment but, most importantly, the modes through which they are articulated are increasingly under the control of a handful of dominant actors who have redefined the boundaries of what should be understood as the private realm. The UK and EU approaches are an unavoidable recognition of this reality, a reflection of a profound and necessary shift in the practice — if not yet more largely in the conceptualisation — of liberal politics. They also point to a growing convergence with the regulatory approaches of other traditions, for which the distinction between the right and the good was never sustainable in the first place — China's example being most helpful for purposes of illustration.

In Western liberal societies, the focus on the right (as opposed to the good) has been reinforced by an overarching conception of the rule of law that requires the state not to distinguish between cases unless in accordance with "criteria of similarity given by the legal rules themselves".[371] It is, in other words, an ideal that prevents engagement with other, extra-legal normative categories. In China, conversely, the ideal of the rule of law is one within a wider constellation of ideals the rule of law needs to be balanced with. The most compelling articulation of this proposition can perhaps be found in the 2016 Guiding Opinions on Further Integrating Socialist Core Values into the Construction of Rule of Law, issued by the State Council and CCP Central Committee, which establishes a framework for

---

be outmoded by the time they are finally enacted, especially to the extent such regulations are technology-specific"), disapproving of the regulation of content online as a result of concerns resulting from "cultural, social, and political *difference*" (emphasis added). President William J. Clinton & Vice President Albert Gore, Jr., A Framework for Global Electronic Commerce (Jul. 1, 1997), online: https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html (last visited Jul. 25, 2022). See also Marcelo Thompson, *The Neutralization of Harmony: The Problem of Technological Neutrality, East and West*, 18:2 B.U. J. SCI. & TECH. L. (2012) (connecting ideas of technological neutrality and liberal neutrality).

[368] See Julie Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism 7 (2019).

[369] For the quintessential articulation of this separation, see John Rawls, *The Priority of Right and Ideas of the Good*, 17:4 Philosophy & Public Affairs 251 (1988), revisited in John Rawls, A theory of Justice (1971, 1999) and Political Liberalism (1993, 2005). But compare Joseph Raz, The Moreality of Freedom (1986), William A. Galston, Liberal Purposes: Goods, Virtues, and Diversity in the Liberal State (1991), and Steven Wall, Liberalism, Perfectionism, and Restraint (1998) (for approaches which, while distinctively liberal, are nevertheless critical to ideals of neutrality). See also Joseph Chan, Confucian Perfectionism: A Political Philosophu for Modern Times (2014) (putting forward a powerful attempt to reconcile the ideals of Western liberal societies with those of Confucianism).

[370] See Cohen, *supra* note 218, at 37 (characterising platforms as the "core organizational logic of contemporary informational capitalism").

[371] John Rawls, A Theory for Justice 208 (1999).

incorporating a set of Core Socialist Values[372] "into all legal and judicial process".[373] Among these, together with values such as democracy and freedom, or justice and harmony, is the value of the rule of law.[374]

What is meant by the rule of law in China is thus not a determination that law must be separated from morality or, more broadly, the legal from the extra-legal. The concept of the rule of law in China reflects, instead, an ideal of integration between "governing the nation in accordance with the law (yifa zhiguo)" and "rule by morality (yide zhiguo)".[375] It is thus no surprise that the governance of data and online activities in China is correspondingly enmeshed with moral ideals, even if the difference here to the European approach might be partly in the willingness of China to openly conceptualise its broader evaluative enterprise — although some differences, of course, run deeper.

This can be seen, for instance, by examining goals recently acknowledged by the Cyberspace Administration of China (CAC) and other governmental bodies in their "Guiding Opinions on Strengthening Overall Governance of Internet Information Service algorithms"[376] and put into practice in the "Internet Information Service Algorithmic Recommendation Management Provisions"[377] (which, in turn, is issued on the basis of also relatively new Cyber Security and Data Security Laws, as well as the Personal Information Protection Law, which earlier papers in this project have engaged with). Ideas found in both documents of, for instance, making sure the governance of Internet algorithms promotes "social fairness and justice",[378] may resound in cross-cultural ways. Others are more debatable, such as that algorithms should "vigorously disseminate positive energy",[379] or that their

---

[372] See CCP Central Committee and State Council, **中共中央**办公厅印发《**关于**进一步把**社会主**义核心价值 观融入法治建设的指导意见》[*General Office of the CCP Central Committee and State Council Issuing 'Guiding Opinions on Further Integrating Socialist Core Values into the Construction of Rule of Law'*], GOV.CN (Dec. 25, 2016), http://www.gov.cn/gongbao/content/2017/content_5160214.htm .. These were first made into formal policy by CCP Central Committee in 2013, in their "Opinions on the Cultivation and Practice of Socialist Core Values". See CPC Central Committee, 《**中共中央**办公厅**关于培育和践行社会主**义核心价值观的意见》[*General Office of the CCP Central Committee Issuing 'Opinions on the Cultivation and Practice of Core Socialist Values'*], CCP CENTRAL COMMITTEE (Dec. 23, 2013), http://www.gov.cn/zhengce/2013-12/23/content_5407875.htm

[373] Supreme People's Court, **最高人民法院**印发《**关于深入推**进社会主义核心价值观融入裁判文书释法说理的指导意见》[*Supreme People's Court Issuing a Notice on the 'Guiding Opinions on Deeply Promoting the Integration of Socialist Core Values into the Analysis and Reasoning of Adjudicative Instruments'*], SUPREME PEOPLE'S COURT (Feb. 2, 2021), https://www.court.gov.cn/fabu-xiangqing-287211.html .

[374] These values, which the 2016 Guiding Opinions recognise as "the spirit of socialist construction of the rule of law" are: the national values of 'prosperity', 'democracy', 'civilization', and 'harmony'; the social values of 'freedom', 'equality', 'justice', and the 'rule of law'; and the individual values of 'patriotism', 'dedication', 'integrity', and 'friendship'. As a reflection of the fundamental character of these values, mandates for the state and the Party to uphold them have recently been incorporated into both the PRC Constitution and the Constitution of the Chinese Communist Party (see XIANFA art. 24, § 1 (2018) (China)—establishing that "[t]he state shall champion core socialist values"—and CPC CONSTITUTION, General Program, § 21 (2017) (China)—establishing that the Communist Party of China "shall strengthen the system of core socialist values" and "cultivate and practice core socialist values").

[375] Delia Lin and Susan Trevaskes, *Creating a Virtuous Leviathan: The Party, Law, and Socialist Core Values*, 6 ASIAN JOURNAL OF LAW AND SOCIETY 41, 42 (2019). Or, to put it as recently articulated by the Supreme People's Court, the idea here is one of "being loyal to the constitution and to the law", but also "organically combining legal evaluation with moral evaluation" and "seeing to it that the rule of law and the rule of morality fit with and complement one another".

[376] Cyberspace Administration of China, **关于印**发《**关于加强**互联网信息服务算法综合治理的指导意见》**的通知** [*Notice on the Issuance of the Guiding Opinions on Strengthening the Overal Governance of Internet Information Service Algorithms*], CYBERSPACE ADMINISTRATION OF CHINA (Sep. 28, 2021), http://www.cac.gov.cn/2021-09/29/c_1634507915623047.htm

[377] Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, and State Administration for Market Regulation, *Provisions on the Management of Algorithmic Recommendations in Internet Information Services*, CYBERSPACE ADMINISTRATION OF CHINA (Jan. 4, 2022) http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm

[378] Cyberspace Administration of China, *supra* note 226, preamble.

[379] *See footnote above*, Section I, § 1.

governance should "create a cyberspace of clean and upright winds".[380] The documents also include yet another set of ideas that are very difficult to assimilate within a Western liberal context, such as that the governance of algorithms should "promote ideological security",[381] "establish" / "persevere in the correct orientation",[382] "uphold mainstream value orientations",[383] "uphold the correct political direction" and "public opinion orientation"[384], among others.

What transpires is that the difference between the Chinese and the European approaches does not lie so much in the engagement with comprehensive normative ideals. Both approaches do so — whether this engagement is conceptualised or not — which, in turn, necessarily entails some narrowing of options in accordance with some threshold of social acceptability. The real difference is where such threshold lies, and how more or less conducive to diversity and value pluralism each regulatory culture is. This is thus a central debate to be had in questions concerning data governance. Any effort to find common ground must begin with an earnest acknowledgment of the unavoidable morality of data governance. Similarly, any institutional framework to tackle data governance questions must endeavour to engage with moral differences between distinct cultural traditions, not to evade these differences. Harmonisation needs to begin with the understanding that harmony is itself a goal — and a moral goal at that — to be reflectively pursued between and in the context of each cultural tradition.[385]

Now, whereas the resemblance between the European and the Chinese approaches to data governance might increasingly be more a matter of degree, the contrast with the approach in the United States could not be starker. Apart from a range of data protection acts at the state level, the approach to data governance at the Federal level has historically been marked by a notable lack of initiatives beyond the realm of trade and, within it, of consumer protection — though even here initiatives are not comparably as comprehensive as those of other jurisdictions.

As noted by Arner et al., the "data governance style of the United States" reflects "the prioritisation of a libertarian free market", support for the "full alienability of data", a "dearth of government regulation for data movement", and so far restrictive recourse to antitrust law.[386] All of these have contributed to the growing concentration of power in a handful of technological platforms.[387] Paradoxically, as the authors also note, it is precisely this approach that is at the "genesis of the dominant philosophy underlying transnational governance of the flow of data" — that is, a philosophy that speaks in favour of "uninhibited flow of information across borders, with a general prohibition on data localisation requirements".[388]

---

[380] *See footnote above*.
[381] *See footnote above*, preamble.
[382] See footnote above, Section I, § 1 and Section IV, § 12.
[383] Cyberspace Administration of China, *supra* note 228, art. 6.
[384] Cyberspace Administration of China, *supra* note 227, Section IV, § 12.
[385] See, e.g., Stephen C. Angle, *Human Rights and Harmony*, 30:1 Human Rights Quarterly 76 (2008) (arguing that "a simultaneous commitment to human rights and to harmony is both coherent and desirable").
[386] Arner et al, *supra* note 193 at 16-17.
[387] *See footnote above*, at 18.
[388] *See footnote above.*

4. THE RETURN OF THE LOCAL

The push against data localisation requirements is a particular feature of the United States approach to the regulation of data flows. It has been expressed in trade agreements originally championed by the United States[389] or to which the United States is presently a party[390]. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (the CPTPP), in Chapter 14 – Electronic Commerce, article 14.13, establishes that "No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory". A similar commitment is adopted toward "allow[ing] the cross-border transfer of information by electronic means".[391]

Interestingly, both provisions contemplate exceptions for Parties to adopt or maintain measures to achieve a "legitimate policy objective"[392], conditioned on a two-fold requirement, the second being a *necessity* requirement: namely, that the measure must "not impose restrictions on transfers of information greater than are required to achieve the objective".[393] This raises interesting questions concerning the interplay between international trade agreements and fundamental rights, such as the right to data protection. We turn to these questions in Part 5.

Important here is to note that again in matters concerning restraints in relation to outbound data transfers, there is more convergence than divergence between approaches taken in the EU and in China. Indeed, in both, instead of unfettered freedom of expression ideals, there is a more pronounced recognition that ideals of reciprocity and membership within a political community entail not only rights, but also *responsibilities*. Data, as an extension of the persons they relate to *and* the political communities into which such persons, qua citizens, are bound, are generally subject to restrictions ensuing from these responsibilities. Among such restrictions are those that prevent data from being transferred to places where there is a perception these responsibilities will not be lived up to. Differences in the ways such restrictions will be put into place in both jurisdictions is again a matter of extent.

In the EU, these restrictions lie most substantively in the realm of personal data protection. Here, requirements for the transfer of personal data to third countries are a fixture of EU data protection law since the 1990s and have been solidified under the General Data Protection Regulation. In their current form under the GDPR, data transfers depend on adequacy decisions by the European Commission,[394] on safeguards provided by the data controller,[395] or on conditions for derogation of

[389] The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (the "CPTPP").
[390] For example, the US-Mexico-Canada Agreement (USMCA) and the Trans-Pacific-Partnership in its original form.
[391] CPTPP, art. 14.11.
[392] *See footnote above*, arts. 14.11.3 and 14.13.3.
[393] *See footnote above*, arts. 14.11.3(b) and 14.13.3(b). The other is that the measure must not be applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade. *See footnote above*, arts. 14.11.3(a) and 14.13.3(a).
[394] See GDPR, art. 45(1).
[395] See GDPR, art. 46. These range from the utilisation of standard data protection clauses adopted or approved by the Commission to the adoption of binding corporate rules or codes of conduct approved by the competent supervisory authorities. *See footnote above*, art. 46(2).

transfer restrictions listed on article 49.[396] Internally, in the context of the Digital Single Market, the Regulation on the Free Flow of Non-Personal Data,[397] while prohibiting the adoption of data localisation requirements by a Member State in relation to other EU Member States,[398] nevertheless enables these measures in instances concerning public security —which are understood within the broad meaning of Article 52 of Treaty on the Functioning of the European Union.[399] Most importantly, the FFNPD does not prevent the adoption of data localisation measures in relation to data processing services taking place outside the European Union.[400] Effectively, the FFNPD regulates the free movement of data within the Union. It does not compel such a movement outwards. Measures taken on these grounds have not been more extensive so far. Examples include initiatives at the national level to develop sovereign architectures for governmental data[401] as well as an important regional effort for the establishment of a pan-European federated cloud infrastructure—namely, the GAIA-X project.[402] Broader in scope, the latter is particularly interesting for how it articulates an ideal of data sovereignty based on European values and seeks to address technical challenges traditionally associated with data localisation initiatives,[403] but at the same time without deferring to received wisdom concerning supposedly immutable characteristics of the global Internet.

In China, data localisation measures are notably more comprehensive and developed from a regulatory perspective. They include both trans-border data transfers and local storage requirements. The latter are imposed to special kinds of data controllers, such as Critical Infrastructure Operators

[396] These include explicit and informed consent to the transfer, necessity for the performance of a contract, necessity for reasons of public interest, among others. *See footnote above*, art. 49(1).
[397] Regulation (EU) 2018/1807 of the European Parliament and of the Council 2018 of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union, 2018 O.J. (L 303) 59 (the "FFNPD").
[398] *See footnote above*, art. 4.
[399] As under the WTO system (see GATS, art. XIV(a), Note 5), the FFNPD establishes that measures taken on the grounds of *public security* presuppose "the existence of a genuine and sufficiently serious threat affecting one of the fundamental interests of society" (see FFNPD, recital 19). The understanding of the Court of Justice of the European Union as to what is encompassed by such interests, however, is broad. It covers, for example, threats to essential public services, the functioning of institutions, the survival of the population, as well as the risk of a serious disturbance to foreign relations or the peaceful coexistence of nations. (*id.*). One can appreciate the breadth of such an understanding by considering that, in a Chinese context, a key institution is the Chinese Communist Party itself, whose leadership is enshrined in Article 1 of the Chinese Constitution as "the defining feature of socialism with Chinese characteristics".
[400] See FFNPD, recital 15 (noting that the FFNPD does "not apply to data processing services taking place outside the Union and to data localisation requirements relating to such data").
[401] See *e.g.* Sylvain Rolland, *Cloud Souverain : La Surprenante Volte-Face de l'Etat en Faveur de l'Écosystème Français*, La Tribune (Sep. 12, 2022, 19:06), https://www.latribune.fr/technos-medias/cloud-souverain-la-surprenante-volte-face-de-l-etat-en-faveur-de-l-ecosysteme-francais-932326.html (on the French "Le Cloud Souverain" initiative). See also Informations Technik Zentrum Bund, *Die Bundescloud – Eine Exklusive, Private Cloud für die Bundesverwaltung*, https://www.itzbund.de/DE/itloesungen/egovernment/bundescloud/bundescloud.html (last visited Sep. 29, 2022) (on the German "Bundescloud" initiative).
[402] Gaia-X *Essentials*, Gaia-X: A Federated Secure Data Infrastructure, https://gaia-x.eu/faq/essentials (last visited Sep. 29, 2022).
[403] See e.g. Peter Swire and DeBrae Kennedy-Mayo, *Hard Data Localization May be Coming to the EU — Here are 5 Concerns*, IAPP (Jan. 26, 2021), https://iapp.org/news/a/hard-data-localization-may-be-coming-to-the-eu-here-are-five-concerns.

(CIIOs),[404-405] who, under Article 37 of China's Cybersecurity Law (CSL), must store within the Mainland any *personal information* or *important data*[406] that they gather or produce during operations within the Mainland territory. If CIIOs are to provide such data abroad — in circumstances where there is a genuine business need — they must follow requirements concerning cross-border data transfers found in Article 37 of the CSL. Namely, they must conduct a security assessment in accordance with measures formulated by the State cybersecurity and information department (that is, the CAC)[407] and the relevant departments of the State Council, unless specific laws and regulations provide otherwise.[408]

When it comes to personal information, Article 40 of the PIPL mirrors requirements of Article 37 of the CSL, but here applying these to CIIOs and to other controllers handling personal information in quantities defined in article 4 of the Outbound Measures. These are, namely: i) controllers handling

[404] Data governance frameworks in China do not employ the terminology 'data controller', or 'control' of personal data. The Cybersecurity Law, for instance, speaks of 'CIIOs' that 'gather', 'produce', or 'provide' information. (See Zhonghua Renmin Gongheguo Wangluo Anquan Fa [Cybersecurity Law] (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 6, 2017), art. 37, 2016 Standing Comm. Nat'l People's Cong. Gaz. 324 (China) [hereinafter ['CSL']. The Data Security Law and the Personal Information Protection Law employ the terminology *data handler* and *personal information handler*. (See Zhonghua Renmin Gongheguo Shuju Anquan Fa [Data Security Law] (promulgated by the Standing Comm. Nat'l People's Cong. Gaz., June 10, 2021, effective Sept. 1, 2021) 2021 Standing Comm. Nat'l People's Cong. Gaz. 951 (China); Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) 2021 Standing Comm. Nat'l People's Cong. Gaz. 1117 (China) [hereinafter 'PIPL']. *Data controller* or *controller* is used here for the sake of consistency.

[405] Critical infrastructure is network infrastructure reputed as "important" in the context of (themselves important) industries and sectors listed in the regulation (e.g. Telecommunications, information services, energy, finance, public service, national defence, and science and technology) or network infrastructure whose "destruction, loss of functionality, or data leakage may gravely harm national security, the national economy and people's livelihood, or the public interest". (Guanjian Xinxi Jichu Sheshi Anquan Baohu Tiaoli [Critical Information Infrastructure Security Protection Regulations] (promulgated by the St. Council, July 30, 2021, effective Sept. 1, 2021), art. 2, CLI.2.5055187 (China) (PKULAW.COM). Under Article 9 of the Regulations, the identification of what *network infrastructure* is reputed as important rests with competent departments and supervision and management departments of the important industries and sectors mentioned in Article 2, which shall formulate critical information infrastructure identification rules and report them to the State Council public security department for filing. Article 9 paragraph 2 lays out 3 sets of factors to be mainly considered in identifying important network infrastructures, namely: i) their degree of importance for the critical and core activities within the industry or sector; ii) the degree of harm that may result from their destruction, loss of functionality, of data leakage; and iii) the associated influence on other industries and sectors".

[406] The identification of what *data* counts as *important*—or, in more recent official translation, *critical*—is an even more complex affair. The "Online Data Security Management Regulations", albeit still in draft form, contains, in its article 73, the most authoritative definition of important data as "data that can endanger national security or the public interest once tampered with, destroyed, leaked, or illegally obtained or used" (See Cyberspace Administration of China) [Notice of the Cyberspace Administration of China Seeking Public Comments on the Online Data Security Management Regulations (Draft for Comment)], Cyberspace Administration of China (Nov. 14, 2021), http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm . The provision includes a non-exhaustive list of seven kinds of data defined as important. A recent Guideline issued by China's National Information Security Standardisation Technical Committee (TC260 (National Information Security Standardisation Technical Committee (TC260) [Notice Seeking Public Comments on the Draft of the National Standard 'Information Security Technology-Guideline for Identification of Critical Data'], TC260 (Jan. 13, 2022), https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20220113195354&norm_id=20201104200036&recode_id=45625—provides further clarification as to what data should count as *critical data* (a terminology it employs in English for the same characters other instruments translate as *important data*).

[407] These measures—the "Outbound Data Transfer Security Assessment Measures" (Outbound Measures)—were issued by the CAC in draft form in October 2021, and have been recently adopted in final form, on 7 July 2022 (Cyberspace Administration of China, 数据出境安全评估办法 [Outbound Data Transfer Security Assessment Measures], CYBERSPACE ADMINISTRATION OF CHINA (July 7, 2022) http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm) [hereinafter 'Outbound Measures'] . They provide an authoritative source of interpretation of the obligations in relation to outbound data transfers by the CSL's main enforcer (namely, the CAC) and apply horizontally as well to outbound transfers in the context of the "Data Security Law" and the "Personal Information Protection Law" (*id.*, art. 1).

[408] Applications for a security assessment must be preceded by an outbound data transfer risk self-assessment report (*id.*, art. 6) and shall be submitted to the local provincial-level cybersecurity and informatisation department (*id.*, art. 4), which will deliberate within 7 days on the acceptance or not of the self-assessment report (*id*., art. 7). Criteria under which the security assessment will be conducted are defined in article 8 of the Outbound Measures.

more than 1 million people overall (regardless of how many of these individuals a personal information handler intends to provide personal information of abroad); or ii) controllers who cumulatively provide personal information of more than 100,000 people abroad or sensitive personal information of more than 10,000 people.[409] Controllers who do not need to undergo security assessments will follow the general requirements for outbound transfers listed in Article 38 of the PIPL, which include, either obtaining a third-party certification through a competent authority according to CAC guidelines,[410] or adopting a standard contractual clause developed by the CAC.[411] In all cases, separate consent must be sought from data subjects (Article 39) and data controllers must make sure recipients abide by requirements under the PIPL (Article 38).

Importantly, Article 38(2) of the PIPL contains an opening for the adoption of commitments relating to outbound transfers in international treaties or agreements. As seen above, circumstances involving CIIOs or critical data are surely to constitute exceptions to such treaties — and exceptions, at that, which the language of international trade agreements, from the GATS to the CPTPP, seems able to accommodate. Indeed, one can hardly think of the measures discussed in this part being struck down on the grounds that they are not necessary to achieve their objectives, in particular, if one takes into account the value systems of the societies such measures are embedded in. Yet, pushes for the liberalisation of international data flows are often represented as a desirable reaction to data localisation restrictions put in place by jurisdictions such as China. They are represented as a reaction to the subjection of data to political systems portrayed as *autarkic*, systems which, in restricting data flow, seek to further the authoritarian interests *of the state itself*, as divorced from the interests *of society*—an interest, presumably, in *unfettered* forms of information flows. Such a representation, however, can only be sustained as an instantiation of ideals of liberal neutrality explored in the preceding section, since what often motivates restrictions on international data flows, are evaluative choices in rights-based realms and beyond — choices that ideals of liberal neutrality assume should not be made by the state. As Cristopher Kuner aptly observes, scholarly debates at times tend to "attribute[...] protectionist motives to some measures seeking to protect constitutional and human rights on the Internet".[412] Some of these measures are put in place in response to "phenomena such as intelligence surveillance, the globalisation of the information economy, and privacy violations by Internet companies".[413] As Kuner also notes, it is important to distinguish these measures from industrial policy disguised as broader public interest. Yet, it *is* the case that many such measures do reflect legitimate public interests.

---

[409] The provision also reiterates the requirement for security assessments for transfers in circumstances under article 37 of the CSL as well as under other circumstances the State cybersecurity and informatisation department may determine data export security assessments must be applied for.

[410] Standards for so were issued by TC260 in June 2022. See National Information Security Standardisation Technical Committee (TC260) [Notice on the Issuance of Practical Guidance on Cybersecurity Standards - Technical Specifications for Certification of Cross-Border Processing of Personal Information'], TC260 (June 24, 2022), https://www.tc260.org.cn/front/postDetail.html?id=20220624175016

[411] Draft Standard Contractual Clauses have been introduced by CAC, in the context of consultations concerning draft provisions on Standard Contracts for the Export of Personal Information, which ended on July 29, 2022. See Cyberspace Administration of China, [Notice by the Cyberspace Administration of China Soliciting Comments on the "Provisions on Standard Contracts for the Export of Personal Information" (Draft for Comments)], Cyberspace Administration of China (June 30, 2022), http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm

[412] Christopher Kuner, *Data Nationalism and its Discontents*, 64 Emory L. J. Online 2089, 2090 (2015).

[413] *See footnote above*, at 2092.

5. BETWEEN TRADE AND HUMAN RIGHTS

A fundamental challenge in questions concerning data governance is thus the co-existence between the international trade system and the international human rights system. More precisely, the challenge is that necessity tests in trade agreements such as the GATT or the GATS transform rights such as the right to data protection, if not fully into externalities, at least into exceptions to be thoroughly justified.[414] Yet the international human rights system, in turn, does the same, since it contains its own necessity tests for restrictions to the rights it recognises — and it does so with much more credibility given the fundamental character of such rights and the system's role in guarding their intra-systemic coherence. This clash between necessities — the utilitarian necessity of unfettered trade and the deontological necessity of human rights — will only get accentuated as data governance questions unfold. There is just no way around it that does not involve urgent and cross-cultural dialogue around the boundaries of human rights commitments concerning international data flows.

Trade agreements have, nevertheless, difficulty in dealing with such questions. The WTO dispute settlement bodies are just not the ideal fora to decide on matters that overlap so intensely with the value systems of different global communities. In a way, the international trade system is a response precisely to the indeterminacy of questions concerning such value systems, but a response that operates by, to a large extent, bracketing off the substance of such questions. Thus, the question of whether censorship measures put in place by China in relation to audiovisual content were necessary (under the public morals exception in Art XX(a) of the GATT) given the policy objectives they sought to achieve remained in substance unaddressed by WTO dispute settlement bodies, which instead engaged with a more circumscribed institutional aspect — namely, whether it was necessary that only certain state-owned enterprises had the rights to import cultural goods into the country.[415]

As much as it is hard to imagine the WTO engaging in substance with the intricate details of China's content regulation regime to make a determination, for example, as to whether a "reasonably available" and "less trade-restrictive" alternative exists that achieves the same policy objectives,[416] it is likewise immensely difficult to imagine the WTO making a similar determination in relation to the substance of different data governance regimes in the context of Art XIV(c)(ii) of the GATS. If one considers data privacy regimes compared in other papers of this workstream — namely, those of the State of California, the EU, and the People's Republic of China — it does not appear likely that dispute settlement bodies would penalise any of the three jurisdictions on the grounds that data privacy regimes embraced by the others are less restrictive. These different regimes set up complex

[414] See, e.g., Svetlana Yakovleva, *Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy*, 74 Univ. of Miami L. Rev. 416, 461 (2020). See, also, Svetlana Yakovleva and Kristina Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection*, 2(2) European Data Protection Law Review 191 (2016).
[415] See, e.g., Joost Pauwelyn, *Squaring Free Trade in Culture with Chinese Censorship: The WTO Appellate Body Report on China – Audiovisuals*, 11(1) Melb. J. Int. Law 5 (2010) (noting how, in *China—Audiovisuals*, both the Panel and the Appellate Body evaded the substance of the necessity test).
[416] Such a task is particularly complicated given the lack of clarity that, as Tania Voon observes, affects the idea of "trade-restrictiveness" as it underpins the necessity test in WTO case law. See e.g. Tania Voon, *Exploring the Meaning of Trade-Restriveness in the WTO*, 14:3 WORLD TRADE REVIEW 451, 476 (2015).

architectures entailing a "multiplicity of interacting measures".[417] The extent to which one or the other is less restrictive is largely a subjective affair, which can only be evaluated with the benefit of time.[418] Even if all these regimes are frameworks for the protection of individual rights, they are also environmental responses to power asymmetries resulting from the instrumentarian forces of surveillance capitalism.[419] In these responses, questions of data privacy cannot be dissociated from broader debates concerning data governance. At stake here is as much an individual right to informational self-determination, which the idea of data privacy can be seen as synonymous with, as more broadly the right to self-determination *tout court*, which one finds recognised in Article 1 itself of both the International Covenant on Civil and Political Rights, and the International Covenant on Economic Social and Cultural Rights.

As a collective right, a right belonging to all peoples, the right to self-determination interfaces with general exceptions in trade agreements, such as the public order and public morals exceptions, and is deeply intertwined with debates concerning data sovereignty discussed in this paper. In sum, questions concerning data sovereignty must be approached from a multifaceted perspective — as questions, that is, which involve the individual, the social, and the political — and comprehensively made sense of within the framework of international human rights law.

This is by no means to deny the outstanding importance of trade-related aspects as well, and the goals the international trade system endeavours to fulfil. As Chander and Schwartz most aptly observe, as remarked at the beginning of the paper, trade must not be seen as purely a neoliberal enterprise. Rather, they note:

> *"[T]rade rules can support the development of human capital across the world. Cross-border trade in services means a democratization of opportunity throughout the world. … [O]n a global scale, the issue of trade implicates distributive justice. This point is especially urgent today as the developing world seeks to enter into valuable markets for digital services".*[420]

For that to be true, however, distributive aspects cannot be purely a matter of unfettered trade regimes either. Rather, trade regimes must be embedded in a broader framework that is mindful of distributive and more broadly normative justice considerations — considerations concerning the justice or propriety of how different reasons or norms get articulated in the information environment, and of the sorts of architectural and substantive constraints their articulation establishes for online

[417] Appellate Body Report, *Brazil — Measures Affecting the Cross-Border Supply of Retreated Tyres*, 151, WTO Doc. WT/DS332/R (adopted Dec. 17, 2007), https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/WT/DS/332ABR.pdf&Open=True (last visited: Sep. 6, 2022).
[418] *See footnote above*.
[419] See Soshana Zuboff, Surveillance Capitalism: The fight for a Human Future at the New Frontier of Power 2 (2019) (presenting surveillance capitalism as "the origin of a new instrumentarian power that asserts dominance over society and presents startling challenges to market democracy).
[420] Chander and Schwartz, *supre* note 192, at 39.

data flows, for instance.[421] There is simply no justice, distributive or otherwise, where such reasons merely allow dominant informational practices to flow unimpeded.

In a privacy context, Helen Nissenbaum has conveyed similar ideas in speaking of a framework for contextual integrity, which on one hand "requires that practices [regarding information flows] be evaluated in relation to entrenched context-relative informational norms" and, on the other hand, enables such norms to be overridden "if new practices are demonstrably more effective at achieving contextual values, ends, and purposes or the equivalent".[422] The normative ends Nissenbaum speaks about spring from different social spheres and, since such spheres must hang together — given that a view of integrity must be pursued between them — privacy considerations are never purely privacy considerations. They must naturally be considered from the perspective of broader data governance debates; and, insofar as such debates find themselves, in turn, embedded in the discipline of international trade, also here they point to questions concerning a broader evaluative universe with which this discipline interacts.

Indeed, as this paper has extensively sought to demonstrate, questions concerning the governance of online data flows, including in a trade-related context, are enmeshed in a universe of indeterminate normative standards that, it might be said, constitute the central cases of data sovereignty debates. This is so since it is here that one can see at its strongest the endeavour of different global communities to identify and affirm the values upon which the authority of their political systems is founded. Whereas the adoption of a global agreement on minimum privacy standards, as advocated in other parts of this project, would be a most important institutional development, an alternative must be found for enduring questions as to how such minimum standards, as well as more ambitious ones, find themselves re-embedded in the domains of locality — in the earthly, contextual realities of digital sovereignty.

As noted at the outset, this alternative could be found in the establishment of a platform for cross-cultural dialogues in relation to such questions, put into place by a two-phased international agreement in the human rights realm, ideally within the United Nations System. The first phase, to be established in the short to medium term, would be procedural in scope. It would come in the shape of a multilateral body that could act independently or be provoked by other multilateral organisations — by dispute settlement bodies within the WTO for instance — to deliberate on the boundaries of indeterminate standards in global data governance questions. Such a body, while not immediately responsible for adopting substantive normative instruments, would enable earnest and open-minded engagement between different countries in seeking to ascertain the reasonable boundaries of their differences. In a case concerning the application of a general exception to the GATT or the GATS, for instance, this multilateral body would provide a more appropriate forum for agreement on the reasonable boundaries of differences between Member States — the boundaries, that is, of what,

[421] See Marcelo Thompson, *Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries*, 18:4 Vand. J. Ent.& Tech. L. 783 (2016) (putting forward a justification for the responsibility of technological platforms grounded on ideals of normative justice).
[422] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 159 (2010).

while being socially acceptable within the value system of one Member State, cannot reasonably be accepted as a restrictive measure in an international context.[423]

While procedural, however, it would be important that this body does not have its policy-setting relevance dissolved as happened to another famous attempt to establish an Internet-related forum under the United Nations — namely, the Internet Governance Forum.[424] This workstream would like to think that, with the benefit of hindsight and having witnessed the cosmopolitan influences that have led, for example, to the transition of a body such as ICANN-The Internet Corporation for Assigned Names and Numbers to the international community, an initiative to establish a multilateral forum would find less resistance this time around.[425] Unlike ICANN, however, it would be important that multilateralism — rather than "multi-stakeholderism" — be the operative word here. Discussions on human rights aspects concerning data governance are, ultimately, discussions involving sovereignty. It is hard to imagine that, in questions of such tremendous importance, which involve the fundamental commitments of different political communities, States would defer to the more loosely institutionalised forms of multistakeholder bodies[426] — indeed, to the challenges of representativeness that typically affect such bodies and the anti-State ethos they epitomise.

In a second phase, in the medium to long term, with the formation of critical mass and a reservoir of reciprocal understanding concerning the boundaries of indeterminate standards in the realm of data governance, this procedural agreement could evolve into a substantive one — that is, into a substantive international agreement on human rights aspects concerning data governance. While complete solutions to problems of indeterminacy in data governance standards will not be found in any single field, there is perhaps not a better — or more urgent — candidate for the pursuit of agreement in relation to such standards than the field of human rights. First, and obviously, due to

[423] Ongoing discussions on a multi-lateral agreement within the WTOs Joint Statement Initiative on E-Commerce (See WTO, https://www.wto.org/english/tratop_e/ecom_e/joint_statement_e.htm (last visited: Sep. 6, 2022)), while surely most important, do not solve the problems of indeterminacy the initiative contemplated here would set out to address. In fact, in its version presently available (https://www.bilaterals.org/?wto-plurilateralecommerce-draft (last visited: Sep. 6, 2022), the draft agreement contains an exception for matters concerning privacy and other legitimate public policy objectives that is very much in line with exceptions we find in the GATS itself (see, e.g., Chander and Schwartz, *supra* note 1 at 49, noting that, in its latest, leaked version, the Agreement also incorporates what they call the "privacy bracket"). The big question that solutions proposed in this paper seek to address is precisely how to solve problems of indeterminacy are found in exceptions such as these and in the data governance realm more broadly. This a question, in this sense, that much transcends the realm of trade alone.

[424] With its mandate defined in the Tunis Agenda of the United Nations-convened World Summit of the Information Society [WSIS], the IGF is a body for multi-stakeholder policy dialogue, devoid of actual decision-making power. It concentrates a range of practical competences (such as to "[d]iscuss public policy issues", "[f]acilitate discourse" between policy bodies, "[i]nterface with appropriate intergovernmental organizations") but has no oversight function in relation to other bodies and its deliberations are explicitly recognised as not binding. See Tunis Agenda, WSIS, Tunis Agenda for the Information Society, Doc. WSIS-05/TUNIS/DOC/6(Rev.1)-E (Nov. 18, 2005).

[425] See Viktor Mayer-Schonberger and Malte Ziewitz, *Jefferson Rebuffed: The United States and the Future of Internet Governance*, 8 COLUM. SCI. & TECH. L. REV. 188 (2006) (describing a proposal put forward by the European Commission, during the run-ups to WSIS, to transition ICANN to the international community—and the resistance that ensued).

[426] It is important to observe the natural difficulties in ensuring that such bodies will recognise and live up to their human rights' responsibilities—including in relation to identifying and making sense of such responsibilities. See, in this sense, Monika Zalnieriute, *From Human Rights Aspirations to Enforceable Obligations by Non-State Actors in the Digital Age: The Case of Internet Governance and ICANN*, 21 YALE J.L. & TECH. 278 (2019) (noting the complicated relationship between ICANN and the international human rights system – for instance owing to the fact that a so-called 'Framework for Interpretation of Human Rights' ('FOI-HR') first proposed by ICANNs accountability working group in 2017 and which, according to ICANNs own Bylaws, is a formal condition for a 'human rights Core Value' recognised by the Bylaws to acquire "force or effect", is yet to be adopted by the Board of Directors of the organisation). Note also that only in October 2016 was such a "Core Value" recognised at last in ICANNs Bylaws, as a result of the more comprehensive internationalisation of ICANN, with the transition of its IANA functions to the international community.

the fundamental character of such rights, but also because this field is pervaded like no other by judgements of moral and political quality. Even prioritisation between such rights — and their separation in two International Covenants within the UN System — reflects a difference between jurisdictions in the making of judgements about their character and contours, with Europe and China favouring the adoption of a Covenant on Economic, Social, and Cultural Rights that the United States, to this date, is yet to ratify, and thus reflecting a more collective-oriented approach that stands in contrast with the more individualistic path taken by the United States, including in relation to its interpretation of the right to freedom of expression.

For countries around the world, freedom of expression indeed is not and cannot be a conversation stopper. Global data governance debates will not be settled or advanced under vague and abstract accusations of 'censorship' and calls for an 'open Internet'. No jurisdiction discussed in this paper would like to see a closed Internet. Global data governance debates will only move forward in the concrete understanding of what forms of practice, discourse, and indeed of restriction are not acceptable by the international community.

In facing the indeterminacy of data governance standards, the urgent task ahead is, instead of pretending evaluative pursuits do not take place, one of establishing procedures to find common ground, if not as to what all countries should pursue at least as to what none of them should. The rest is the domain of sovereignty, of the foundational values that each political community should be left free to reaffirm and pursue on its own. And this is as much a matter of policy as it is one of design.

6. CONCLUSION

The two recommendations put forward in this paper are one of a more concrete substance and the other of a more abstract character. The concrete recommendation is the establishment of a two-phased international agreement on human rights aspects concerning data governance. The more abstract one is the recognition of the inevitability, in fact, the desirability that the design of technological processes —including Internet-based ones — be informed by the affirmation of sovereign values.

This sovereignty of design is not something to be lamented, decried under calls for ideals of neutrality. Rather, it is something to be cherished as an enjoinment for different political communities to, from the perspective of their different value systems, affirm their possibilities of jointly endeavouring in a common interpretive enterprise. Data governance challenges are calls for a pursuit of the integrity of and between the values of these different political communities.

This paper has pointed to the European Gaia-X and International Data Spaces projects as positive examples of how a sovereign infrastructure can be established around common principles, here for the sharing of data within different data spaces in the European Digital Single Market. These are examples of technological determinism being replaced with institutional imagination in thinking about how human values can be best promoted in the context of harmonisation processes. It is hoped that institutional solutions being proposed in this project may work as a springboard for similar initiatives in a global context.

cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS

ADDRESSING THREATS TO DIGITAL INFRASTRUCTURE

MARC BOURREAU
RICHARD FEASEY

TABLE OF CONTENTS

1. AIM AND APPROACH

This paper discusses issues arising from threats to the functioning of digital infrastructure. Policymakers generally consider digital infrastructure to be critical to the effective functioning of modern-day economies and societies. Despite this, we find that they have paid insufficient attention to ensuring that digital infrastructure is adequately protected and sufficiently resilient. This is for several reasons. First, the digital landscape and the threats facing it are complex and constantly changing, and there is often a large information asymmetry between policymakers and the owners of digital infrastructure. This means there is a need for policymakers to take a strategic view of risks to the system as a whole, rather than reacting to ad hoc events or working in silos. Second, broader political objectives or considerations may distort how questions about threats to infrastructure are approached and which issues are given the most attention, as we illustrate in the discussion of foreign ownership and control restrictions. Third, policymakers and States have ambiguous or conflicting motives when it comes to managing threats to digital infrastructure, or in pursuing resilience objectives alongside other objectives. Finally, much of the world's digital infrastructure is owned and operated by private sector actors, who may have motives or interests which may not promote resilience or which conflict with the objectives of policymakers or States.

A wider recognition and appreciation of these factors would allow both policy makers and private owners to better focus on those issues which affect the reliable functioning of digital infrastructure and to take tangible actions to improve things. However, understanding these factors involves recognising the limits of what might be achieved under existing institutional arrangements and geo-political circumstances.

The paper is organised as follows:

- First, we explain what we mean by 'digital infrastructure', 'threats' and 'resilience';
- Next, we provide an overview of events or actions which commonly threaten to disrupt the operation of digital infrastructure;
- We provide an overview of the efforts of owners and policy makers to reduce threats and ensure that digital infrastructure is resilient;
- We critically assess actions taken to date by policymakers in light of the threats that we have previously identified; and
- Finally, we make a number of recommendations on how threats may be reduced and the resilience of digital infrastructure may be improved.

2. DIGITAL INFRASTRUCTURE AND RESILIENCE

'Digital infrastructure' refers to the networks which convey digital information around the world. These networks comprise physical assets, such as buildings, towers, cabinets or ducts in which electronic equipment, racks or cables are installed, as well as the software code which enables individual components of the network to perform their functions and to interwork with each other. Networks that provide digital connections to individual users or premises are often referred to (and will be referred to here) as 'local access' networks. These can employ either fixed or wireline technologies that use fibre or copper cables to convey information, or mobile or wireless technologies which use radio spectrum and radio systems to convey data. In the past, the local access network was generally a private or State-owned monopolist. In recent decades the owners of these networks have been privatised and State influence is now exercised through regulation (and foreign ownership restrictions). Local access networks are increasingly subject to duplication and competition from rival networks which compete with them to provide connections to the same premises.

'Local access' networks will be connected to 'core' or 'national' networks which convey information from one location to another throughout a country. The distinction is relevant for our purposes because a core network can be designed to re-direct traffic over another physical route if the functioning of one part of the network is disrupted. Thus, core networks will have a degree of physical redundancy designed and built into them in order to reduce the risk of service disruption in the event that some part of the core network fails or is otherwise degraded. Such a failure is likely to affect a significant number of customers. In contrast, customers of fixed local access networks will generally rely upon a single physical connection which, if it fails, will result in a total loss of service. But this loss will be confined to the premises which rely on that particular connection. The position of customers of wireless local access networks, which are shared amongst multiple users, is more complex and discussed later in this paper. The owners of local access networks may own and operate their own national networks or may rely upon connections with national networks operated by others. As with local access networks, core networks are privately owned and subject to regulation. Markets for core network infrastructure are competitive and there is significant duplication in most countries today.

National networks are connected to each other by means of submarine cables or overland connections between core networks at a national border[427]. For obvious reasons, submarine cables are much more difficult to deploy than overland cables and may be hundreds or thousands of kilometres in length. Historically, these cable systems were built and operated by consortia of national network operators (who may be competitors within the national market and who may operate in either or both of the States or regions that are connected by the cable). When those operators were privatised, so too was their ownership interest in cable systems. More recently, some submarine cables have been commissioned by individual firms, such as Google and Facebook, rather than by consortia of telecom operators (or consortia of tech firms). Like national networks, submarine cable systems are designed

[427] Only a small fraction of digital communications is undertaken or capable of being undertaken via satellite systems although they may play an important role in emergency situations. For example, the Ukrainian Government has received Starlink LEO satellite terminals from Space X in March 2022, although information as to their use and effectiveness is not yet available.

with physical redundancy in mind, such that national operators will generally connect to several different cables in order to route traffic between particular destinations. The global nature of digital infrastructure (and the relatively low level of utilisation on the individual cables)[428] means that traffic can often be re-routed via other cables in the event of a disruption, although submarine cables may also exhibit bottlenecks. Some developing countries may still rely on one or a small number of cables, to connect with the rest of the world. More developed countries may have multiple cable routes, but there may still be choke points as multiple cables converge at a small number of landing stations (being the location at which the submarine cable connects to the national networks) or must pass through a narrow stretch of water (such as the Suez Canal, through which most cables connecting Europe to Asia run).[429] The extent of competition between submarine cable system providers will depend upon the route in question.

In the past, telecommunications operators owned and operated both the physical infrastructure and the software which together comprise the network. Specialist electronic equipment which used proprietary software was distributed in cabinets, buildings, or on towers across the country. Today, however, the telecommunications industry is in the midst of fundamental changes as networks become increasingly 'virtualised', with functions increasingly being centralised and controlled by open source software that is hosted on standard IT physical infrastructure (although, as we note later, developments in edge computing also mean that some functions and capabilities may also become more distributed as they are located at the edge of the network in order to be closer to the customer). The technical architectures of networks are therefore undergoing significant and fundamental transitions, with long-term implications which remain uncertain today. Ownership models are also changing, with some operators outsourcing physical assets, such as portfolios of towers, to specialist 'TowerCos', or the centralised hosting of data and software applications in data centres and other infrastructure that are operated by third-party cloud service providers such as AWS, Microsoft or Google. These cloud service providers may, in addition to hosting software applications for telecommunications operators, host 'critical' applications for many other businesses and organisations. Unlike the local network, the physical location of a data centre will not generally be determined by the location of its customers, but by other factors such as the availability of cheap and reliable power and good digital connections (and the need for geographic diversity to improve resilience). This means that, in the future, it will be technically feasible for a physical network that is owned by one entity and located in one State to be controlled and operated by a different entity using software applications that are hosted in data centres located in another State.[430] Encryption technologies may also mean that neither entity has full control over certain aspects of the infrastructure or the services which are provided over them. Cloudification may also mean that system

[428] Average utilisation is 15-30%, see: https://www.mdpi.com/1424-8220/20/3/737 p.2. One obvious reason for this is that retrofitting additional capacity to submarine cable systems is difficult and expensive, so very large fibre bundles or amounts of capacity are laid when the cable is installed on the seabed. Fibres are then activated or 'lit' at either end of the cable when additional capacity is required.
[429] Other notable bottlenecks include the landing site in Brazilian Fortaleza for traffic between North and South America, the Strait of Malacca, the Luzon Strait, the Red Sea, and the Gulf of Aden.
[430] This is something which already occurs to some extent with existing telecommunications networks in Europe, see: https://www.telekom.com/en/media/details/the-pan-european-network-pan-net--442220 We discuss concerns that suppliers of network equipment like Huawei may also be able to 'control' networks in the US and Europe (or extract communications from them) at the request of the Chinese Government later in this paper.

risks are pooled if several operators who would each have previously operated independent networks come to share the same cloud service provider.

Digital infrastructure therefore comprises local access networks, core or national networks, submarine cables that connect national or regional networks internationally and data centres that host software and applications to run the networks.[431] Most of the assets required to operate these networks are owned and operated by privately owned and controlled telecommunications operators. In recent years digital service providers like Google and Facebook have made investments in submarine cable infrastructure and, to a lesser degree, local access networks. In addition, industry trends such as network virtualisation and cloudification are likely to mean, amongst other things, that a greater proportion of the assets that comprise the networks of the future will be owned and operated by parties other than the traditional telecommunications operators. These include cloud service and data centre providers, and, for physical assets such as towers, other specialist asset providers. Many of these companies will operate on an international basis, meaning that infrastructure in one State may be controlled by an entity that resides or is controlled in another State, or that the functions controlling the physical assets will themselves be located outside of the State. These developments (as well as others) are likely to have significant implications for the future resilience of digital infrastructure and the issues which arise in relation to it.

A 'threat' to digital infrastructure for the purposes of this paper is anything that has the potential to disrupt its effective functioning. We discuss the many types of threats that might arise later. Some threats may be avoided, or at least the probability of their arising reduced, either by taking steps to prevent them from having any impact on the functioning of the infrastructure or by taking actions that deter particular actors from engaging in the threatening activity. Other threats, including unintended errors when writing computer code or operating or making changes to complex systems, are better viewed as being impossible to avoid. Threats from unpredictable or black swan events, including those arising from climate change, solar storms[432], or terrorist acts may also fall into this category. Recognising this, operators of critical infrastructures have increasingly focussed on ensuring the resilience of the infrastructure in the face of disruptive events that cannot be avoided. The resilience of digital infrastructure refers, for the purposes of this paper, to its capacity to continue to perform functions when it has been degraded or is operating under adverse conditions, and to the time that is required to restore it to full working order.[433]

As we noted earlier, one way in which the resilience of a system may be improved is to introduce a degree of redundancy for individual components or even networks. Redundancy in this context refers to the availability of alternative assets which perform the same or similar function if one set of assets

[431] This would include facilities hosting a wide range of applications, including for example DNS servers and IPX and roaming hub providers.
[432] See: https://www.ics.uci.edu/~sabdujyo/papers/sigcomm21-cme.pdf -This is one of the few studies we have seen to model the impact of a high risk event (a solar superstorm) on digital infrastructure performance on a global level.
[433] See: https://www.oecd-ilibrary.org/sites/02f0e5a0-en/1/2/2/index.html?itemId=/content/publication/02f0e5a0-en&_csp_=eb11192b2c569d5c3d1424677826106a&itemIGO=oecd&itemContentType=book The NIST defines cyber resiliency as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources," at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

were to fail or be degraded. In relation to digital infrastructure, this normally refers to the availability of alternative physical routes or connections through which to send digital information but, in relation to software, it may refer to the duplication or 'mirroring' of databases and software applications at different physical facilities with the ability to switch seamlessly between them. An individual firm may ensure a degree of redundancy within its own operations ('firm specific resilience'), but it may also be possible for policymakers to require that firms co-operate amongst themselves so that traffic is re-routed from one firm's network to another if the first network is subject to disruption, contributing to 'system-wide resilience'. This may be feasible when there is a number of duplicate or competing networks, as in the case of enabling users to switch or roam between competing wireless networks which we discuss later in this paper. However, the ability of a network to absorb the demand of users from a competitor will depend upon the amount of spare capacity it has available or the speed at which additional capacity can be added to the system.

It should be noted that complex systems may still exhibit bottlenecks or have single points of failure which, if they fail, cannot be bypassed and which will compromise the performance of the entire system. This can be the case in networks operated by a single entity or within a single State, but it can also apply between entities or States when networks are interdependent upon each other. Resilience in one part of the system may be of little benefit if other parts of the system remain susceptible to failure.

Another aspect of resilience in relation to digital infrastructure relates to the diversity of suppliers of equipment and the way in which that equipment is deployed in networks. We later discuss concerns that have arisen about the lack of diversity of supply of local access infrastructure, where all operators of infrastructure within a country may rely on the same supplier or a small number of suppliers. This means that if errors or vulnerabilities arise in the software or hardware of a particular supplier, this is likely to adversely affect the functioning of all networks in that country. Again, individual firms will generally make unilateral decisions about who supplies their network equipment and how that equipment is deployed in the network, and they are likely to do this without regard to decisions being taken by other firms.

Redundancy is not, however, the only means by which resilience can be improved. Reducing the time between the detection of a failure or error in a network, diagnosis of that failure or error, and the taking of steps to remedy it, may also be important. This is important with respect to submarine cables, where locating a break in the cable in the middle of the ocean and then repairing it can be a formidable engineering and logistical challenge taking many weeks. Getting physical access to local network assets for engineers to restore them may also be challenging if the roads surrounding the site at which the equipment is located remain impassable due to flooding or fallen trees. This highlights the dependency that those operating digital infrastructures have on the providers of other forms of infrastructure, especially electricity to power the network. Operators of digital infrastructure, including those running data centres, will generally have batteries, generators or other power sources which can be used in the event of a failure of the power grid supply. However, the extent to which these prove sufficient will depend upon how long it takes to restore the grid, something over which the digital infrastructure owners may have no influence.

3. THREATS TO DIGITAL INFRASTRUCTURE

Those operating digital infrastructure, which today generally means regulated businesses in the private sector, have long been concerned about threats to their physical network assets. These are relatively easy to visualise although they may still be difficult to detect or prevent. It is worth recalling that the foundational architecture of what we refer to as 'the internet' reflects the intention of the creators of its predecessor, the ARPANET, to design a system that could dynamically route traffic to sustain communications in the event of an attack by a hostile State. Local access and core networks are frequently disrupted by fires, whether accidental or deliberate, other (often isolated) acts of vandalism, theft or terrorism, climate-related incidents such as flooding or hurricane damage, damage to street furniture when motor vehicles collide with them and many other more esoteric activities. Jamming and GPS spoofing devices may also be used to disrupt wireless networks at particular locations for a variety of motives.[434] Official data about the frequency or sources of disruption of local and core networks is not generally available and so is difficult to quantify.

Data centres are subject to similar types of threats to their physical facilities as local access and core networks, although the consolidation of the assets at a single location means that it is easier to ensure appropriate security and access measures are in place and easier to determine where damage has occurred.

Submarine cables are vulnerable to similar types of threats as overland networks, but these threats take a different form. Natural events include underwater volcanic eruptions and tsunamis, whilst damage arises from ships' anchors and dredging equipment rather than motor vehicles. There have also been isolated incidents of thefts of submarine cables.[435] Ensuring the physical security of submarine cables which are located in remote parts of oceans and in international waters (over which no individual State has jurisdiction) is particularly challenging. This has led to concerns in recent years that hostile States or other agents might sever submarine cables to disrupt military or civilian communications.

In recent years, the focus of policymakers and owners of infrastructure has shifted to consider the threat of deliberate actions to disrupt the operation of the network by inserting, corrupting or gaining control of the software applications on which today's networks depend, or risks arising from errors in the coding (which may disrupt the functioning of the network or create a security vulnerability that another actor can exploit to install other software which will disrupt or threaten to disrupt the functioning of the network). When deliberate, this mode of attack often involves lower costs (software tools or information about vulnerabilities may be readily purchased on the dark web) and may be more easily accomplished than attacks on physical assets (which may require submarines or other equipment or assistance from employees within the operator of the infrastructure to obtain access to

[434] These can be used for legitimate purposes, such as to inhibit wireless use in prisons or cinemas, as well as illegitimate purposes.
[435] For example, off the Vietnamese coast in 2007, see: https://www.computerworld.com/article/2541664/fishermen-pull-the-plug-on-vietnam-s-web--steal-cable-for-scrap.html

assets). Importantly, it is likely to involve significantly lower risks of detection or punishment. Unlike attacks on physical assets, cyberattacks do not require the originator to be physically present at the location of the network assets.[436] This means that attackers can operate remotely, including in other States where they may be beyond the reach of the law enforcement agencies of the State in which the effects of the attack are experienced. Sophisticated hackers can also employ various techniques to disguise their identity, or may assume the identity of others, including innocent, parties.

Although data on the number or nature of threats to software, as opposed to hardware-related elements of digital infrastructure, is not readily available (in part because owners have limited incentives to publicise the extent to which their networks are vulnerable to such threats), it is clear that the significance of cyber threats for owners of digital infrastructure has grown significantly in recent years and is expected to continue to grow. Some of these threats arise from other States, which may use cyberattacks to engage in hybrid warfare.[437] This refers to actions that stop short of full, overt, offensive action and which have plausible deniability (whilst attacks on physical assets inside foreign States may not have).

However, many threats arise from organised criminal groups who are seeking to use the threat of disrupting what are now critical services in order to extort money from the owners of digital infrastructure or their customers. As already noted, the costs and capabilities required to enter this market can be relatively low (at least compared to other ways of threatening digital infrastructure or other forms of criminal activity to earn similar economic rewards), whilst the valuations which firms and States place on avoiding the disruption of critical digital infrastructure may be very high. Thus, large financial gains may be available with risks of detection and punishment that are relatively low. This situation is not unique to digital communications infrastructure and cyber threats to other parts of the economy for financial gain, such as the banking sector or energy networks, are also growing in significance. Even if such criminal activities rarely cause actual disruption to digital infrastructures, the owners of the infrastructure will have incurred costs in defending their assets against the threat or, if their defences have been breached, in removing the software from their systems and repairing the damage done. In some cases, the costs may involve ransom payments by operators of networks, or their suppliers, to criminal organisations or to individual hackers, either to prevent disruption after the network has been compromised or to acquire information about vulnerabilities and stop that information from passing to other malicious actors. Again, data on the magnitude of the threats or the costs to owners of digital infrastructure of avoiding them are not generally available.

The 'commercialisation' of threats to digital infrastructure – as distinct from the threats posed by States, by other ideological groups or arising from errors and accidents on the part of suppliers to or operators of the networks – is a significant development and one which appears to be experienced in

[436] Although there is increasing concern about the potential of terrorist or other groups to use drones to attack physical infrastructure.
[437] The UK Government has said that the greatest cyber threat to telecoms infrastructure in the UK is presented by hostile States, citing Russia as the instigator of an attack on UK telecoms infrastructure in 2017, see: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf p.23.

all countries. The focus of this paper is therefore upon threats from States and from criminal actors pursuing financial gain. Threats also arise from other sources, such as terrorists, religious groups, disgruntled employees or private individuals with no motive other than notoriety or recognition. But the threats which these groups pose appear to be of less significance and concern for owners of digital infrastructure than those arising from States or criminal actors.

4. ACTIONS BY POLICYMAKERS AND FIRMS TO DATE

In this section, we explain, in general terms, actions that have been taken by the owners of digital infrastructure and by States to address the threats described above and to ensure the resilience of digital infrastructure. However, we start with a consideration of the interests and incentives of the private sector owners of the infrastructure.

4.1 Private Owners of Digital Infrastructure

The availability of services and the reliability of digital infrastructure is clearly a matter of concern to the customers of the providers of infrastructure. This is particularly so for corporate customers and other organisations who rely upon digital infrastructure to provide services that must themselves be provided without interruption. Private owners of digital infrastructure will therefore have powerful incentives to minimise disruption and will design and operate their networks with this in mind. Customers may be entitled to financial compensation in the event of service outages and, in competitive markets, customers may move to other suppliers. Firms may also suffer reputational damage with consequences for their longer term financial performance if their networks are disrupted.[438]

The implication of this is that firms will tend to focus their attention most on the resilience of those parts of the network for which they are responsible, which support customers for whom reliability is an important consideration and who may have choices of alternative providers, and/or where disruption is likely to affect large numbers of customers and/or to be highly visible. Data centres provide a good example of this. Corporate users of data centres, including operators of digital infrastructure, require them to host critical software applications without which their own businesses may not be able to function and the failure of which would have significant financial and reputational consequences. Users often have a choice of competing data centre suppliers, both nationally and potentially internationally, and are sophisticated purchasers. The data centre market is also a relatively recent phenomenon and still growing rapidly, with the result that suppliers are less exposed to legacy infrastructure which often make it more difficult or more costly to improve resilience. The consequence of this is that competition between private sector suppliers of data centres seems to have created very strong incentives to provide very high levels of resilience without any need for regulation.[439] New data centres are located with physical security considerations in mind from the outset, including future threats posed by climate change-related events such as flooding, and are designed with a high level of redundancy, both in terms of the facilities which they provide directly and in terms of the supporting infrastructure, such as power supplies, access roads and digital connections. Industry standards have also been developed which allow users to assess and compare

[438] Although there is also evidence that firms which are subject to cyberattacks that disrupt services do not see any adverse long term impact on their share price, see: https://www.jstor.org/stable/27751241

[439] For a discussion, see: https://www.techuk.org/asset/E21741A9-2403-4C4E-A71753C8362861DB/ We note, however, that in May 2022 the UK Government began to consult on whether some regulation of data centres was required, noting that 'it is relatively unregulated for security and resilience, see: https://www.gov.uk/government/publications/data-storage-and-processing-infrastructure-security-and-resilience-call-for-views/data-storage-and-processing-infrastructure-security-and-resilience-call-for-views#part2

the resilience and security of rival data centres. These developments have largely occurred without intervention by policymakers, although of course Government and other public institutions are themselves important customers of data centre providers.

In contrast, owners of local access networks may have weaker incentives when it comes to resilience (although this may vary with the nature of the customer that is being served).[440] In some cases, customers may have no opportunity to switch providers if a network proves to be unreliable. Outages may only affect a small proportion of the operators' customer base, some of whom may not even be aware that the disruption has occurred. Local access networks – particularly fixed or wireline networks - have also been constructed over many decades. This leaves a large legacy of physical assets at locations that may not have been chosen with security or resilience concerns in mind and which are costly and difficult to relocate or protect. Moreover, the location of many assets in local networks will be determined by the location of the customers that they serve, rather than being something over which the owner of the infrastructure has much discretion. To the extent that local communities face threats from, for example, climate change-related events, then the local access networks on which they depend will necessarily be exposed to the same threats.

Core or national networks combine aspects of both local access networks and data centres. Disruption to core networks is likely to affect a larger proportion of customers than the failure of individual local connections. Core network physical infrastructure may be easier to reconfigure than local access networks, but will have a more significant legacy component than most modern data centres. Failures of submarine cables may have even more significant consequences for customers, or for entire populations[441] since multiple networks within a given State are likely to depend on the same cables for connections to the rest of the world. Competition between systems may provide some degree of choice and resilience for users. Private owners and users of submarine cables would therefore appear to have strong incentives to ensure resilience and security, but may also face very significant costs in providing redundancy or in reconfiguring legacy infrastructure, and some bottlenecks may be unavoidable.

Cyber threats to software affect all components of the digital infrastructure. These threats are unlikely to be confined to individual firms, since firms are likely to share software suppliers. In many cases, the responsibility for addressing threats that emerge lies with the supplier of the software code, who will develop patches that are implemented by the owner of the infrastructure or by the supplier themselves. All firms using the software are likely to share a collective interest in addressing vulnerabilities and their suppliers may perform an important role in coordinating such efforts. Since the software is typically updated and installed more frequently than changes to the physical assets of the network (particularly as networks are virtualised), activities to address cyber threats have become

[440] For example, local connections to other critical infrastructure, such as hospitals, energy providers or the banking system, will have a high degree of redundancy.

[441] As seen in Tonga, where volcanic eruptions produced a tsunami which severed the Tonga Submarine Cable which provides the only digital connection (other than satellite) with the rest of the world (via Fiji). It took 5 weeks to repair the cable, see: https://subtelforum.com/tonga-cable-successfully-repaired/

a part of the normal course of business of all owners of digital infrastructure and their software suppliers.

As explained earlier, the past several decades have seen the emergence of economically-motivated cyber threats to businesses on an industrial scale. These criminal actors are well organised and often share information or supply services to each other, as well as to other actors including States, in various marketplaces. Software producers may find themselves bidding against hostile interests to acquire information about vulnerabilities from hackers and prevent them from being more widely distributed. Defending against these threats has become an ongoing cost for businesses, including the operators of digital infrastructure. These costs are generally invisible to customers and often not well understood by policymakers. The total cost of actions to defend against cyber threats is reported to have doubled since 2015.[442] Data on the costs specifically incurred by owners of digital infrastructure is not generally available.

In this context, it is important to recognise that private owners of digital infrastructure will be seeking to pursue a number of other objectives in addition to addressing threats to and the resilience of the infrastructure in which they operate. Most firms operate within markets in which they face competitors and will be seeking to differentiate their services in ways that appeal most to customers. These include other capabilities of the networks, but also their costs. To the extent that measures to address threats or improve the resilience of infrastructure represent additional costs to firms which they cannot reflect in higher prices to customers, an individual firm will find it challenging to adopt them unless all firms in the market are required to do so. It may be difficult to reflect costs in prices because most customers may attach very little significance to the reliability of the network until they experience disruption (resilience is what economists call an experience good, the value of which is difficult to assess in advance) and may find it very difficult in any event to assess how resilient a particular network may be. Customers may also underestimate the costs of switching to another network if their own provider fails. We discussed data centres earlier, but most other customers of other digital infrastructure services are likely to attach greater significance to other factors, such as the price of the services being provided when deciding which supplier of infrastructure to use. It is only when their digital connection is disrupted that resilience is likely to become an issue for most customers and even in those circumstances they may be unsure where responsibility for the disruption lies.

Since a firm's capacity to pass costs onto its customers is, to some extent, a function of how competitive the market in which they operate is, efforts by policymakers to promote greater competition in the provision of digital infrastructure may reduce the ability of firms in those markets to collectively invest in efforts to improve resilience, even if the threat of losing customers means that individual firms may have greater incentives to do so. Other factors may also come into play when considering the relationship between competition and resilience. For example, digital infrastructure owners in more concentrated markets may be willing to assume more financial risk in their operations

[442] See: https://publications.jrc.ec.europa.eu/repository/bitstream/JRC121051/cybersecurity_online.pdf p.1.

in the expectation that the State would provide support in order to avoid failure.[443] The relationship between market structure and resilience is therefore complex and requires an assessment based on specific facts, as we discuss further below.

Irrespective of the extent to which firms can or will pass costs onto customers, they have incentives to reduce the costs they face. This means that operators of digital infrastructure will seek to ensure a competitive supply of their inputs. As we discuss further below, the past twenty years have seen the opposite trend, with significant consolidation in the market for digital infrastructure equipment, notwithstanding the entry of Chinese firms, such as Huawei and ZTE. But this does not alter the commercial incentives of the operators, which remains to ensure competition or diversity in supply. Recent efforts to promote Open RAN technologies, also referred to below, are partly motivated by these considerations. At first sight, greater diversity of suppliers might be expected to contribute to greater resilience. This is both because greater competition between suppliers can be expected to drive up the quality of the goods and services supplied, and because different operators may then deploy equipment from different suppliers, providing a greater degree of redundancy and differentiation if a threat arises to the equipment of one supplier, but not another. However, the extent to which diversity in the supply chain contributes to resilience is more ambiguous than might commonly be supposed. Diverse suppliers can increase the range of potential vulnerabilities in the equipment, or increase the risk of errors when trying to integrate equipment from multiple suppliers into a network. Moreover, different suppliers may themselves rely upon common components, systems or standards, with the result that diversity may be more apparent than real.[444]

Competition on other aspects of service may also make it more difficult for firms to co-operate with each other in order to address collective or system-wide challenges in relation to resilience. Firms may be reluctant to share information about common threats with their competitors or may seek to 'free ride' on the actions of others. On the other hand, to the extent that competition in digital infrastructure promotes duplication and diversity in infrastructure, it could contribute to system-wide resilience. This will depend crucially on users being able to switch between competing networks and upon those networks retaining the sufficient spare capacity to be able to accommodate additional users in exceptional circumstances. Competition between networks tends to discourage the hoarding of excess capacity, and firms are unlikely to want to incur the costs of providing additional capacity for the benefit of their competitors.

4.2 Role of States

A role for policymakers arises precisely because there are reasons to think that private firms in competitive markets may not optimise the resilience of the system as a whole. The provision of the

[443] The financial collapse of a number of digital infrastructure providers including Global Crossing, KPNQwest in the early 2000s threatened significant disruption of the internet both globally and in Europe which was narrowly averted. Worldcom carried around 40% of the world's internet traffic and KPNQwest carried around 25% of the internet traffic in Europe at the time of their demise, see: https://www.zdnet.com/article/kpnqwest-collapse-shakes-european-internet/

[444] See: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf p.22.

world's digital infrastructure is complex and highly interdependent undertaking involving many actors with different and sometimes conflicting incentives. Individual firms are likely to ignore any costs or consequences of disruption which are imposed on other actors, or which do not place them at a competitive disadvantage, and to be reluctant to assume costs for activities which benefit others. If all networks are disrupted by a particular event in a similar manner (such as, the failure of a submarine cable on which all networks in the particular country depend), then no individual operator may suffer commercially, but customers as a whole will still do so. This may create incentives for firms to pool rather than diversify risk. Alternatively, operators which become aware of a particular threat may be reluctant to share details with competitors or may be unwilling to incur costs to eliminate the threat if their competitors would also benefit from those actions while avoiding the costs. States exist to address these kinds of collective action and co-ordination problems, of which there are many when it comes to the resilience of digital infrastructure.

Although various forms of market failure might justify State intervention to improve resilience in digital infrastructure at a national, regional or global system level, the ability of States to intervene may also be compromised by conflicts of interest, competition and limits to the exercise of power. In this context, firms with global reach, such as Google, Amazon and Facebook, may have the capacity to bypass the limitations of States by provisioning and operating their own digital infrastructure on a multi-State or near-global basis. This reduces the dependency of these firms both on other national firms and on States to ensure the resilience of the facilities on which their operations depend, allowing them to internalise or 'privatise' many of the co-ordination issues which otherwise exist between firms in different States or within a State.[445] This may have implications for competition between these firms and other firms that lack the resources or scale to do this, but it may also contribute to the resilience of other operators of digital infrastructure who use the cloud platforms operated by these firms to host their own network operations. This may then introduce questions for policymakers who seek to retain a role in regulating or otherwise overseeing the digital infrastructure that is controlled by these global providers, or which is hosted on their platforms at a physical location that is outside of the State in question. This is another way in which the virtualisation and cloudification of digital networks will present challenges for policymakers who continue to operate in a world in which legal jurisdiction remains tied to physical boundaries. Some of the current concerns in Europe about the dependency of European firms (including owners of digital networks) on United States' cloud service providers over which EU authorities have had limited oversight is an illustration of this.

4.3 Threat Evaluation

Actions by States in Europe and elsewhere have already been taken to address some of the challenges in co-ordinating action by a large number of individual firms. The first feature of these is the assumption that private firms may have insufficient commercial incentives to adequately identify and address threats or invest in resilience. This has led to measures, such as the (revised) Network and

[445] Note that global self-provision by these firms is, to date, largely confined to submarine cable facilities on major routes and data centres. The global firms still remain highly dependent on local telecommunications operators for the provision of local connections to their final customers.

Information Security and (revised) Critical Infrastructure Directives[446] in Europe and to similar initiatives in the United States.[447] These enable regulators or other public authorities to require firms to undertake their own audits of potential threats and provide evidence of plans and strategies to mitigate them. Regulators are required to review these plans and are given powers to impose financial penalties and otherwise take enforcement action if measures that regulators consider to be required are not taken. These exercises, therefore, involve the sharing of information by firms with public authorities, both to enable the authorities to obtain an overall view of the system as a whole and of the specific actions which individual firms are taking or propose to take. This helps to break down the large information asymmetry which otherwise exists between the firms and public authorities with regard to the operation of digital infrastructure. It also enables public authorities to intervene and require further measures to be taken if they identify any gaps. In some cases, such as the UK, very detailed requirements and expectations for the security and resilience of networks have now been developed by public authorities.[448]

This seems to be a sensible first step, although its effectiveness will depend on the capacity of the regulatory bodies charged with overseeing the exercise to assess and challenge the information which is provided to them by the firms and by the willingness of those bodies to take enforcement action if firms fail to alter their behaviour or take actions which the authorities conclude are required.[449] Without this, it becomes an exercise in describing what the market is doing, rather than moving the market to a position to deliver a better set of outcomes. Critics of the European NIS Directive, which is currently being revised, note that enforcement to date, which is the responsibility of Member States, has been very weak. There is also a risk that audits which focus on threats and risks for individual firms do not adequately recognise the system-wide risks or mitigation measures which will require actions by many or all firms.

4.4 Information Sharing

A further step is to take action to overcome barriers to information sharing that firms may face. These do not aim to change the incentives which firms have or the actions they might take to prevent disruption, but they might enable other firms (and policymakers) to respond to threats more effectively once they become known. One issue is that firms may be reluctant to share information with customers whose interests may be affected by the disruption. Measures to require firms to explain to customers what has happened and the steps they are taking to resolve an incident may allow customers to take greater account of resilience when choosing between competing suppliers, sharpening the incentive for firms to invest in it. Measures that require firms to share information with States or regulators may enable public authorities to obtain a better understanding of the threats that are faced and so be in a better position to develop policies that might help address them. In

[446] The first CIS Directive applied only to energy and transport networks.
[447] See: https://www.cisa.gov/sites/default/files/publications/2021_ncf-status_update_508.pdf
[448] See: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1057446/Draft_telecoms_security_code_of_practice__accessible_.pdf
[449] In the case of the 2008 Critical Infrastructure Directive, 16 Member States failed to designate any entity as being governed by it.

Europe, the proposed Directives also require the Member States to share information with each other and with the European Commission. Measures that require firms to share information with other firms, including their competitors, may help those firms collectively anticipate threats, allow other firms to take defensive action once one firm has been attacked and/or reduce overall costs for the industry. On the other hand, information sharing may also encourage 'free riding' by firms who rely on others to inform them about threats rather than assuming that responsibility themselves. It may also open the door to the sharing of information beyond that which relates to potential threats, which could undermine competition.

4.5 Collaboration with Public Authorities

A third set of measures may involve direct collaboration between public authorities and firms in responding to significant threats. This recognises the limitations which private firms may face in detecting or apprehending parties responsible for malicious acts, and the role of the State in prosecuting criminal activity and in addressing threats that are posed by other States. For instance, the European Directives anticipate significant co-operation between dedicated Computer Security Incident Response Teams in Member States and ENISA, the pan-European cybersecurity agency in addressing specific incidents.

In addition, States have taken action to help in the pursuit and prosecution of those responsible for the disruption of infrastructure or to restrict the availability and proliferation of technologies that facilitate such acts. The most important of these is the 2001 Cybercrime Convention (Budapest Convention) amongst the Council of Europe members concerning the prosecution of crimes committed on the internet[450], which enables law enforcement agencies to co-ordinate their activities when seeking extradition and prosecution of actors residing in other signatory countries.[451] In a similar vein, the Waassenaar Arrangement of 1996 seeks to prevent the sale of all kinds of weapons technologies (including cyber technologies) to 'States of concern'. Most European countries and the United States are signatories, but some important States are not, and critics contend that these agreements have not prevented the widespread proliferation and use of cyber technologies.[452] Efforts being undertaken through the United Nations' Cybersecurity Open Ended Working Group have yet to produce tangible outputs[453] (with informed observers believing that this is unlikely to happen in the foreseeable future)[454].

4.6 Foreign Ownership and Control

Other measures adopted by States which may be relevant for resilience and other concerns, relate to limitations on the foreign ownership of digital infrastructure. The measures we have described so far presuppose that all firms will share the same commercial and corporate objectives, irrespective of

[450] See: https://rm.coe.int/1680081561
[451] See: https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf
[452] See: https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/
[453] See: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
[454] See: https://www.monash.edu/__data/assets/pdf_file/0019/232525/clough.pdf, p.37

who owns the firm. Following privatisations and efforts to promote new entry into markets, the ownership of digital infrastructure, particularly in Europe, has become very diverse, with assets owned by firms based or controlled in Asia, the United States, UK and Russia. Some limits on foreign ownership on national security or protectionist grounds have been applied: for example, America Movil, a Mexican firm, offered to acquire the remaining 70% interest (having already acquired 30%) in the Dutch operator, KPN, in 2013 but found the bid opposed by the Dutch Government on 'national security' grounds. On the other hand, Orascom, an Egyptian firm, owned significant wireless assets in Italy and Greece, some of which were subsequently sold to Veon, in which a Russian firm, Alfa Group, is a significant shareholder. In 2019, China Mobile opened a data centre in the UK and, in 2021, a second one in Frankfurt, and Huawei is an investor in a major new submarine cable system that is expected to connect Europe with Asia.[455]

The United States has screened foreign firms seeking to acquire significant assets, including digital infrastructure assets, under its Committee on Foreign Investment or CFIUS regime for many years. More recently, Europe has adopted measures that encourage Member States to screen foreign investors in critical infrastructure, as in the KPN case, and to co-operate with each other when doing so.[456] The UK has recently adopted a similar regime.[457]

Although States may screen the ownership of assets physically located within national borders, it may be more difficult for States to influence the ownership of submarine cables on which those national networks may depend for connections to the rest of the world. The Australian Government has intervened on several occasions to fund submarine cable projects which were considered to be of strategic significance and would otherwise have likely been developed by Chinese firms.[458] The United States' Government provided funds to the Federated States of Micronesia under similar circumstances in 2021.[459]

'National security' concerns are generally cited when justifying decisions to prohibit certain forms of foreign ownership, although detailed reasons are rarely made publicly available. It appears that many of the concerns are motivated by an assumption that firms residing in certain States, most notably China, should be viewed as agents of the State rather than independent commercial entities.[460] On this view, if these firms were to control digital infrastructure in another State then this would mean

---

[455] See: https://www.bloomberg.com/news/articles/2021-03-05/china-s-peace-cable-in-europe-raises-tensions-with-the-u-s

[456] See: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452&from=EN Interestingly, decisions on security grounds remain a matter for Member States despite many reviews of mergers on competition grounds often being undertaken by the European Commission rather than the Member States.

[457] See: https://www.gov.uk/government/collections/national-security-and-investment-act

[458] The first case in 2018 related to funding provided by the Australian Government to build a submarine cable to the Solomon Islands, a project which would otherwise have been undertaken by Huawei, see: https://www.reuters.com/article/us-australia-solomonislands-internet/australia-keeps-china-out-of-internet-cabling-for-pacific-neighbor-idUSKBN1J90JY . In the second case, in 2021 Telstra purchased Pacific assets of Digicel (which included submarine cable interests) with significant financial support from the Australian Government, alleging to ensure that they were not acquired by China Mobile, see: https://www.reuters.com/article/digicel-group-m-a-telstra-corp-idUSKBN2HE0K9

[459] See: https://www.reuters.com/world/asia-pacific/exclusive-us-funding-tapped-pacific-undersea-cable-after-china-rebuffed-2021-09-03/

[460] China Mobile is directly controlled by the Government of China, with just under 30% of shares listed on public markets. Huawei states that it is owned by its employees. A Chinese State owned enterprise is the largest (30%) shareholder in ZTE.

that the Chinese Government would be exercising de facto control over those assets. This control could be exercised for various purposes, including obtaining access to sensitive communications or data. However, it might also allow another State to disrupt the functioning of the digital infrastructure over which it exercised a significant degree of control. Moreover, if the operators of digital infrastructureare agents of a hostile State, they might have very different incentives and objectives compared to other commercial operators. The threat of losing customers or reputation as a result of disruption may be less of a concern to them, than for conventional firms owned by private shareholders. The ability of regulators and public authorities to influence the conduct of the firm by influencing its commercial incentives may therefore be more limited than if it were to be owned by private investors independent of any State influence.

We are not aware of any specific evidence to suggest that any State has sought to disrupt the operation of digital infrastructure in another State through its influence over the ownership of that infrastructure. However, advocates of restrictions argue that it is better to take a precautionary approach than to discover after the event that digital assets are controlled or subject to influence by foreign States.

Recently, concerns in Europe and the United States about the indirect exercise of State influence have extended beyond the ownership of the digital infrastructure to those supplying the network equipment. Over the past 20 years, Chinese firms such as Huawei and ZTE have become major suppliers of telecommunications equipment to operators of digital infrastructure throughout the world (with the exception of the United States). The nature of today's digital infrastructure is that suppliers of equipment, including software, will provide continuous support to their customers, many of whom lack the technical capabilities to undertake tasks for themselves. This requires the supplier to have continuous access to the software after it has been deployed within the operational network.[461] This in turn means that equipment suppliers could be in a position to exercise significant control over the functioning of the network, and may be able to do so in ways that may not be easily detected or controlled by the owner of the assets. To the extent that Chinese suppliers are considered to be capable of being directed or influenced by the Chinese Government, this means that the Chinese State may obtain a degree of control over the digital infrastructure in other States, even if that infrastructure is owned by a firm that is not itself considered to be a threat.

The history of this issue provides a good illustration of the conflicting objectives which States may have, as well as conflicts between the objectives of individual firms and States. Initially the emergence of Chinese firms such as Huawei and ZTE as global equipment suppliers had been greatly encouraged by European owners of network infrastructure who were seeking to lower their equipment costs and increase diversity and competition in their supply chain (otherwise dominated by Ericsson and Nokia

[461] 'The risk of exploiting legitimate network access is hard to mitigate. Most importantly, it cannot be reduced by equipment certification, source code inspection or other technical requirements on the level of standards, implementation or configuration. Certain operational practices can potentially reduce the risk – strictly controlling a vendor's remote access, extensive logging of remote support sessions, anomaly detection, to name a few', p.14, see: https://www.stiftung-nv.de/de/publikation/whom-trust-5g-world-policy-recommendations-europes-5g-challenge

following the earlier consolidation of the telecoms equipment supply market in the 2000s). These firms were under pressure to lower their costs as a result of competition, particularly in the European wireless market. Many of the early European customers for the Chinese firms were new wireless companies who obtained financial support from the suppliers to assist in building new local access networks. European policymakers were promoting entry by new wireless operators, believing that increasing competition would benefit consumers. In 2013, the European Commission raised concerns that Chinese Government support for Huawei and ZTE enabled them to offer unfair financial terms to European customers, thereby unfairly undercutting European equipment suppliers like Ericsson and Nokia.[462] It was claimed that the European firms themselves did not pursue a formal trade complaint because of fears that they would then be excluded from supplying the Chinese market. Economic considerations were in European policymakers' minds, but there was no reference to security concerns.

An exception was the Government of the UK, which had in 2010 established an Oversight Board in co-operation with Huawei to screen the Huawei products and services which UK infrastructure owners wished to purchase and deploy in their networks. The UK Government did not seek to deny UK operators access to Huawei's technologies but sought to screen software and hardware to mitigate against any 'back door' security risks. A later review of the process by the UK Government concluded that "Given the range of alternative attack routes available, an adversary would not find implementing 'backdoors' either the lowest risk, easiest to perform, or the most effective means of performing a major cyber attack on UK telecoms networks today".[463] The review concluded that the greater threat arose from the poor quality of some of the software supplied by Huawei (and its failure to address vulnerabilities when informed about them by the UK Government). Software errors would have made UK networks vulnerable to cyberattack by any third party, not just the Chinese State.

In the United States, Congressional policymakers in 2012 had concluded that they should prohibit the use of Chinese equipment in digital infrastructure operated within the United States. Owners of digital infrastructure in the United States were 'discouraged' from purchasing equipment from Chinese vendors, and in 2018 a Bill formally prohibited any operator of infrastructure using Huawei or ZTE equipment from working with federal agencies. The Secure Equipment Act of 2021 (finally) prohibits the holding of any network equipment licence by Huawei or ZTE. In 2019, the United States' Administration also prohibited its domestic firms from supplying Huawei with technologies that it used in products that it sold elsewhere in the world. This therefore had implications not only for Huawei's ability to sell services in the United States, but on its capacity to supply services to firms in other States around the world (and hence those States' assessments of their own commitment to using Huawei equipment).

[462] See:https://www.reuters.com/article/uk-eu-china-telecoms-idUKBRE93F1DC20130416

[463] See: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf p.25.

The European Commission sought to encourage a common approach to the issue in Europe by introducing a '5G toolbox' to help Member States undertake a risk assessment of 5G networks.[464] Rather than prohibit all Chinese equipment, France and Germany have implemented oversight regimes (with powers to prohibit the use of equipment that is deemed to represent a threat) similar to that adopted in the UK since 2010. Security risks, such as access to sensitive data, may vary depending on the function of the components that are being supplied. Some owners and States consider, for example, that the core network represents a greater security risk than the local access network.[465] On this basis, equipment from Huawei or ZTE may be employed in the local access network, but not in the core network. Whether the same considerations apply in relation to concerns about network resilience is unclear.

Other States, including Sweden, Australia and the UK itself, have followed the United States in prohibiting the use of equipment supplied by Chinese firms.[466] The UK has required owners to remove all existing 5G (but not 4G) equipment provided by Huawei by 2027.

Actions by States have led to tensions with the operators of the digital infrastructure, many of whom will incur significant costs in removing existing equipment or who fear that the removal of the competitive constraint which Huawei and ZTE had imposed on the remaining suppliers, Ericsson and Nokia, will result in higher costs for equipment in the future. In an effort to mitigate these concerns, the United States, United Kingdom and European Governments have taken an active role in promoting the development of 5G Open RAN technology, which is regarded by operators of digital infrastructure as providing an opportunity to enable the entry of new equipment suppliers for 5G. Furthermore, the UK Government has set a target of 35% of traffic to be carried over Open RAN networks by 2030,[467] however it remains to be seen how this will develop.[468] What is clear is that decisions to prohibit the use of Chinese equipment have, in many cases, been taken by policymakers before it was clear whether suitable alternative suppliers would emerge to replace them.

As Chinese firms came to play a significant role in the supply of existing technologies for digital infrastructure, they have also assumed an increasingly important role in the global development of the next generation of technologies, including 4G and now 5G and 6G wireless technology. The two aspects are interrelated and it is difficult to see how firms could participate in standardisation activities without also participating in the supply of the technologies that are based upon them.[469] This work is

[464] See: https://digital-strategy.ec.eurohttps://undocs.org/A/Res/74/247pa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

[465] Whether the distinction between local and core network can be sustained in the 5G context has been disputed by some commentators, see: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_115-129_Purdy-Yordanov-Kler.pdf?ver=-b6UQO4hfPEjis5OQlYdZA%3d%3d p.121.

[466] Australia in 2018, the UK in 2020, see: https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy

[467] See: https://www.gov.uk/government/news/a-joint-statement-on-the-sunsetting-of-2g-and-3g-networks-and-public-ambition-for-open-ran-rollout-as-part-of-the-telecoms-supply-chain-diversification

[468] See: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Donahue_14-35.pdf for a discussion of the options open to the US Government to promote alternative sources of equipment supply.

[469] The industry-led ORAN Alliance incudes at least 30 Chinese firms according to Baldwin and fails to address US security concerns in various other ways as well, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3861826_code1037494.pdf?abstractid=3861826&mirid=1,, p.6.

undertaken through global standards bodies, such as 3GPP, which enable collaborative activity and contribution to the joint development of standards with which all suppliers can work. This enables equipment produced by different suppliers to interoperate and perform certain common functions, and it also enables a framework within which holders of essential patents can be recognised and subsequently remunerated for their contributions.

These standards bodies occupy an interesting position. Most originated as private firms who might otherwise compete recognised the need to co-operate to develop new technologies which required the pooling of knowledge and expertise. States have taken an interest in the standards setting process when disputes have arisen between firms (such as, in relation to the licence fees payable to holders of 'standards essential' patents), but the process is otherwise led by the private sector. The growing involvement and influence of Chinese firms, many State-owned, in the global standards process has led to concerns from other States that this is another route by which the Chinese Government may be able to exercise influence over future network technologies, potentially to the disadvantage of other States or their firms. Again, we are not aware of any evidence that this has in fact been demonstrated to be the case. Nonetheless, States, including the United States and European States, are now being urged to consider how to address the question of inappropriate State influence in these bodies.[470]

[470] See: https://itif.org/publications/2021/11/08/mapping-international-5g-standards-landscape-and-how-it-impacts-us-strategy, p.34 at https://www.cybersecuritycouncil.nl/documents/reports/2021/02/17/report-strategic-autonomy-and-cybersecurity-in-the-netherlands Similar concerns arise in relation to other technical bodies that undertake important global governance functions relevant to global digital infrastructure, such as the Internet Engineering Task Force and ICANN, see: https://www.swp-berlin.org/publications/products/research_papers/2019RP14_job_Web.pdf

5. CRITICAL ASSESSMENT

Several themes emerge from our discussion of the actions of firms and States to address threats to and ensure the resilience of digital infrastructure.

The first observation is that States are responsible for policies and actions which seek to improve resilience or mitigate threats whilst at the same time themselves often being the source of threats. Although the discussion above focussed on concerns of other States about threats posed by Chinese firms and the Chinese State, European States, the UK and the United States have all developed cyber capabilities of their own that allow them to disrupt the functioning of the digital infrastructure of other States. It is not only that States themselves engage in such activities, but that the people, skills and technologies developed for this purpose are also transferable, and frequently do transfer to the private sector, including criminal organisations.[471] States will seek to remove vulnerabilities in digital infrastructure within their own territory, whilst retaining the capacity to find and exploit vulnerabilities in other territories. In this sense, States will always be both part of the problem and part of the solution when it comes to thinking about resilience in digital infrastructure.

Secondly, States have often been pursuing objectives in relation to digital infrastructure which may conflict with each other. The privatisation of digital infrastructure results in a loss of direct control by States and a reliance on other means, such as regulation or ownership restrictions, to influence the conduct of the owners of digital infrastructure. Policies to promote competition in network infrastructure may improve redundancy and hence resilience and the threat of losing customers may incentivise firms to invest more in the resilience of their networks, but competition also imposes greater financial pressures on firms and may lead to fragmentation. One response of European operators to these pressures was to turn to Chinese equipment suppliers which, twenty years later, has now led to new concerns about the security of European digital infrastructure. Similarly, competing firms may find it more difficult to share information about common threats and vulnerabilities amongst themselves if they think this might be exploited by others for commercial or reputational advantage. They may also find it difficult to co-ordinate actions without external direction. Firms in competitive markets may also have incentives to minimise the amount of excess capacity in their networks or to fill it by reducing their prices rather than have it available for the users of other networks who find their services disrupted.

5.1 Resilience and Merger Policy

To date, consideration of security or resilience concerns has tended to be conducted by policymakers in silos and the pursuit of other economic policy objectives, such as the promotion of competition that is often the primary responsibility of the telecommunications regulator, do not systematically take resilience considerations into account. It is therefore not surprising to find that there is often some tension or misalignment between the two.

[471] A well-known example is NOS, the developer of the Pegasus surveillance software, based in Israel and supplier to both States and many private actors.

A good illustration of this is merger policy. Many merger regimes allow some mergers to be assessed on national security grounds, but these assessments invariably consider the identity of the prospective owners of the assets rather than the implications of changes in market structure for the resilience of supply. Any assessment by the European Commission of a merger or network sharing arrangements which would result in the consolidation of networks (and so potentially lead to a loss of redundancy and greater concentration of risk) will today be undertaken on competition or economic grounds alone and there has, in the past, been considerable resistance on the part of competition authorities to consider other 'non-economic' factors in their assessment. This view is beginning to change, with the European Commission, for example, recognising that competition policy has an important role to play in the pursuit of climate change objectives.[472] The UK Competition and Markets Authority has also recently published a paper which explicitly addresses the relationship between competition policy generally and concerns about resilience.[473] Merger policy is one way in which market structure can be influenced, as in the case of the mergers which resulted in the rapid consolidation of the telecoms equipment supply market in the late 1990s, but other aspects of competition policy, such as those relating to the review of network sharing arrangements between owners of digital infrastructure, are also important.

In addition to competition authorities, European and national regulators also have a role in promoting entry and expansion in digital infrastructure markets and, in doing so, can influence market structure. Article 3 of the European Electronic Communications Code requires national regulators to promote the interests of citizens by 'maintaining the security of networks and services',[474] but makes no specific reference to resilience, including any consideration of resilience at a system wide level. It is therefore unclear, for example, whether the existing regulatory framework would allow national regulators to direct individual firms to maintain surplus capacity in their networks in order to improve the systemic resilience of a country's digital infrastructure, or how they would be expected to consider such objectives alongside other objectives.

5.2 Redundancy and Switching

National regulators have taken actions to promote switching between networks in order to facilitate competition between suppliers, but very little consideration has been given as to whether measures could be taken that would improve the ability of users to benefit from resilience that is provided by having competing networks by enabling large groups of users to switch networks in the event of disruption.[475] It is possible that the audits which are envisaged by the revised European Directives will

[472] See, for example: https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/competition-policy-support-green-deal_en

[473] 'Resilience and competition policy', see: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1064924/Resilience_and_competition_policy_-_AC.pdf

[474] See: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1972

[475] During the war in Ukraine, the Ukrainian mobile operators have implemented national roaming arrangements, with one commentator noting 'this was a world's first in that it never been implemented by any country for any extended period of time. Isolated cases in the past have included T-Mobile and AT&T sharing radio access in an ad-hoc manner after Hurricane Sandy in 2012. By doing this, the authorities have massively increased the ability for the Ukrainian population to use their mobile networks. This meant at a practical level, that even if

identify actions which firms will then be required to take to ensure that customers can switch between networks (whether local, core or international) quickly in the event of disruption, but we noted earlier the risk that these audits will focus on individual firm resilience rather than system-wide measures, of which switching would be an example. Additionally, as far as we know, no consideration has been given as to how to ensure there is sufficient excess capacity on networks to accommodate users if they were able to switch. Finally, relatively little thought seems to have been given to ensuring diversity in the actual deployment of equipment in networks, such that a failure of the equipment supplied by one firm did not result in disruption to all the networks in a country or any particular geographic region or location.

5.3 Foreign Ownership or Control

It may be politically interesting for policymakers to focus on threats that are said to be posed by foreign ownership of assets or influence over suppliers. However, when it comes to digital infrastructure this risks ignoring the many other, lower cost and more difficult to detect, means by which a foreign State could disrupt digital infrastructure in another State. It is sometimes difficult to avoid the impression that these concerns might be appropriate in a world where threats to physical assets were still the primary concern. However, when digital infrastructure is more likely to be disrupted through cyberattacks that originate outside of the country, it is not obvious why controlling the ownership or source of the physical assets is likely to have much influence over the resilience of the infrastructure. As noted above, the UK Government, which has developed significant experience and expertise in these issues, concluded that the threat arising from the use of Huawei's equipment in UK networks was not because it provided a secret 'back door' to the Chinese Government, but because poor quality software had vulnerabilities which Huawei appeared slow to address. Prohibiting the use of Chinese equipment in domestic digital infrastructure may be an act which is easy to understand and communicate and which appeals to patriotic or popular sentiments, but it will do little to address the more complex, and likely more difficult to resolve, sources of vulnerability.

5.4 Submarine Cables

Ironically, the assets where physical threats and therefore ownership might be most significant are those policymakers appear to have paid the least attention to, at least to date. This may be because ownership of submarine cables is often shared amongst owners from States on either end of the cable or because projecting State control over physical assets which reside in international waters is a

one or 2 of the mobile operators had damaged or de-powered cell-towers in an area, as long as a single operator served an area any Ukrainian mobile phone subscriber could use it. National roaming was further enhanced on the 12th when limited 2G/3G internet was made available. This meant that people using the service could use popular messenger apps to communicate, as well as voice and SMS.', see: https://blog.adaptivemobile.com/the-mobile-network-battlefield-in-ukraine-part-1?hsLang=en Following a major mobile network outage in Canada in 2022, the Minister for Industry directed the mobile operators to implement emergency national roaming and improve communications with customers and with each other. These reflected in a Memorandum of Understanding on Telecommunications Reliability, adopted in September 2022, 'to ensure the reliability and resiliency of communications networks that are a significant lifeline for those in need during natural disasters, network failures and other impactful emergencies', see: https://www.commsupdate.com/articles/2022/09/08/canadian-operators-agree-to-emergency-roaming-and-mutual-assistance-commitments/

difficult and complex matter.[476] It may also be because submarine cable systems are largely invisible most of the time. Australia is a country which does appear to have concluded that the ownership of certain submarine cable infrastructure is a strategic concern, with implications for the resilience of its domestic networks which rely upon that infrastructure to connect to the rest of the world. As noted above, the Australian Government has sought to exclude Chinese firms from owning certain cable infrastructures by providing funding directly to other States or to Australian firms who have then acquired the assets. We found a few examples of other States (other than China) taking a strategic interest in submarine cables, although a number of reports and studies, including by NATO researchers, have highlighted the issue.[477] One UK study by Policy Exchange concluded that: "A successful attack would deal a crippling blow to Britain's security and prosperity. The threat is nothing short of existential. Working with global partners it is crucial that we act now to protect against these dangers, ensuring that our century's greatest innovation does not also become its undoing".[478] Recognising the importance of resilience, new sensing technologies are beginning to be deployed by owners of submarine cable systems in order to monitor their systems in real-time.[479]

5.5 State Influence

Controls on ownership or the origin of equipment may, of course, be relevant to the pursuit of a variety State objectives, including national security, privacy or industrial policy, even if the impact on the resilience and security of digital infrastructure is relatively marginal.[480] They may also be part of wider geo-political considerations which are beyond the scope of this project. Indeed, one of the concerns among European and United States' policymakers appears to be that Chinese firms, whilst nominally pursuing commercial objectives, are, or could be, subject to other opaque influences, outside the rule of law, which European or United States' firms – where privatisation has established a clear legal boundary between firm and State – may not be.[481] Boundaries between organised criminal activity that originates in some States and the State itself may also be unclear in some instances (as is often alleged with Russia). In activities such as standards-setting, European and United States' policymakers have generally assumed that the activities are being pursued with commercial interests rather than State or wider geopolitical interests in mind. However, the involvement of Chinese firms may alter this, which may in turn mean that European and American firms find themselves increasingly under pressure from their own Governments to pursue actions or take positions that may not be in their narrow commercial interest, but which are considered to be in some broader national or regional interest.

---

[476] The laying of cables is governed by the UN Convention of the Law of the Sea of 1982, with States having obligations to impose criminal and civil penalties on those responsible for negligent or intentional injury to cables. Many commentators regard the UN Convention as being out of date and poorly enforced.

[477] See: https://www.mdpi.com/1424-8220/20/3/737

[478] See: https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf, p.5.

[479] See: https://www.ptc.org/2022/01/fibersense-and-sx-announce-world-first-live-fiber-solution-to-monitor-and-protect-submarine-cables/

[480] For example, Donahue discusses the resilience of US digital infrastructure in terms of ensuring US global military capability during war (which he refers to as planning for 'the worst possible day'). The requirements for resilience under these circumstances, and the steps a State might need to take to secure them, may prove quite different from concerns about the resilience of commercial services at other times, see: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Donahue_14-35.pdf

[481] To note there are many allegations that European and US private firms also engage in unlawful or secret activities on behalf of the State, see e.g. https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

The 5G experience suggests that policymakers in Europe and the United States will need to take a more strategic and forward-thinking approach to these matters in the future than has been taken in the past. Chinese equipment has been deployed in European digital neworks for several decades without significant concerns being raised. Suddenly, however, owners of digital infrastructure have been required to remove Chinese 5G equipment that has already been deployed, leaving them reliant on only two suppliers for equipment and without clear evidence of other credible suppliers to replace them. The costs of extracting and replacing legacy equipment are significant, and the time required to do so may mean a network remains exposed to threats in the meantime.[482]

This suggests policymakers ought to anticipate and assess threats at an earlier stage, and determine what actions are required to address them while also considering the implications of those actions for commercial actors. In doing so, it will be important to distinguish between threats that might be thought to arise from the participation of a hostile State in the standardisation process, involvement in the equipment supply chain, involvement in the deployment and configuration of the equipment, or involvement in ongoing maintenance and upgrades. It would also be important to consider how any approved equipment or software is then actually deployed by firms. If all firms rely upon the same supplier to provide network infrastructure at the same locations, then any benefits from diversity or redundancy (or from the removal of foreign suppliers that are not trusted) are likely to be lost or at least greatly undermined.

The prospect of greater State involvement in standards bodies or early-stage development of new technologies should also be weighed against other, particularly economic, considerations. As just noted, many of the most significant developments in digital technologies have, to date, been the result of global collaboration between private sector firms, including firms which may be regarded as controlled by States (as well as being driven by early-stage Research and Development that is funded by States). Ownership or import restrictions that risk Balkanising future technological developments may deprive all owners of the digital infrastructure of access to new technologies or raise the costs of supply. Either could lead to lower levels of resilience throughout the world's digital infrastructure and so actions which inhibit collaboration and trade in an attempt to improve security may end up having the opposite effect.

The evidence in this paper suggests that State involvement in developing new technologies will need to be more strategic and much less reactive than it has been to date. The push to 'virtualise' digital infrastructure by abstracting the physical hardware from the operational software and, increasingly, to host the software in a third-party cloud environment, has been led by the private owners of the networks (and by the big digital services firms that rely on that infrastructure to deliver services to their customers). Policymakers in Europe and the United States have enthusiastically adopted Open RAN technology, which disaggregates the front haul antennae from the control and other functions of

[482] The UK Minister has said of the ban on all Huawei equipment by 2027:' Today's decision to ban the procurement of new Huawei 5G equipment from the end of this year will delay rollout by a further year and will add up to half a billion to the costs. Requiring operators, in addition, to remove Huawei equipment from their 5G networks by 2027 will add hundreds of millions to the cost and further delay roll out. This means a cumulative delay to 5G rollout of two to three years and costs of up to two billion pounds.'

the base station, as a means of enabling entry by (non-Chinese) suppliers into the 5G local network equipment market in the hope of remedying the loss of competition resulting from their efforts to exclude Huawei and ZTE. At the same time, work is only beginning to be undertaken on the question of whether Open RAN technology could introduce new vulnerabilities into wireless networks (such as, through the exposure of more open interfaces).[483] It is beyond the scope of this project to undertake this assessment[484], but it is at least possible that Open RAN equipment supplied by a trusted vendor might prove less resilient than alternative technology. Private firms may still favour Open RAN networks on cost or other commercial grounds, but States will first need to have undertaken a full technical assessment of the implications for security and resilience objectives before coming to a view.[485] Another important development which will have implications for resilience that are difficult to predict and which requires further study is Mobile (Or Multi-Access) Edge Computing, which involves the deployment of cloud computing capability at the edge rather than the centre of the network in order to support very low latency applications.[486]

In addition, national policymakers will continue to struggle with how to regulate and oversee infrastructures that are hosted and controlled in global cloud environments and for which there is no 'switch' that is located at a particular geographic location. Requirements that equipment or software be 'onshored' so as to fall within the legal jurisdiction of the State may involve other costs and may create the illusion of oversight rather than the reality. Moreover, the controller of the physical network assets may have little or no control over the communications which run over them.[487] Again, the tendency of policymakers to associate the physical location of assets with the exercise of jurisdiction or control will be increasingly challenged by the virtualisation of the infrastructure.

Finally, it would appear that State efforts to prevent the proliferation of tools and technologies used by cyber criminals or to apprehend and prosecute them, have not been very effective to date. There is widespread recognition that the threat posed by cybercrime continues to grow[488] and this is reflected in rising costs for the private owners of digital infrastructure and their suppliers (as well as many other businesses). To the extent that owners of digital infrastructure have the resources and are

[483] A recent study was undertaken by the NIS Cooperation Group for the European Commission, concluding : 'Overall, the NIS Cooperation Group concludes that Open RAN will have a significant impact on a number of risks that were already identified in the EU Coordinated risk assessment of 5G networks published in October 2019. In addition, it identifies several new risks and vulnerabilities introduced by Open RAN. If not adequately mitigated, those risks could have a particularly strong negative impact on the security of large-scale 5G deployments using Open RAN', para 2.1, at https://ec.europa.eu/newsroom/dae/redirection/document/86603

[484] ORAN is simply one example of how trends such as virtualisation and open interfaces might affect resilience. It seems clear that such trends will introduce new risks but also new opportunities for addressing both existing and new risks in a more flexible manner (e.g. by using AI to detect and mitigate threats).

[485] In addition to the NIS Cooperation Group report cited above, the UK Government has also recently undertaken a detailed assessment of the security implications of digital network virtualisation, at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1057446/Draft_telecoms_security_code_of_practice__accessible_.pdf and the US President's National Security Telecommunications Advisory Committee produced a report on Software Defined Networks in August 2020, at https://www.cisa.gov/sites/default/files/publications/NSTAC%20SDN%20Report%20%288-12-20%29.pdf

[486] See: https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/ETSI-MEC-Public-Overview_Generic.pdf

[487] See, for example, the debate about Apple's iCloud private relay service which encrypts browsing and which some European operators say will mean that they are unable to comply with European laws that require the blocking of unlawful content or other measures, at: https://www.macrumors.com/2022/01/10/eu-mobile-operators-icloud-private-relay/

[488] See: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime

generally successful in sustaining the reliable operation of their infrastructure, it may be preferable for States to focus their own limited resources on addressing cyber threats that are more visible or that affect entities or individuals who are less capable of defending themselves. This means that the costs of ensuring reliable functioning of digital networks remain 'privatised' and internalised within the industry and are also likely to remain opaque and difficult to measure.

6. RECOMMENDATIONS

In this section we make a number of recommendations to policymakers. These follow from our assessment of the challenges in ensuring adequate resilience of digital infrastructure and the responses of policymakers and States in addressing some of those challenges to date.

6.1 Capacity Reserves and Switching

Policies to promote competition in the provision of digital infrastructure by the private sector over the past thirty years have resulted in extensive duplication and diversity of digital infrastructure at all levels of the network. If properly co-ordinated and planned, this could greatly contribute to resilience by allowing those who rely on digital infrastructure to avoid disruption by switching their demand from one network to another in the event of disruption. To date, however, we think policymakers have paid insufficient attention to ensuring either that switching at times of disruption is feasible, or that there is sufficient capacity within the system as a whole to allow such arrangements to be implemented in practice. To the extent that policymakers and regulators have focussed on switching, it has been to promote competition between network providers rather than to enable the rapid migration of large groups of users between networks under exceptional circumstances. Little, if any, consideration has been given to reserving capacity in digital infrastructure, with policymakers and regulators assuming that the market itself will determine a level of output that is sufficient to meet user demand. This is in stark contrast with the approach taken in other strategic infrastructure sectors, such as energy markets, where European and United State policymakers have long taken a close interest in ensuring there are sufficient reserves to avoid disruption in supply.

We do not consider it feasible to anticipate switching between local fixed or wireline access networks since this will invariably involve the installation of new equipment on or near the affected premises, the time required to implement this will likely exceed the period during which service is interrupted, and any disruption will be highly localised in any event. We do, however, consider that switching between national wireless networks, in the form of national or emergency roaming in the event of a disruption (as we noted earlier is currently being done by the wireless operators in Ukraine and was undertaken by AT&T and T-Mobile following Hurricane Sandy in the United States), should be given further and serious consideration by policymakers and planned for in advance.

We recognise, however, that there are a number of issues to be addressed before such arrangements could be implemented. These include defining the conditions under which the arrangements could be activated and when they would cease, ensuring that firms do not free ride on the network investments of others (meaning that obligations would almost certainly need to be reciprocal), determining how and whether spectrum would be reassigned by regulators and operators during the outage to provide additional network capacity on other networks, and defining how reserve capacity would be measured, how much would be required, what proportion of existing demand would need to be served and, importantly, who would pay to maintain it.

This will also require an assessment of the additional costs of maintaining reserves of capacity in markets where aggregate demand for capacity from the existing users of the network is expected to

continue to grow at around 25% p.a.[489] This means that wireless operators already pre-provision significant capacity in their networks and that reserves on any individual network will quickly be absorbed by the growth in the demand from their own users rather than remaining unutilized for long periods of time. However, it also means that additional capacity will then need to be provisioned in order to ensure that an adequate reserve is maintained. Introducing such mandatory capacity reservations into the system could also have implications for how competition works in the downstream market which would need to be considered and which may affect how the arrangements are designed and implemented. It is important to emphasise that we do not propose that switching arrangements would be implemented on a permanent basis, but that they would be activated only under certain clearly prescribed circumstances, likely at the direction of the public authorities.

Switching demand between core or national networks in the event of disruption is more straightforward and private operators already diversify their suppliers to ensure a degree of redundancy. However, competition between network providers means that they will have strong incentives to utilise surplus capacity and generate revenues from the assets instead of holding them in reserve as a contingency. We think there is a supervisory role for public authorities, likely in the form of the national regulatory authority, to ensure that network operators retain sufficient reserve capacity to provide resilience to the system in the event of the failure of any of the other participants in the system. Again, to the extent that the reservation of excess capacity imposes additional costs on private firms, policymakers will need to decide who will bear those costs (but we consider it likely to be customers rather than taxpayers in this context).[490] This will require that regulators or other authorities have the legal powers to direct firms to reserve capacity and that they have the information gathering powers to enable them to assess whether overall system requirements are being met.

The aim of this recommendation is to ensure that today's diversity in digital infrastructure, which has developed because policymakers have sought to promote competition between network providers, can also contribute effectively to improving the resilience of the system as a whole. This requires that users can switch demand between networks when they need to and that there is sufficient spare capacity in the networks to ensure that their services, and those of other users, are not degraded when switching on a large scale occurs. Achieving this requires that regulatory authorities have powers to direct operators to reserve capacity in their networks and to enable switching of users under exceptional conditions.

As with a number of our recommendations, implementing these proposals will require public authorities in Europe and the United State (but perhaps not in China) to take a much more active role in the co-ordination and oversight of the conduct of private firms that are operating in competitive markets than has been the case to date. It may also require States to provide financial compensation

[489] See: https://www.ericsson.com/en/reports-and-papers/mobility-report/dataforecasts/mobile-traffic-forecast

[490] States appear to have been reluctant to contribute to the costs of improving resilience to date. For example, the effect of States prohibiting the use of Chinese 5G wireless equipment has often been to force operators to decommission existing 4G Huawei equipment. So far as we know, private firms have been required to write off these investments without any compensation (although policymakers may argue that State investments in and support for Open RAN development goes some way towards offsetting these costs for the industry).

or other incentives to private firms in order for them to act in a way which ensures that the resilience of the system as a whole (as opposed to the assets of the individual firm) is maximised. Without more State direction, private firms will not have the incentive or ability to act in a way which contributes to system-wide resilience.

6.2 Co-Ordinating Network Deployment

Whilst capacity reserves and switching capability can contribute to resilience, we consider that policymakers should also pay greater attention to how the underlying assets which provide the capacity are sourced and deployed. As we explained earlier in the report, we think that too much emphasis has been given in recent years to (a) the country of origin of equipment, as illustrated by the various prohibitions on the use of equipment supplied by Chinese vendors (recognising that there may be other motivations behind such policies which we have not considered in this report), and (b) the physical location of assets in a way which fails to recognise that the virtualisation of networks means that control over assets is increasingly separated from their physical location. Instead, we recommend that greater attention is given by public authorities to oversee the way in which assets perform and how they are actually deployed by operators.

Any operators of digital infrastructure should assume that all equipment will potentially be vulnerable to threats or to accidental failure, irrespective of the country of origin or vendor (for example, they should take a vendor-agnostic approach when assessing risks). We noted earlier that the United Kingdom's Government has concluded that poor quality software is a greater risk to resilience, given the threats from both criminal and State actors in general, than any threat from 'back doors' that have been installed at the request of any individual State. We, therefore, consider that the best way to ensure resilience in equipment is for States to establish technical testing facilities, or to co-ordinate testing by operators, of any and all equipment that is to be deployed within the network. States could pool information and knowledge, either through standards bodies such as 3GPP[491] or through other fora. We note that the European Commission's 5G Toolbox does not envisage the Commission facilitating the sharing of the results of technical audits between Member States and that the 2020 report on implementation of the Toolbox by the NIS Cooperation Group suggests that progress by Member States in implementing auditing and assessment measures is in any event not very well advanced.[492] In our view, pre-approvals would be required for any digital infrastructure equipment deployed within the State (or in submarine cable systems) and not just equipment relating to 5G or any other particular technology standard.

Trusted suppliers and diversity in the supply chain will not contribute to resilience if the operators choose to buy and deploy the equipment in a way which produces a technological monoculture. In other words, if all operators in a country choose the same supplier and deploy the same equipment at the same locations then any benefits from diversity will be lost. To date, regulators and

[491] See: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_9-1/prism_9-1_115-129_Purdy-Yordanov-Kler.pdf?ver=-b6UQO4hfPEjis5OQlYdZA%3d%3d, p.123.
[492] See: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68510, p.13-17.

policymakers have paid little attention to how assets are actually being deployed by operators of digital infrastructure, or the implications of these decisions for the resilience of the system as a whole.

This means that there is a large legacy of digital infrastructure which may or may not ensure diversity, but which would be costly to replace or reconfigure in the short term (although we noted earlier that this has not stopped some States from requiring operators to remove existing Chinese 4G equipment from networks at considerable cost). Fortunately, continuous innovation means that digital network infrastructure is constantly being upgraded and so, going forward, we recommend that regulators are given legal powers to intervene and direct operators so as to block deployments of new equipment which would pool technical risk by creating monocultures.

To do this would require public authorities to have much greater visibility of the network investment plans and strategies of the operators concerned, including their intentions in relation to the use of cloud providers as well as local access network hardware. These information gathering and powers to direct operators would be in addition to the powers to require operators to sustain capacity reserves but would likely operate alongside them. The NIS Directive and similar measures in the United States, discussed earlier, may to some extent already facilitate this.

Again, we recognise that a number of important questions would first need to be addressed before this recommendation was adopted, including defining the circumstances that would trigger intervention and whether an operator against whom a direction is made would be compensated for any economic or competitive disadvantage which they might sustain by being prohibited from using the equipment which they think would otherwise best meet their commercial interests. If the supply chain for the equipment is itself concentrated, as is the case today, then directing operators to use an alternative supplier may significantly reduce the bargaining power of all operators in the market. It may therefore also be necessary for regulators to give such directions and to have powers to intervene if the prices or other terms of the agreement with the alternative supplier diverge significantly from those that were available on a commercial basis. Future developments in technologies such as Open RAN may increase competition in at least some parts of the infrastructure supply chain, which would mitigate this concern.

The aim of this recommendation is to ensure that private operators only deploy equipment in their networks that has been assessed as being secure and resilient, regardless of country of origin, and that the equipment is deployed by operators in a way which contributes to the diversity of the system as a whole. This requires that regulators be able to direct operators not to deploy certain equipment at certain locations if this would undermine resilience, even if it was otherwise in their best commercial interests to do so. Anticipating risks in this way is better, in our view, than having the State direct private firms to remove equipment which they have already deployed in their networks.

6.3 Market Structure

In addition to ensuring diversity through oversight of where and what equipment will be deployed by firms, policymakers and regulators will need to ensure diversity of supply and ownership in the

underlying infrastructure. To date, any assessment of mergers or network sharing arrangements between digital infrastructure providers has tended to be undertaken on competition grounds alone or by having regard to national security considerations arising from the identity of the acquiring party. It has generally not involved consideration of the implications of the proposed transaction for the resilience of the system as a whole.[493]

In addition, whilst regulators of digital infrastructure may already have objectives to ensure the security of individual networks on which users depend[494], they will not generally make decisions having regard to the overall resilience of the system. These regulatory authorities can have a significant influence over the diversity of the digital infrastructure through the application of policies to promote entry or which result in exit from particular parts of the market. For example, in Europe, national regulatory authorities have sometimes differed in their views as to whether duplication of local access networks is a feasible or desirable objective, or whether competition should be better promoted though the competitive resale of services which are provided over a single infrastructure. These decisions are likely to have significant and enduring consequences for resilience, even if this aspect is not considered by regulators when making them. We recommend, therefore, that the duties of regulators are updated to include a requirement that they are required to consider the implications for resilience of any measures they adopt, alongside the various other objectives which they are required to pursue.

We also recommend that merger policy in relation to digital infrastructure providers is adapted to ensure that the implications for resilience are properly taken into account in the assessment. We note that European competition policymakers now recognise that competition policy may need to take environmental and climate change objectives into account when undertaking merger assessments[495], and that the European Commission is currently revising its Horizontal Guidelines in order to give effect to this.[496] These Guidelines will also inform how sharing arrangements between owners of digital infrastructure will be assessed by competition authorities in future. United States' competition policymakers also argue that the objectives of competition policy need to be reassessed.[497] Resilience objectives give rise to many of the same issues (externalities and market failure problems, system wide performance, and so on) as environmental objectives. The inclusion of resilience objectives might either be done by adjusting the approach that is taken by competition authorities themselves, or by introducing an additional or parallel review of the merger by another body (such as the regulator that will assume the various other responsibilities for ensuring resilience which we proposed above) which would assess the effect of the merger from a resilience perspective.[498]

---

[493] For example, some of the current concerns about resilience in digital infrastructure arise in part because mergers between firms, particualrly the consolidation of the telecoms equipment supply market in the 1990s and 2000s, were approved by competition authorities.
[494] Article 3 of the European Electronic Communications Code requires regulators to 'promote the interests of citizens by …maintaining the security of networks and services'.
[495] See, for example: https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/competition-policy-support-green-deal_en
[496] See: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1371
[497] See: https://www.yalelawjournal.org/forum/the-ideological-roots-of-americas-market-power-problem
[498] As noted earlier, the US CFIUS process provides for a parallel review of a proposed merger on national security grounds by a separate body that is established specifically for this purpose.

We intend that the practical effect of these proposals will be that mergers or other network sharing arrangements which might otherwise be approved, could be prohibited (or approved with additional remedies to address resilience concerns) after having taken the impact for resilience into account and having weighed this against the other considerations which competition authorities are already required to have regard to. The same would apply in relation to mergers which might otherwise have been prohibited (and we make no assumptions as to what the overall effect of this recommendation on the merger process might be). Similarly, regulators may adjust their approach in order to prioritise diversity and resilience in digital infrastructure over other objectives, or prefer measures which preserve resilience over other measures which might otherwise achieve the same objective. In practice, this is likely to mean that duplication of wireless local access infrastructure will remain an important feature of the market for both competition and regulatory authorities.

6.4 Submarine Cables

In addition to the above recommendations, which would apply to most or all forms of digital infrastructure, we think submarine cable systems present particular challenges for which additional measures are recommended.

We have found in this report that today's submarine cable systems offer a significant degree of resilience in terms of diverse routing and surplus capacity which can quickly be brought online, but that a number of bottlenecks remain in the global system and States may have single points of failure at cable landing stations. Changes to the legacy infrastructure are likely to be very costly. Concerns about foreign ownership of submarine cables on which other States depend have been addressed in a rather ad hoc and uncoordinated manner to date. Governance and oversight of submarine cables in extraterritorial waters is inherently challenging from both a legal and logistical point of view.

Thus, we do not think it is feasible or necessary for policymakers to pursue measures that would be intended to ensure the resilience of the entire global submarine cable system given both the costs of doing so and the difficulty in undertaking multi-lateral action (such as might be required to modernise the UN Convention on the Law of the Sea). Instead, we suggest policymakers focus on those assets which are most vulnerable and the disruption of which would have the greatest adverse consequences. As an initial step, we propose that the European Commission, the United States, Chinese and other authorities should undertake a comprehensive assessment of the global submarine cable system in order to identify the points of greatest vulnerability and identify measures that might be taken, over time, to improve resilience. Vulnerability in this context could arise from the physical location or co-location of the cable, but also from the identity of the owner or owners of the assets. Consideration would need to be given to the availability of alternative routes, but also to the availability of spare capacity on those routes, both today and in the future, and the ease and speed at which demand could be switched from one cable to another, something which may depend upon the capacity in the national networks as well as in the submarine cables.

We would exclude the possibility of re-routing existing cables but recommend that any applications for new cable systems should be assessed for their contribution to the overall resilience of the global

system. If necessary, State assistance (perhaps from groups of States acting together) may be required to ensure that appropriate investments are made. At a national level, we assume that the introduction of digital infrastructure audits, as discussed earlier in the report and which are now being undertaken in Europe and the United States, will include consideration of submarine cable landing stations.

Secondly, we recommend that States consider taking further and more effective unilateral actions to protect submarine cables within national waters from damage by fishing and other vessels. The actions taken by Australia, referred to earlier in this report, to implement exclusion zones for fishing and other vessels in coastal waters, is one example to follow - the enforcement of which may be assisted by the detection measures we propose. In this regard, we recommend that owners of submarine cables should, in the future, be required to make greater investments in detection systems which are available or are being developed, to enable them to detect interference or disruption in the cables and to locate specific points of interference or disruption, as well as to potentially identify the source or perpetrator. Some studies on the effectiveness of different detection technologies already exist[499] and some systems are already being deployed, but more research is likely to be required and should be sponsored by the European Commission, the United States and other authorities. The obligations to deploy detection technologies should depend on whether the cable is deemed to be important to sytem-wide resilience, based on the assessment we proposed above. Obligations might be imposed under the existing national licensing arrangements for landing cables which are operated by many States, or by means of a new legal framework. Fees levied on, or penalties imposed on, submarine cable providers might also be modified to reflect the resilience and performance of the cable in question to the extent that they do not already do so.

These measures are intended to ensure that incremental improvements in the resilience of the global submarine cable infrastructure will be made as new cables are deployed in the future, whilst the resilience of existing cable systems will be improved by augmenting them with new detection systems to deter threats and enable faster restoration of service when faults do occur.

6.5 Anticipating Future Technological Developments

An important theme to emerge from this report is that, to date, policymakers in Europe and the United States have tended to approach questions of security and resilience in digital infrastructure in a reactive manner. This means that their focus has often been on those aspects of the issues which have greatest political saliency, rather than necessarily being the most effective or important. Foreign ownership or country of origin restrictions is a case in point. Other aspects that are (literally) less visible, such as submarine cables, have been neglected. Decisions have been made and policies pursued, such as promoting entry by new wireless operators in Europe in the 2000s, allowing the consolidation of the major telecoms equipment suppliers or the promotion of Open RAN technologies, which can have unintended consequences for security and resilience later on. Correcting for these

[499] See: https://www.mdpi.com/1424-8220/20/3/737/pdf?version=1581329530

mistakes can then be very difficult and costly after the infrastructure has already been deployed at scale by the private sector.

Our final recommendation is therefore that policymakers adopt a more forward-thinking approach to resiliency in digital infrastructure. This involves anticipating developments in the industry before they are carried out in the deployment of equipment or software in the field. The standardisation process will provide an insight into likely technology trends and States should engage more strategically with that process than they have in the past (although it is still not clear to us at this stage exactly how that is to be done). In the meantime, the trend towards the virtualisation and cloudification of networks is well advanced and developments in edge computing are ongoing, but the implications for security and resilience are only now beginning to be given proper consideration by policymakers and their technical advisers. The rate of technological change is unlikely to slow in the future. This report suggests that policymakers in Europe and the United States have been catching up in recent years, but we think they now need to get ahead of the curve.

cerre Centre on Regulation in Europe

GLOBAL GOVERNANCE FOR THE DIGITAL ECOSYSTEMS

BUILDING THE BENEFITS OF DIGITAL TRADE

PATRICK LOW

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The academic workstream lead for this paper, Dr Patrick Low, would like to thank Chad Bown, Craig Burchell, Richard Feasey, Carl Gahnberg, Henry Gau, Jan Kramer, Pascal Lamy, Soledad Leal, Bruno Liebhaberg, Hamid Mamdouh, Zainab Mchumo, and Alexandre de Streel for their comments and suggestions on earlier drafts of this paper. The author remains exclusively responsible for the views expressed therein.

1. INTRODUCTION

The growing dominance of the digital economy promises substantial economic and socio-political gains. Tens of millions of digital transactions occur daily among producers, consumers and governments engaged in a vast variety of commercial and non-commercial activities. Digital transactions within and across borders offer new opportunities, not least to small businesses that can reach new customers on distant shores. However, challenges of access remain, with approximately one-third of the world's population lacking access to the internet.[500] Digital transactions also have direct economic efficiency gains that can contribute to increased growth stimulated by lower product prices and transaction costs, along with enhanced productivity. Seamless interconnectivity buttressed by internationally compatible national regulatory frameworks can greatly increase the potential gains from digital exchange. It is thus in the interests of governments, especially those with the market power to influence the regulatory environment, to co-operate in the name of mutual gains.

The volume of domestic and international data flows underlying digitally driven exchanges climbs sharply year after year, and the growing technology-enabled complexity of exchange through digital means continues to boost the scale and scope of electronic interaction. A World Bank estimate of the size of the digital economy puts the latter at 15.5 per cent of global GDP in 2021. This share has been growing two-and-a-half times faster than GDP, on average over the previous 15 years.[501] COVID-19 gave a significant fillip to the digital economy in general, including digital trade. No precise global estimates exist of the quantitative dimensions of global digital trade, which reflects the considerable statistical challenges of capturing the detail of changes in international exchange underlying the medium. According to UNCTAD, in 2018 Business to Business (B2B) digital transactions far exceeded those that were Business to Consumer (B2C). The former are estimated to account for some 83 per cent of e-commerce sales, and the latter for 17 per cent.[502] These estimates do not count government transactions separately.

1.1 Defining Digital Trade

Digitally enabled international trade is growing at a dizzying pace, penetrating the life experiences and opportunities of an ever-larger proportion of the world's population, both as producers and consumers. Despite this, no consensus definition has been developed for digital trade - one definition is as follows: cross-border transactions made possible by digital technologies.[503] Such transactions are enabled fully or in part by electronic data flows that transmit goods and services across frontiers from origin to destination.

[500] A widely used set of statistics relating to the digital economy can be found at: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
[501] See the World Bank website (2022) https://www.worldbank.org/en/topic/digitaldevelopment/overview
[502] UNCTAD (2018) UNCTAD Estimates of Global E-Commerce 2018. https://unctad.org/system/files/official-document/tn_unctad_ict4d15_en.pdf
[503] For a discussion of definitional issues, see UNCTSD (2021) Digital Economy Report. https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf

A complicating factor with this definition is that trade agreements (both multilateral and preferential) define services as transactions involving both product markets and factor markets. In the latter case, cross-border foreign investment and cross-border movement of services suppliers effectively extend the definition of trade to behind-the-border transactions,[504] thus not all digital trade is cross-border. This extends the definition to transactions encompassing the entire value chain from production to delivery. To render these definitions more manageable and consistent, Chapter 84 of the United Nations Central Product Classification (CPC) Version 2.1 defines these products as "digital content services". This conforms to the notion that all digital trade comprises trade in services, but does not, of course, extend to physical infrastructure that enables the digital economy to operate.

In the trade of goods case, final delivery may take a physical form. This aspect of transactions is not considered part of digital trade, although elements of the supply and demand sides of such transactions are digital. Thus, an electronic purchase via an online platform of a product could culminate in delivery in a physical form, which could be the case, for example, of a book. Alternatively, the electronic purchase of a book could also lead to the digital delivery of an e-book.[505] Fundamentally, however, the digital economy resides in the realm of services as inputs, outputs and in consumption. Data flows are both a carrier medium and a conveyor of underlying content. Data flows themselves can be a source of value going beyond a delivery function where, for example, large datasets accumulate information on consumer behaviour and preferences. Such information possesses a commercial value. From a policy perspective the distinction between data as a carrier medium and data as a conveyor of content is important. Policies may sometimes be seen as acting solely on data flows, although this may be with the intention of distinguishing among flows in terms of content.

At the level of data as a carrier medium, a lesser level of commitment to low-cost, facilitated delivery, and interoperable efficiency may be intentionally protectionist in character. At other times, restrictions on data flows are manifestly linked to content and driven by specific regulatory requirements, and there is no basis for a presumption that outcomes are protectionist rather than expressions of legitimate public policy. In practice, agreements can be designed to minimise opportunities for using a legitimate public policy rationale as a vehicle for hidden protectionist intent. No digital trade agreement exists without provisions designed to guard against such 'dual-use' policy strategies.

Some policies, nevertheless, are directed at the facilitation of data flows and not specifically at content. This distinction is analogous to the difference, for example, between the WTO's Agreement on Trade Facilitation, and the Agreement on Textiles and Clothing. A commitment on interoperable infrastructure for digital trade is more analogous to the former, and a commitment on regulatory prerequisites for lawyers to transact in a given market to the latter. Ultimately, the most important

[504] As discussed more fully in Section II.
[505] The OECD distinguishes between digitally ordered trade and digitally delivered trade in order to capture this distinction. The definition encompasses computer-based transactions, excluding transactions effected through phone, fax or manually typed email. See OECD, WTO, and IMF (2020) Handbook on Measuring Digital Trade. p.11. https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf

determinant of the terms under which data can flow between jurisdictions is content-driven and determined by regulation and conditions of market access.

Digital trade encompasses a wide range of activities, including the provision of online services, the sale of products on the internet, and data flows underlying a myriad of applications and platforms. Digital trade relies on the physical and virtual infrastructure that sustains interconnectivity and is enabled by the degree of ease with which data can flow among distinct jurisdictions. The role of governments in determining these outcomes is fundamental.

In some discussions, 'e-commerce' and 'digital trade' are used interchangeably to refer to electronic transactions via the internet, but no generally accepted definitional distinction has been established. E-commerce is a term developed in the early years of digitalisation referring to the sale and purchase of goods and services via electronic means. The term electronic commerce (e-commerce) was introduced at a time when the use of analogue technology was dominant. The growing adoption of digital technology to replace mechanical and analogue technologies brought the terms digital economy and digital trade into more common usage. Moreover, the enriched data environment accompanying digital technology has led to more expansive definitions of the medium. One definition of digital commerce or digital trade, for example, is the "purchase [of] goods and services through an interactive and self-service experience [that] includes the people, processes, and technologies to execute the offering of development content, analytics, promotion, pricing, customer acquisition and retention, and customer experience at all touchpoints throughout the customer buying journey."[506]

1.2 The Role of Government Policy, Regulation and Market Access

Interoperability, adequate transborder access, and streamlined regulation across multiple dimensions of the digital universe are essential for digital exchange to fulfil its promise. If full advantage is to be taken of the many opportunities offered by this medium, efforts are required to avoid a friction-laden patchwork of localised arrangements supported by heterogeneous regulations espousing incompatible objectives. This is not a description of today's international digital landscape, where considerable scope exists among governments for mutually beneficial co-operation based on shared interests and broadly comparable approaches to policy and regulations. The closer governments are in these respects, the greater the opportunities for convergence towards a seamless global digital ecosystem. Where convergence is unattainable the challenge is to manage divergences in ways that sustain a coherent and co-operative framework of rules and commitments that maximise the gains from global digital trade.

Issues where differences typically arise in matters of digital trade governance include privacy, domestic data storage requirements, cyber security, and prudential measures in the financial sector. These and other aspects of the regulatory policy choices preferred by different governments are

[506] This definition is attributable to Gideon Gartner. See Neil Rowett, (2021): https://www.columbusglobal.com/en-gb/blog/why-digital-commerce-is-about-more-than-just-e-commerce

referred to further in due course. Another key element of differing policy friction concerns the taxation of the digital economy.

Linked to the issue of differing regulatory approaches to digital trade, is a concern about how far a country's regulatory preferences reflect genuine public policy imperatives, and how far they double as protectionist measures designed to favour national interests and frustrate foreign competition. These matters relate both to the design of regulations and their administration.

A digital trade agreement is more complete if it contains both regulatory norms and market access. The latter is not always present in preferential digital trade agreements, in part because these are often folded into broader trade agreements that cover market access in other provisions. The absence of market access commitments leaves no room for expanding the coverage of a broader range of digital activities with tailor-made regulatory structures for digital trade.

1.3 Organisation of the Paper

The GGDE project has divided the analysis of the digital economy into workstreams on infrastructure resilience, online platforms, data, and digital trade. These are interconnected elements of the digital ecosystem and must ultimately be melded into a joined-up narrative. What follows is a discussion of the trade aspects of the digital economy. While some elements of policy are specific to international exchange, trade is affected to a degree by all aspects of national policy frameworks.

Section 2 of the paper seeks to single out elements of policy affecting digital trade that are particularly relevant to the multilateral trading system under the World Trade Organization (WTO). Section 3 briefly examines some of the distinguishing features of digital policies pursued in China, the EU, and the United States. This provides part of the background to a consideration of prospects for an international agreement on digital trade and the shape such an agreement might take. Section 4 examines some of the dozens of existing preferential trade agreements containing digital trade provisions. Contrasts and complementarities here help to reveal the scope for developing a multilateral framework to govern digital trade. Section 5 reviews progress so far in establishing a multilateral agreement on e-commerce under the auspices of the WTO, as well as some of the issues relevant specifically to a multilateral approach to digital trade relations. A key question here concerns the possible design, reach, and institutional context of an international digital trade agreement. Section 6 contains conclusions. Lastly, this is followed by a brief summary of recommendations.

2. KEY POLICY ISSUES SPECIFIC TO DIGITAL TRADE TRANSACTIONS AND WTO RELEVANCE

Digitally driven exchange among jurisdictions raises a specific set of policy issues specific to trade. Some of these policies are, of course, also relevant in the national context. Digital trade outcomes are the result of interactions between supply and demand. But the terms on which supply and demand interact are influenced by a range of factors including prevailing conditions in the market, the conditions of competition, and the characteristics of different business models on the supply side. Both data flows and their content are affected by the policy environments shaped by governments. Conditions imposed on data flows typically reflect a range of public policy concerns such as national security, cybersecurity, privacy, and social preferences. Digital trade policies will also determine the desired blend of non-discriminatory policy treatment, sector-specific market access obligations, and regulations and standards affecting international transactions. Other elements include transactions that encompass a physical cross-border component and a range of inter-jurisdictional tax matters. This section takes up some of these issues, while at the same time reviewing aspects of the WTO Agreements in terms of their relevance to digital trade agreements.

2.1 Non-Discrimination

The policy of non-discrimination between foreign and local interests is generally a cornerstone – explicit or otherwise – of international trade agreements, applying to transactions among all members of an agreement. Such trade agreements could be multilateral under the WTO, or preferential, usually among a subset of members of the WTO.

2.1.1 Most-Favoured-Nation and National Treatment provisions in WTO agreements

Two overarching rules generally apply under preferential and multilateral agreements, often referred to as principles. They are the most-favoured-nation (MFN) treatment and national treatment (NT) principles. MFN requires that all foreign supplies or suppliers to a market must enjoy the same non-discriminatory treatment. Like any simple principle, MFN embodies exceptions. In GATT the two leading areas where exemptions have been made to MFN are in relation to preferential trade agreements (PTAs) and special and differential treatment (SDT) for developing countries. The MFN exemption for PTAs is of a permanent nature and sets out regime design requirements intended to minimise the discriminatory impact of preferential market access. The SDT exemption comprises two main parts. One is the right for developing countries to benefit from non-reciprocal, non-contractual tariff preference granted unilaterally by importing countries on a voluntary basis. These are unlikely to be permanent and beneficiaries have little say on their form or duration. By contrast, SDT relating to regulations is negotiated and intended to be transitory, leading eventually to convergence around common rules.

Except in the case of voluntary non-reciprocal tariff preferences granted by some parties to selected developing countries, it is unclear how SDT might be defined. While the GATT/WTO generally seeks to promote market opening, there is no such thing as free trade, even in the most open economies. This means that every WTO member maintains some restrictions in the form of import tariffs or

comparable measures. This suggests that in this domain no clear dividing line exists between WTO members in relation to SDT and there is no MFN exemption in play. Trade opening is an ongoing process, and free trade is at most a directional aspiration, not an objective. Perhaps the same applies to free data flows.

Turning to NT, this principle imposes a non-discrimination requirement upon an importing jurisdiction with respect to all measures affecting trade (such as standards, licensing, technical perquisites and so on) once access has been gained to a market on an MFN basis. In the case of trade in goods, which was the exclusive domain of the GATT agreement, the distinction between MFN and NT is clear. This is because products face potential barriers at the border such as import tariffs or quantitative restrictions as well as behind-the-border regulatory measures. MFN matters in the former case and NT in the latter.

2.1.2 MFN and NT in the realms of services trade

This neat analytical distinction has become outmoded, partly because of a growing tendency for policy to penetrate further behind the border, thus more readily raising internal MFN and NT issues. More importantly, however, it was the introduction of the General Agreement on Trade in Services (GATS) in 1995 that rendered the frontier-based distinction between MFN and NT much less relevant when it comes to the conditions of competition in a given market. This is particularly important for digital trade, since with few exceptions cross-border digital trade is all about intangibles, or in other words, services.[507] Unlike the GATT, the GATS covers services products as well as factors of production (capital and labour dedicated to the supply of services).

While MFN is a prior principle in both GATT and GATS, NT only has that status in GATT. NT is subject to negotiation at the sectoral and product level under GATS, with commitments reflected in product-specific schedules of specific commitments.[508] One important reason for this is that services are defined under GATS to include the flow of products and of factors of production (investment and labour). Under these circumstances it makes no sense to treat NT as an exclusively behind-the-border measure. In the schedules of specific commitments under GATS many WTO members have largely excluded a fully non-discriminatory approach to NT, especially when it comes to investment flows (commercial presence) and labour movement (the movement of natural persons). Many of the exemptions from non-discrimination relate to subsidies.

As far as MFN is concerned, the GATS treats this as a principle in the same way as the GATT. Unsurprisingly, the GATS has comparable provisions for MFN exemptions, albeit with different labelling, also relating to PTAs and development. In addition, the GATS has a provision that allows countries to take exemptions from MFN in specified product areas, which are supposed to be temporary and subject to review. In practice, the exemptions have largely taken on a life of their own.

[507] An exception to this is the case where digitally driven trade ends up with cross-border delivery for consumption through physical means. This is discussed below.
[508] Individual national schedules of commitments are made by members of the WTO to reflect what they have agreed to in terms of market access for services or goods.

2.2 Market Access and Regulatory Provisions under GATS Relevant to Digital Trade

If MFN and NT are written into a digital trade agreement, they can contribute to a more seamless regime among jurisdictions, but they do not guarantee the free flow of data. This is because of multiple barriers that may stand in the way of free flow. These barriers can be about access to markets as well as regulatory conditions where access has been granted.

Such limitations are imposed to protect certain domestic activities via denial or restricted conditions of market access. It is here where GATS Articles XVI and XVII come in, as these control what is allowed to cross frontiers (Article XVI – Market Access) and the degree to which entry is permitted under non-discriminatory conditions (Article XVII – National Treatment). Article XVI limitations are essentially quantitative in nature, allowing restrictions on the number of service suppliers, the value of services supplied, the legal entities involved in services trade, and the share of permitted foreign ownership of a service supplier. As noted above, unlike the GATT, the GATS has jurisdiction in both product markets and factor markets. The measures listed under Article XVII discriminate against foreign supplies and suppliers that are in the market *vis à vis* their domestic counterparts. A common national treatment limitation, for example, is the denial of subsidies that a government may grant to its domestic services or service suppliers.

The GATS defines trade in services in terms of how they are delivered by mode of supply. The modes are cross-border service delivery (Mode 1); consumption occurring in the supplier's jurisdiction (Mode 2); trade based on foreign investment in services enterprises (Mode 3); and the movement of individual service suppliers (natural persons as opposed to juridical persons or firms) across frontiers (Mode 4). All product- and producer-related conditions attached to market access and NT are inscribed in the GATS schedules of specific commitments of each WTO member under the relevant mode of supply. The schedules also indicate when there are no restrictions under any (or all) of the modes of supply on the listed services sectors and subsectors. Where services are not listed in schedules of specific commitments, they are only subject to rules such as MFN and general transparency provisions that embrace all services activities.

While the GATS has provided a framework for enhanced market access at the product-specific level since its inception in 1995, its results have been disappointing. For most WTO members, schedules of specific commitments remain modest in coverage, both in terms of their sectoral scope and depth of openness. In fact, very little has been done by way of expanding coverage since the initial commitments were made when the GATS first entered into force. Moreover, many of the current commitments do not reflect the *de facto* degree of openness, which limits the degree to which the GATS provides market certainty built on justiciable commitments.[509] There exists, nevertheless, the opportunity to use the GATS framework for market opening under a comprehensive digital trade agreement.

[509] A number of reasons explain why more has not been done, but an analysis of this is outside the scope of this paper.

In contrast to the conditions of market access specified under GATS Articles XVI and XVII, Article VI focuses on regulations that relate to various aspects of public policy. These regulations are supposed to be entirely non-discriminatory in both a *de jure* and *de facto* sense as between domestic and foreign services and service suppliers. They should also be as least trade restrictive as possible in attaining their objectives. Tension can exist between maintaining legitimate, non-discriminatory regulations designed to serve various public policy objectives, and allowing their design or application to afford an additional degree of protection to domestic services and service suppliers. In short, public policy and other interventions should not be dual-purpose.

2.3 What Service Sectors Matter Most for Digital Trade?

Not all services sectors covered by the GATS are equally relevant to digital trade. Some producer services such as telecommunications services are crucial conveyors of digital content. Financial services are a core component of digital content. Taking telecommunications first, there is a GATS Annex on Telecommunications, a contribution of which is to ensure that foreign service suppliers are guaranteed "access to and use of public telecommunications networks and services on reasonable and non-discriminatory terms and conditions for the supply of a service included in its schedule".[510] Notwithstanding the limitation that this access right only applies to services where specific scheduled commitments are made, the Annex provides a useful element for managing one element essential to digital trade – interconnectivity.[511]

A further development in the GATS telecommunications negotiations that took place shortly after the GATS had come into existence in 1995, was the development of a Reference Paper on Telecommunications. The Reference Paper embodies six regulatory principles involving the following policy areas: competitive safeguards, interconnection, universal service, licensing, allocation of scarce resources, and the existence of an independent regulator. The Reference Paper is a template that was adopted by a subset of the WTO membership, and it contains certain variations in the case of some members who have subscribed to it. The Reference Paper is inscribed under a third Article appearing in members' schedules of specific commitments, Article XVIII (entitled Specific Commitments). Article XVIII has been used for other sectors besides telecommunications and is a place where regulatory commitments that help to define conditions of market access falling outside the purview of Articles XVI and XVII, can be inscribed.

Despite the partial subscription to the Reference Paper among members, the underlying commitments are nevertheless applied on an MFN basis. Countries that have acceded more recently to the WTO have all been required to include the Telecommunications Reference Paper in their schedules of specific commitments. However, the Reference Paper was crafted over 25 years ago, and technology has moved on considerably since then. While a template of this nature could prove useful in a digital trade agreement it would likely need updating. Indeed, this is precisely what the European

[510] Paragraph 5(a) of the Annex on Telecommunications.
[511] Another essential element for digital trade relates to product and process standards that underwrite interoperability. Standards are discussed in a separate section below.

Union suggested in a communication submitted in 2018 to the WTO e-commerce negotiating process.[512]

Turning to financial services, another explicit commitment relevant to data flows is to be found in the Understanding on Commitments in Financial Services. This requires WTO members who have followed the Understanding in scheduling their specific commitments to refrain from taking any measures that frustrate the transfer of financial data by electronic means. Such a commitment could obviously be subject to any limitation required to meet public policy objectives such as privacy or confidentiality. Once again, a provision of this nature, duly adjusted, could prove relevant to a digital trade agreement. Several other services sectors are also relevant to digital trade. Division 83 of the UN's Central Product Classification Version 2.1,[513] for example, encompasses a range of sectors and subsectors under the broad rubric of professional, technical, and business services. No fewer than 79 five-digit subsectors are classified separately under Division 83. Similarly, Division 84 includes 38 five-digit categories covering telecommunications, broadcasting, and information supply services. The main point to be made here is that governments can and do sometimes go beyond essential least-trade restrictive regulation by way of intervention. Resort to discriminatory market-access-restricting conditions on foreign supplies and suppliers reduce the benefits offered by digital trade. The case made here, therefore, is that market access negotiations would be a useful accompaniment to the development of digital trade regimes.

2.4 Domestic Regulation Disciplines for Services

A further area where some WTO members have acted recently is in the field of domestic regulation. When the GATS entered into force in 1995, several mandates for continuing action through negotiations were included in the text. One of these was on domestic regulations, namely qualification requirements and procedures, technical standards, and licensing requirements.[514] The negotiations were to ensure that regulations were based on objective and transparent criteria and were not more burdensome than necessary to ensure the quality of services. Additionally, in the case of licensing requirements, these should not become restrictions in and of themselves. There is also a provision requiring that international standards of relevant organisations are considered. Provisions like these are relevant to many contemporary digital trade agreements.

Discussions aimed at completing these domestic regulation provisions did not go anywhere for many years, until a subset of WTO members decided to launch a negotiation among themselves at the WTO's 11th Ministerial Conference in 2017. In December 2021, 67 WTO members accounting for over 90 per cent of world trade reached an agreement. Like the Annex on Telecommunications, the Joint Initiative on Services Domestic Regulation took the form of a Reference Paper to be inscribed in

[512] European Union (2018) Exploratory Work Towards a Revision of WTO Rules in the Field of Telecommunications Services. JOB/GC/194, 20 July 2018.
[513] United Nations. Central Product Classification (CPC) Version 2.1. ST/ESA/STAT/SER.M/77/Ver.2.1 Department of Economic and Social Affairs Statistics Division Statistical Papers Series M No. 77, Ver. 2.1 https://unstats.un.org/unsd/classifications/unsdclassifications/cpcv21.pdf
[514] GATS Article VI:4 and Article VI:5.

members' schedules of specific commitments. The 12-page document fills out, in considerable detail, how the relevant regulations are to be designed and administered. As with the Telecommunications Reference Paper, obligations are extended on an MFN basis to the entire WTO membership. The 2017 Joint Initiatives are discussed further in Section 5.

2.5 The Relevance of GATT/WTO Provisions on Standards Covering Goods

As with services, a key element of trade regimes dealing with goods addresses various aspects of both the formulation and administration of standards. In considering the provisions on these matters that an international agreement on digital trade might embrace, it is useful to summarise briefly the provisions of existing WTO agreements in this field. In the case of goods, the relevant agreements are the Agreement on Technical Barriers to Trade (TBT) and the Agreement on the Application of Sanitary and Phytosanitary Measures (SPS). The TBT Agreement covers such matters as regulations on packaging, marking, and labelling, as well as requirements relating to particular products and processes. The agreement distinguishes between technical regulations, which are mandatory, and voluntary standards. There is a presumption of desirability, but not a requirement, for governments to adhere to international standards where they exist. In the case of voluntary standards (as opposed to technical regulations), governments must adhere to a Code of Good Practice for the Preparation, Adoption and Application of Standards. This Code forms part of the TBT Agreement.

The core requirements underlying both the TBT and SPS Agreements are that standards, associated application provisions, and conformity assessment procedures are not a disguised restriction on international trade nor an instrument of arbitrary or unjustifiable discrimination. The non-discrimination obligation applies between both the country concerned and its foreign suppliers, and among its trading partners. The SPS Agreement is arguably somewhat less relevant to digital trade as it is concerned specifically with measures necessary for the protection of human, animal and plant life or health. The SPS Agreement, however, is a later WTO agreement[515] and adopts a more stringent approach to the applicability of existing international standards. It therefore requires that, as far as possible, members must base measures on international standards, guidelines, and recommendations where these exist. Specific mention is made of the Codex Alimentarius, the International Office of Epizootics, and the International Plant Protection Convention. Members are required to participate as actively as possible in relevant international organisations and their subsidiary bodies. The Agreement does state, however, that an exception may be made if governments wish to aspire to higher standards than those required by other international standards bodies.

2.6 Low-Value Digital Trade Involving Physical Delivery

Low-value digitally enabled purchases of goods across frontiers result in physical delivery, often direct to the consumer in the importing country (B2C). In this case more traditional trade policy issues arise

[515] The TBT Agreement entered into force as a GATT agreement in 1979, while it SPS Agreement was introduced in 1995 at the time the WTO was establishes.

at the border, involving customs administrations and aspects of fiscal policy (parcel post, tax thresholds, and so on). As the volume of low-value e-commerce imports increases, challenges also arise for delivery companies which, at least in some jurisdictions, are subject to accountability aimed at ensuring competitive pricing arrangements.[516]

A solution applied by some customs authorities to the fiscal issue is to set a *de minimis* duty and tax value below which small packages are exempt from fiscal charges. The World Customs Organization has identified and sought to address some of the challenges posed by growing reliance on small parcel post facilitated by the digital economy.[517] Among the challenges arising are the revenue risk resulting from rapidly growing small-package low-value trade, risks from illicit trade, and increased administrative costs associated with the multiplication of small-package suppliers that are often unknown to customs authorities.

As long as these exemptions involve lower values of foregone revenue than the costs of collecting the tax, they make sense from an efficiency perspective. However, where a *de minimis* threshold is not triggered, collection systems for low-value shipments can prove particularly burdensome for small enterprises, especially if brokerage fees are incurred on top of the taxes. Moreover, for those governments that are heavily reliant on indirect taxes (including trade taxes) for state budgets, the challenges associated with collecting charges due on small consignments are aggravated by the growing opportunities for cross-border digital trade.

One set of proposals for alternative approaches to managing the importation of low-value shipments has been put forward by the Global Express Association (GEA).[518] The basic idea behind the proposal is that a low-value shipment band would be established where duties and other indirect taxes apply, but the taxes would not be collected at the border. Customs administrations would focus exclusively on public policy diligence relating to such matters as health, safety, security and guarding against importation of prohibited goods. This would be achieved by making vendors in exporting jurisdictions responsible for collecting import duties and other taxes for periodic payment to the tax authorities of the importing jurisdiction. The simplified tax structure could amount to a uniform rate or a series of product bands with their own uniform rates.

A clear distinction would be required between import duties and value-added or sales taxes since the latter are NT-consistent taxes under which a uniform rate applies to imports and domestic production of like products. The GEA proposal recognises that, whatever arrangements are made to lower transaction costs on small package imports, it is essential that they ensure non-discriminatory treatment between imports and domestic products when it comes to excises or taxes such as a sales or a value-added tax. It seems that Australia, Canada, and New Zealand have adopted various elements of this proposal. Doubtless, there are other possibilities for simplification, cost-saving and

[516] In the case of the EU, see: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_5203
[517] World Customs Organization, see: http://www.wcoomd.org/es-es/topics/facilitation/activities-and-programmes/ecommerce.aspx
[518] Global Express Association (2021) Proposal on Tax/Duty Collection on Imported Low Value Shipments. https://global-express.org/

the nurturing of trading opportunities offered by the digital economy, particularly in the interests of smaller enterprises.

2.7 The Relevance of Market Access in Goods to Digital Trade

The evolution, over time, of the multilateral trading rules under GATT, and later the WTO, has resulted in a degree of bifurcation between goods and services in the design of rules. This does not always adequately reflect the joined-up nature of trade in goods and services, where products are typically a bundle of both. As discussed below, the WTO's current efforts to negotiate an agreement on e-commerce (digital trade) seek to rectify this in the digital domain, recognising that the prices, quality, and availability of a range of goods are key to a streamlined and efficient digital economy.

An important WTO initiative that addresses this matter is the Information and Technology Agreement, the first iteration of which (ITA I) entered into force in 1997. The covered product list was expanded in 2015 (ITA II). Over 80 WTO members are signatories to the Agreement, covering around 97 per cent of trade in the relevant products. Covered products include computers, telecommunication equipment, semiconductors, semiconductor manufacturing and testing equipment, software, scientific instruments, GPS navigation equipment, and medical equipment. The objective of the Agreement is to reduce all tariffs on covered products[519] to zero, and each signatory to the ITA maintains a schedule of tariff commitments reflecting their assumed obligations.[520]

2.8 The Taxation of Digital Trade

In general, import duties are not imposed on services, which explains why, unlike the GATT, the GATS is largely silent on fiscal matters. In the case of GATT, import duties and individual members' commitments on their incidence are central to the agreement. The main references to taxation in GATS fall under two paragraphs of the general exceptions provisions of the Agreement (Article XIV). Article XIV(d) allows a departure from NT (Article XVII) which permits members to ensure the equitable or effective imposition or collection of direct taxes on services or service suppliers of other members, while Article XIV(e) allows departures from MFN (Article II) to avoid double taxation that might arise as a result of the tax policies of another member.

The absence of a basis for addressing digital taxation under GATS, which would also likely be the case in a WTO agreement on e-commerce, makes the Organization of Economic Cooperation and Development (OECD) the primary forum for overseeing the discussions and negotiations on this subject. The need for co-operative action among governments to address digital taxation became apparent as an increasing number of countries embraced unilateral approaches towards digital services taxes (DSTs) and similar instruments. Not only were such unilateral approaches designed in ways likely to fall afoul of the WTO's non-discrimination rule, but they were becoming a troubling

[519] Estimated at some US$1.7 trillion in 2016.
[520] For greater detail, see World Trade Organization (2017) 20 Years of the Information Technology Agreement: Boosting trade, innovation and digital connectivity. https://www.wto.org/english/res_e/publications_e/ita20years2017_e.htm

source of trade friction among several countries.[521] A particular, *de facto* discrimination issue arose from unilaterally determined thresholds for in-scope coverage that relied on criteria such as firm size, product composition, and means of product delivery. Another problem resulting from the patchwork of unilateral DSTs was the occurrence of double taxation in some instances.

In 2016, the OECD began working on the OECD/G20 Inclusive Framework on Base Erosion and Profit Sharing (IF), and the current working text was presented in 2019. According to the OECD, some USD $ 240 billion is lost annually as a result of the tax avoidance strategies of multinational enterprises. Some 141 countries and jurisdictions have participated in discussions, and 96 have signed the Multilateral Instrument on Base Erosion and Profit Sharing (BEPS).[522] The initiative addresses both the base for tax collection on certain digital trade transactions and minimum threshold rates for profits taxes. In this sense, this is not only about fiscal challenges arising from digital trade, but also about corporations parking profits in low-tax jurisdictions.

Thus, the Inclusive Framework is a complex and novel structure, representing a far-reaching change in terms of international tax competition. Its underlying objective is to secure a redistribution of the tax take among jurisdictions to better match tax receipts where profits are made. One of the earliest unilateral initiatives to achieve this was the European Union's design of a DST under its Fair Taxation of the Digital Economy package.[523] The European Commission sought to tax value created by consumers of digital assets in the European Union market produced by enterprises that were located in other jurisdictions. The tax was aimed at the suppliers, not the consumers. In other words, the idea was to tax a digital presence in the absence of a corporate presence.

These efforts reflected the reality that the European Union is not home to the major digital platforms. The tax rate was set at 3 percent on gross revenues, and enterprises covered by the tax would have an annual turnover exceeding € 750 million globally and € 50 million in the European Union. Not least because of this proposed design of the arrangement, it was seen as directed against the large United States platforms, sometimes referred to in the discussions as GAFA (Google (Alphabet), Amazon, Facebook (META), and Apple).

The European Commission's proposed package effectively created a new taxation nexus between corporate profits and revenue. The European Union did not implement the package because consensus was lacking among the Member States to do so. France, however, designed its own scheme based largely on the European Commission's proposal. The implementation of the French scheme was postponed several times, being conditional upon progress in the OECD's work, and when France imposed the tax in 2019 it provoked trade retaliation from the United States – a foretaste of what a world without agreement on the issue might look like. A significant number of other countries also

[521] Low, P. (2020) Digital Services Taxes, Trade and Development. Jean Monnet Network TIISA Working Paper No. 2020-12. https://tiisa.org/working-papers/
[522] OECD (2021) What is BEPS? https://www.oecd.org/tax/beps/about/
[523] European Commission (2018) The Fair Taxation of the Digital Economy. https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en

began to implement DSTs and similar initiatives. The instability, inefficiency, and conflict that these unilateral initiatives threatened to reign upon the global digital economy provided impetus for the OECD's work.

The OECD/G20 Inclusive Framework initiative comprises a two-pillar solution.[524] Pillar 1 retains the new tax nexus whereby corporate taxes are assessed on revenue instead of on profits. This feature is key to permitting the tax burden on enterprises to shift to where they sell rather than where they locate their corporate headquarters or seek to stash profits in low-tax jurisdictions. Under Pillar 1 companies falling within the scope of the tax have a global turnover above 20 billion Euro and profits before tax of over 10 per cent. Complicated rules around the calculation of the so-called Amount A and Amount B can affect these thresholds as well as the amount of tax paid and to whom.

Pillar 2 is also complicated in design, but its core objective is to impose a minimum corporation tax of 15 per cent payable in all jurisdictions. These arrangements are designed to address the invoicing practices of multinational companies that shift taxable profits to low-tax jurisdictions. These rules are to apply to companies earning more than 750 million Euros in revenues. Pillar 2 has considerable support from many quarters, although it is possible that wealthy low-tax havens may be tempted to offset the tax with compensatory subsidies.

The package is supposed to be fully agreed in all its complex detail and implemented by 2023. The key elements of the package are seemingly agreed in principle, but legislative approval processes may prove challenging for some governments. It is therefore premature to suggest that inter-jurisdictional digital taxation challenges have been fully addressed. It should be noted that the OECD Inclusive Framework carries implications beyond the digital economy, encompassing aspects of real economy taxation as well.

The Tax Foundation[525] has suggested that an indirect tax, such as a consumption or sales tax, might serve the purpose of redistributing tax takes among jurisdictions more effectively than the Inclusive Framework arrangements. The proposal suggests that a broad-based tax covering both goods and services, and collectible across frontiers as well as locally on a non-discriminatory basis, could also shift tax liabilities in the desired fashion. Similar questions would doubtless arise as to scope, as well as the possibility of multi-tiered rates and how these would be decided. One concern with a consumption-based indirect tax is that the consumers, and not the large digital platforms, would end up paying it. The outcome in terms of incidence would depend on the degree of tax shifting that occurs, which in this case is a function of the extent of market power enjoyed by the platforms. Whatever direction this debate takes in the future, the alternative to convergent international co-operation in this field would be expensive and disruptive.

[524] OECD (2021) Statement on a Two-Pillar Solution to Address the Tax Challenges Arising from the Digitalisation of the Economy. https://www.oecd.org/tax/beps/statement-on-a-two-pillar-solution-to-address-the-tax-challenges-arising-from-the-digitalisation-of-the-economy-october-2021.htm

[525] Bunn, D. Asen, E. Enache, C. (2020) Tax Foundation, Digital Taxation Around the World. https://taxfoundation.org/digital-tax/

2.9 Import Duties on Electronic Transmissions: The WTO Moratorium

The WTO began to think about the implications of e-commerce and the digital economy for international trade rules in the late 1990s.[526] A decision was taken by WTO members in the context of the 1998 Geneva Ministerial Declaration on global electronic commerce[527] "to continue their current practice of not imposing customs duties on electronic transmissions." A moratorium had been proposed by the United States earlier in the same year which was, in part, a response to the idea of introducing a bit tax to compensate for losses in VAT collected as a result of digital sales, which was floated by the European Commission in a White Paper. A core objection to a bit tax – as compared to alternatives – relates to its regressive nature and the fact that it would apply to an excessively wide range of digital activities that are generally not taxable, including, for instance, internet surfing and email.

The wording of the moratorium was carefully negotiated. The reference to customs duties rather than taxes was aimed at avoiding any suggestion that internal taxes were covered, and the moratorium was thus understood to refer to discriminatory taxes levied on electronic transactions of foreign origin. The reference to electronic transmissions reflected an effort to settle on "constructive" ambiguity as to whether the commitment related to the content of transmissions or to the medium of delivery.

The moratorium is not legally binding under the WTO nor permanent. It has been subject to periodic renewal by consensus over the years, normally at ministerial meetings. Given that the moratorium is not legally enforceable, an adjudicated dispute would be very unlikely to render an authoritative ruling absent further negotiation on its wording and meaning. The Work Programme on Electronic Commerce,[528] launched by the General Council in 1998, has not produced any definitive interpretation of the moratorium.

The deliberations that have taken place over the years under the auspices of the 1998 Electronic Commerce Work Programme have deepened the understanding of the implications of the digital economy for trade rules and trade relations. It has also sought a common understanding of relationships between e-commerce and GATS provisions, but it has not led to a negotiating process.[529] The absence of progress in this regard was an important motivation for the initiative taken at the 11th WTO Ministerial Meeting in 2017 to launch the Joint Statement on Electronic Commerce.[530]

As the digital economy has grown rapidly, spurred on by COVID-19 and new technologies, concern regarding the value of foregone import duties has increased. If the moratorium is interpreted as

[526] Bacchetta, M., Low, P., Mattoo, M., Schuknecht, L., Wagner, H., Wehrens, M. (1998) Electronic Commerce and the Role of the WTO. Special Studies 2. World Trade Organization.
[527] World Trade Organization. (1998) Electronic Commerce Declaration. WT/MIN(98)/DEC/2. https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm
[528] World Trade Organization (1998) Work Programme on Electronic Commerce. WT/L/274. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/WT/L/274.pdf&Open=True
[529] Rowett, N. (2021) https://www.columbusglobal.com/en-gb/blog/why-digital-commerce-is-about-more-than-just-e-commerce
[530] This WTO-based work programme on e-commerce is discussed further in Section V below.

applying to the content of electronic transmissions, the share of impacted tariff revenue will grow over time. Against this background, the continuation of the moratorium has been called into question by several WTO members, including India, Indonesia, and South Africa. In addition to the loss of fiscal revenue, the argument has also been advanced that the loss of import duty revenue on physical goods as these are substituted by digital delivery could disturb the negotiated balance of rights and obligations under the WTO.

Apart from the restraining influence of the moratorium, one reason why no WTO member has attempted to impose duties on content could be the considerable difficulty in ascertaining the taxable content of transmissions on a systematic basis. Internet service suppliers will not know the content of encrypted transmissions, much of the traffic on the internet would in any event need to be exempted, and leakage would likely be significant. A further consideration could be a potentially negative impact on investment in digital assets and on digital engagement more generally if a jurisdiction tries to tax electronic transmissions or their content.[531]

A number of empirical studies have been undertaken to assess the revenue risk arising from the digitalisation of products that can also be delivered in non-virtual form.[532] A review of this work by the OECD[533] in 2019 reports a huge variation in estimates of lost revenue, ranging from USD $ 280 million to USD $ 8.2 billion. These highly varied results reflect different underlying assumptions and methodologies. Part of the difficulty is the difference between estimating what has been digitised and what could be digitised. In any event, the OECD study reports from its own estimates the highest possible average tariff take would amount to 1.2% of total trade. This share may be higher today. From an economy-wide perspective, however, additional tax revenue is unlikely to come close to the cost and efficiency savings associated with digital delivery compared to its physical counterpart.

A recent note by Evenett and Fritz (2022)[534] challenges the calculations and conclusions of a South Centre (2022)[535] paper on tariff revenue losses accruing to developing countries as a result of the moratorium, which the South Centre estimated at USD $ 56 billion between 2017 and 2020. Among their criticisms, is the observation that five of the ten most affected countries are not WTO members and are therefore unconstrained by the moratorium. It seems that, nevertheless, they do not apply customs duties on electronic transmissions. This may in part reflect the technical difficulties of doing so, as alluded to above. In addition, the most affected developing countries apply actual tariff rates below their WTO-bound maximum rates, indicating that more revenue could be collected in the

[531] It may be noted that South Korea has an interconnection regime that allows ISPs to charge international (and domestic) online services for carrying the data. This has adverse technical consequences. See: https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-south-koreas-interconnection-rules/ A net neutrality provision in an international agreement would obviate the problem.
[532] See, for example, UNCTAD. 2017. Rising Product Digitalisation and Losing Trade Competitiveness. https://unctad.org/en/PublicationsLibrary/gdsecide2017d3_en.pdf See also WTO (2016) Fiscal Implications of the Customs Moratorium on Electronic Transmissions: The Case of Digitizable Goods. WT/GC/W/798.
[533] OECD (2019) Electronic transmissions in international trade – Shedding new light on the Moratorium Debate. Working Party of the Trade Committee. https://tad/tc/wp(2019)19/final
[534] Evenett, S. and Fritz, J. (2022) Correcting Misleading Empirical Evidence and Other Errors About the Moratorium on Customs Duties on Electronic Commerce. https://www.globaltradealert.org/reports/93
[535] South Centre. (2022) WTO Moratorium on Customs Duties on Electronic Transmissions: How much tariff revenue have developing countries lost? https://www.southcentre.int/research-paper-157-3-june-2022/

traditional manner on goods should the governments concerned place revenue concerns above other considerations.

The estimates in the literature of the actual/potential fiscal consequences of doing away with the moratorium are predicated not only on the assumption that electronic transmissions refer to product content rather than the medium of conveyance, but also that the contents of transmissions are goods and not services. The debate continues unabated as to whether the content of electronic transmissions comprises goods (where electronic and physical conveyance of products are substitutes) or services. If content is deemed to comprise goods, the limiting constraint on the degree of discrimination between physically and digitally delivered substitutes would be negotiated maximum GATT tariff levels (bindings).

Indeed, the moratorium was once again renewed by Ministers of WTO members at their recent Twelfth Ministerial Conference held in mid-June.[536] The renewal was until the next WTO Ministerial Meeting, expected by the end of 2023. If no Ministerial Meeting has been held by 31 March 2024, the moratorium will expire, barring an explicit consensus decision to the contrary. It is noteworthy that some proposals made in the context of the 2017 Joint Statement on Electronic Commerce called for a permanent legally binding commitment to replace the moratorium.

[536] World Trade Organization. (2022) WT/L/1143. 17 June.

3. DIFFERING APPROACHES TO THE DIGITAL ECONOMY AMONG THE THREE MAJOR PLAYERS

Some writers have referred to the United States, the European Union, and China as the three digital realms or kingdoms, highlighting the fact that these jurisdictions, through their dominance by size, are the pacesetters shaping the digital ecosystem.[537,538] On the face of it, emphases are quite different in the underlying perceptions of national interests and priorities. It is, however, a separate question as to how far these differences inhibit the scope for mutually beneficial co-operation in developing a global ecosystem that enables and facilitates digital trade.

While the focus of this paper, and the GGDE initiative more generally, is on the major economies and their influence on the evolving global digital ecosystem, it should be noted that other players such as APEC have also been active in developing initiatives in this domain. The *APEC Framework for Securing the Digital Economy,*[539] *for example, establishes non-binding* principles and recommendations. The grouping has also developed an APEC Internet and Digital Economy Roadmap,[540] which is a framework to guide areas and actions to facilitate technological and policy exchanges to promote growth through digitisation. From the business side, ABAC (the business advisory arm) has worked on policy-specific aspects of the digital economy.

3.1 A Summary of Contrasts and Prospective Complementarities

A highly summarised characterisation of digital economy priorities in each of the three major economies offers an indication of the differences that would need to be finessed in an encompassing digital trade agreement. Although on the surface the characterisations described in what follows may appear difficult to bridge in the quest for a seamless digital trade environment, in practice there is scope for convergence. The possibilities of realising policy convergence that promises shared benefits for all concerned are discussed in subsequent Sections of this paper.

The United States favours the free cross-border flow of data by electronic means and eschews any suggestion of data localisation requirements. In short, the United States emphasis privileges a business-friendly environment. This reflects in part the fact that the United States is home to many of the major digital platforms. On the consumer welfare side of the equation, the United States has also focused on privacy and competition policy.

The European Union, on the other hand, does not host many significant platforms and is more concerned with consumer interests in the world of digital exchange. The protection of privacy is

[537] Aaronson, Susan Ariel & Leblond, P. (2018) Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. Journal of International Economic Law. Oxford University Press, vol. 21(2), pages 245-272. https://academic.oup.com/jiel/article-abstract/21/2/245/4996295

[538] Gao, H. S. (2021) Data Sovereignty and Trade Agreements: Three Digital Kingdoms. https://ssrn.com/abstract=3940508

[539] APEC. 2019. Apec Framework for Securing the Digital Economy. https://www.apec.org/publications/2019/11/apec-framework-for-securing-the-digital-economy

[540] APEC. 2017. APEC Internet and Digital Economy Roadmap. http://mddb.apec.org/Documents/2017/SOM/CSOM/17_csom_006.pdf

prioritised, as witnessed by the development of the General Data Protection Regulation (GDPR). The European Union also tends to focus on facilitation issues to ensure the minimum of unnecessary cost-augmenting regulations. The EU has recently overhauled its domestic regulatory setup for the digital economy on an EU-wide basis. The rules are aimed at controlling the activities of platforms and are structured to apply proportionately to platforms according to their market share and degree of domination. The Digital Services Package consists of the Digital Services Act (DSA) and the Digital Markets Act (DMA). The DSA aims to protect the rights of users online, including through the control of illegal content while the DMA focuses more on market structure, competition, and contestability. So-called "gatekeeper" or core-service platforms with a certain market share are subject to a range of pro-competitive obligations. This new structure which is being put in place conforms to the European Union's concern with consumer interests and will influence its positioning in international negotiations on digital trade rules.

China hosts some of the biggest platforms in the world, but they are mostly oriented towards the domestic market. China's approach to digital trade, and the digital economy more generally, is more hesitant, with a focus on national security and the role of the state. When it comes to the question of how data are controlled and used, an argument can be made that there is no difference between a commercial platform and a state authority. The difference in practice, however, may depend on what governments do to control monopolistic power potentially wielded by platforms in contrast to any comparable constraints on state authorities. A separate consideration, of course, is how far and for what purpose state authority is enabled in different jurisdictions. The reality is not simply binary as between jurisdictions. The distinction made between "important data" and "core data" in China's 2017 Cyber Security Law is key in defining data flow restrictions.[541]

China's rules on privacy are like those of the EU in some respects, as reflected in some likeness between the European Union's GDPR and China's Personal Information Protection Law (PIPL).[542] Like the European Union, China also places emphasis on facilitation to minimise unnecessary costs in the digital economy. It has recently promulgated a five-year plan on the development of the digital economy[543] which is part of China's 14th Five-Year Plan (2021-2025). The plan foresees the added value from core industries in the digital economy accounting for 10 per cent of GDP and focuses on improving digital governance, making the sector more competitive, and better integrating the real economy with digital technology. There is also a digital trade component of the plan which, like the European Union and United States' aspirations, seeks to extend technology and networks to other countries.

Behind different positions of governments on the free flow of data, are issues such as data localisation, mandatory commercial presence, cybersecurity, privacy, network neutrality, and taxation. In contrast to the embrace of free data flows by the United States, the European Union only does so to the extent

[541] See Gao op. cit. fn 39.
[542] Privacy Policies (2022) The GDPS vs. China's PIPL. https://www.privacypolicies.com/blog/gdpr-vs-pipl/
Xinhua. 2022 January 12. Plan focuses on digital economy development during 14th Five-Year Plan period. https://english.www.gov.cn/policies/latestreleases/202201/12/content_WS61de9a35c6d09c94e48a385f.html

of an exception for flows of private data,[544] where the policy centrepiece is its Global Data Protection Regulation (GDPR), which the European Union has sought to export to other jurisdictions. The US-EU Privacy Shield,[545] as well as the domestic application[546] of the GDPR are not free from design and implementation challenges. China's recent adherence to the Regional Comprehensive Economic Partnership Agreement (RCEP),[547] has signalled a more open approach to data flows, along with commitments to avoid data localisation requirements and the acceptance of cross-border transfer of information by electronic means. But like all digital trade agreements – and indeed trade agreements more generally – commitments are conditioned by language that permits data flow controls on public policy grounds considered legitimate by the government concerned and measures considered necessary to protect essential security interests.[548]

3.2 A Blend of Convergence and Divergence Reflecting Co-Operation and Rivalry

The contrasts and similarities in policies towards the digital economy of the big three offer a mixed picture of the prospects for convergence and co-existence in the context of shared rules for digital trade. Some policy developments reflect growing geopolitical competition, technological competition, notions of sovereignty, security, strategic autonomy, and so on.

Technological and geopolitical rivalry among the big three can influence policy choices and the scope for co-operation in shaping multilateral digital trading rules. At the same time, ongoing efforts to negotiate a digital trade deal suggest that nationalistic motivations are tempered by perceptions of prospects for positive-sum outcomes from co-operation. In the interests of mutual gains from convergence, one can only hope that efforts such as those taking place in the WTO with its e-commerce initiative (see Section 5), may assist in emphasising a search for common ground.

In June 2021 the EU and the United States established the US-EU Trade and Technology Council. This initiative describes itself as "a transatlantic forum fostering co-operation on trade- and technology-related issues, based on shared democratic values."[549] The Council meets twice a year and has 10 working groups focusing on a wide range of digital economy policy and regulatory issues. Its initial focus was China-oriented, but recently it has also been concerned with Russia and Ukraine.

---

[544] It should be noted, however, that the EU is the only one of the three jurisdictions discussed here that has a clear net neutrality provision in its 2016 Open Internet Access Regulations.

[545] Politico Digital Bridge (2022) Privacy Shield: Some Things Never Change. https://www.politico.eu/newsletter/digital-bridge/privacy-shield-update-3-0-semiconductor-subsidies-eu-us-policy-spat/

[546] Brinnen, M. and Westman, D. (2019) What's Wrong with the GDPR? Description of the challenges for business and some proposals for improvement. Swedish Enterprise, December.

[547] RCEP has fifteen member states including *the Association of Southeast Asian Nations* (ASEAN - Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Vietnam), along with five other regional economies – Australia, China, Japan, New Zealand, and Republic of Korea.

[548] Legal Text – RCEP (2022) https://rcepsec.org › legal-text *The relevant provisions can be found in Articles 12.15.2 and 12.15.3 of the v-Agreement.*

[549] European Commission (2022 July 10) Digital in the EU-US Trade and Technology Council. https://digital-strategy.ec.europa.eu/en/policies/trade-and-technology-council

In addition to its co-operative efforts with the European Union on privacy issues, the United States has established the Global Cross-Border Privacy Rules (GCBPR) Forum with Canada, Japan, South Korea, the Philippines, Singapore, and Taiwan to work on privacy rules in order to "promote interoperability and help bridge different regulatory approaches to data protection and privacy".[550] These cross-border privacy rules are based on the APEC GCBPR. The recently established Indo-Pacific Economic Framework for Prosperity (IPEF)[551] is still under construction, including in terms of how formally binding outcomes will be, and it is likely to include significant digital trade provisions. For the United States, this is an effort to reassert influence in the region following the abandonment by President Trump of membership of the Trans-Pacific Partnership in January 2017.

Each of the big three has in recent times issued vision statements or action plans aimed at promoting their digital trade policies and their global positioning. The European Union, for example, has its Next Generation Internet Initiative[552] which seeks to promote what it refers to as an internet for humans. The European Union has also set out its Digital Decade Principles which establishes targets for 2030.[553] The United States, the European Commission, and the European Union member states, along with 33 other countries, have also signed the Declaration for the Future of the Internet, which seeks to promote a vision and the principles of a trusted internet.[554,555]

As already noted, China includes a focus on the digital economy in its 14th Five-Year Plan (2021-2025), which, among other things, emphasises international co-operation and data and network security.[556] In 2014, China established the World Internet Conference (WIC). Its founding members include institutions, organisations, businesses, and individuals from nearly 20 countries. At its second meeting in 2019, the Organizing Committee of the Conference issued a document entitled Jointly Build a Community with a Shared Future in Cyberspace, which called for enhanced solidarity and co-operation in cyberspace.[557] In 2017, China and six other countries launched the Belt and Road Digital Economy International Cooperation Initiative,[558] and in 2020 China also launched a Global Initiative on Data Security.[559]

[550] U.S. Department of Commerce (2022) Global Cross-Border Privacy Rules Declaration. https://www.commerce.gov/global-cross-border-privacy-rules-declaration

[551] Center for Strategic and International Studies (2022) Unpacking the Indo-Pacific Economic Framework Launch https://www.csis.org/analysis/unpacking-indo-pacific-economic-framework-launch May 23. The fourteen parties to IPEF are Australia, Brunei Darussalam, Fiji, India, Indonesia, Japan, South Korea, Malaysia, New Zealand, the Philippines, Singapore, Thailand, the United States and Vietnam.

[552] European Commission (2019) Next Generation Internet initiative. https://www.ngi.eu/about/

[553] European Commission (2022) Europe's Digital Decade: digital targets for 2030. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[554] The White House (2022) FACT SHEET. The United States and 60 Global Partners Launch the Declaration for the Future of the Internet. https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/

[555] European Commission (2022) Declaration for the Future of Internet. https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet

[556] Xinhua (2022) Op.cit. fn.33.

[557] China.org.cn (2022) http://www.china.org.cn/business/2020-11/18/content_76924176.htm

[558] Government of China (2017) Initiative on Belt and Road digital economy cooperation launched. http://www.scio.gov.cn/31773/35507/35520/Document/1612635/1612635.htm

[559] Government of China. 2020. Global Initiative on Data Security. https://www.mfa.gov.cn/ce/ceus/eng/zgyw/t1812951.htm

The involvement of the big three in these various vision statements and aspirational declarations is not only about co-operation among governments, advancing new thinking, and keeping up with technological innovation in the digital economy. They are also about competition for leadership in the digital ecosphere. What remains to be seen is whether such competition can be harnessed to feed cooperative outcomes, or whether it feeds a fracturing process that complicates the quest for mutually beneficial convergence.

3.3 Sovereignty, Trust, and International Co-Operation

The degree to which governments succeed in creating a seamless digital ecosphere with open digital trading arrangements depends on attitudes towards sovereignty and trust. Sovereignty is a multi-faceted concept that has received considerable attention in scholarly literature. Gao (2022)[560] offers a brief summary of what sovereignty means to various authors and why there is no shared definition of the concept. Pohl and Thiel (2020)[561] have discussed the concept at length and highlight the different normative definitions informing the positions of governments. Ultimately, they argue that digital sovereignty is more of "a discursive practice in politics and policy than a legal or organizational concept."[562] For practical purposes, perhaps a simple way of thinking about sovereignty is in terms of the degree of willingness of governments to share authority with one another over their national policies. The degree of willingness to pool such authority is a major factor determining the quality and reach of international co-operation in regime-building in areas such as digital trade. The disposition to do so is conditioned by the degree of similarity among national regimes, the economic benefits to be gained, and the degree of trust underlying the relevant relationships.

Multiple definitions of trust are available, seeking to tease out how the concept should be understood. At its most generic, trust is about the degree of belief in the reliability of someone or something in relation to future actions. In terms of international trade agreements, it is about the quality and reach of mutual pre-commitment to a set of behavioural rules. The quality and reach of rules depend on what governments consider credible and how intrinsically important the outcomes are for the parties involved. Trust can be thought of in terms of a probability distribution that determines how much risk a person or a government is willing to assume when an outcome depends on the ability and willingness of a party to comply with its prior commitments – an outcome that cannot be controlled *ex-ante.*

Trust is central to a range of prerequisites for a viable digital ecosystem that supports digital trade.[563] Some of these elements are less controversial than others, and more susceptible to convergent rules, such as, arguably, the maintenance of interoperable infrastructure, electronic signatures and authentication, e-contracts, e-invoicing, online consumer protection, paperless trading, and cybersecurity. More challenging elements of the digital ecosystem that may need accommodation around divergent approaches, and in that sense may be more demanding in terms of trust, include

[560] Gao, op.cit, fn.30, Pp.4-6.
[561] Pohl J. and Thiel T. (2020) Digital sovereignty. Internet Policy Review 9 (4). https://doi. org/10.14763/2020.4.1532
[562] Ibid. p. 47.
[563] Schneider, J. (2022) The World Without Trust: The Insidious Cyberthreat. Foreign Affairs. January, February.

free flow of data, data localisation, technological neutrality, and taxation. It is arguable that a shared understanding on all these matters, even if at the end of the day it is about agreeing to disagree, is essential to an effectively functioning global ecosystem. Section 4 below discusses salient features of digital provisions in numerous preferential trade agreements (PTAs).

In relation to the trust issue, however, it is perhaps worth mentioning an agreement at one end of the spectrum, namely the Digital Economy Partnership Agreement (DEPA).[564] This Agreement is built around a strong assumption of mutual trust. The original signatories are Chile, New Zealand, and Singapore. These countries may be regarded as relatively like-minded in the relevant areas of trade policy, and other countries interested in joining are invited to apply. The agreement is regarded by its members as holistic and comprehensive. At the same time, signatories enjoy some leeway in developing the specificities of their regulations on the assumption that like-mindedness obviates the need for uniform regulatory formulations. It is also modular in its construction, giving rise to the possibility that it can be drawn upon for other agreements. Table 1 contains the modular headings.

A notable feature of DEPA is that most provisions take the form of soft law – that is, many commitments are not subject to justiciability. Module 14 of the Agreement contains detailed dispute settlement provisions, with scope for consultations, mediation, and ultimately arbitration. Dispute settlement provisions are not applicable to Article 3.3 (non-discrimination among parties), Article 3.4 (ICT products using Cryptography), Article 4.3 (cross-border transfer of information by electronic means), and Article 4.4 (locations of computing facilities). The reason for the absence of more stringent and far-reaching legal enforceability in this instance is that the three signatories enjoy a high level of mutual trust, fundamentally because they pursue similar objectives in relation to digital trade.

Table 1: DEPA Modules

Module 1: Initial Provisions and General Definitions.
Module 2: Business and Trade Facilitation (including paperless trading, domestic electronic transactions framework, logistics, electronic invoicing, express shipments, and electronic payments).
Module 3: Treatment of Digital Products and Related Issues (including customs duties on electronic transmissions, non-discriminatory treatment of digital products, and commitments on technology products that use cryptography).
Module 4: Data Issues (including personal information protection, cross-border transfer of information and location of computing facilities).
Module 5: Wider Trust Environment (including cybersecurity co-operation and online safety and security).
Module 6: Business and Consumer Trust (including spam, online consumer protection, and access to the internet).
Module 7: Digital Identities.

[564] Honey, S. 2021. Enabling trust, trade flows, and innovation: the DEPA at work. Hinrich Foundation. https://www.hinrichfoundation.com/research/article/digital/enabling-trust-trade-flows-and-innovation-depa-at-work/

Module 8: Emerging Trends and Technologies (including financial technology, artificial intelligence, government procurement, and competition policy co-operation).
Module 9: Innovation and the Digital Economy (including public domain, data innovation, and open government data) Module.
Module 10: Small and Medium Enterprises Co-operation.
Module 11: Digital Inclusion.
Module 12: Joint Committee (including a raft of institutional arrangements).
Module 13: Transparency Module.
Module 14: Dispute Settlement Module.
Module 15: Exceptions Module.
Module 16: Final Provisions (including processes for entry into force, amendments, accession, and withdrawal).

Source: Honey, op. cit.

Like other digital agreements, DEPA commits to the free flow of data, and parties recognise the "inherent right to regulate and resolve to preserve the flexibility of the Parties to set legislative and regulatory priorities, safeguard public welfare, and protect legitimate public policy" (Preamble). Other features of the agreement focus on reinforcing communality in approaches. Module 4 on data recognises the OECD general principles of personal data protection, ensures their non-discriminatory treatment between international and internal data, promotes interoperability between different data protection systems and encourages the adoption of data protection trust marks. The Agreement also established a Joint Committee that deals with accession requests and takes responsibility for administering the Agreement.

Trust considerations aside, full global convergence of digital trade regimes is a pipe dream, even for a small group of like-minded countries. It logically follows from this that, especially in agreements among larger groups of more heterogeneous countries, digital trade will be regulated in ways that layer degrees of co-operation among subsets of digital domains. PTAs effectively secure such outcomes through their ability to discriminate between signatories and non-signatories. As discussed in the next section, PTAs abound. Subsequent sections will pose the question of how a non-discriminatory outcome might be built at the multilateral level.

4. DIGITAL TRADE PROVISIONS IN PREFERENTIAL TRADE AGREEMENTS

Various efforts have been made over the years to analyse digital provisions in PTAs.[565] TAPED[566] is a comprehensive database that maps and codes all PTAs with chapters, provisions, annexes, and side documents relevant to digital trade. Some 346 PTAs were established between 2000 and October 2019, of which 184 or more than 50 per cent included provisions on digital trade.[567] Seventy-eight PTAs in the sample contain dedicated e-commerce chapters or side agreements. It is notable that more than 75 per cent of these are bilateral PTAs, over four-fifths of which contain digital provisions.

Two basic observations arising from the database are worth mentioning. The first is that trade agreements have been embracing digital realities with growing intensity. In some ways, this places the PTAs ahead of the multilateral e-commerce negotiations at the WTO. The WTO is playing a game of catch-up where, after more than two decades, it has achieved limited results by way of advancing a digital agenda. The number and diversity of participating parties in the WTO exercise render it far more challenging to come to closure than under PTAs. Indeed, if the WTO had succeeded in advancing the multilateral agenda there probably would have been less activity by PTAs in this area.

The second is that there exists a high degree of heterogeneity among PTAs in relation to provisions that are important for attaining open flows of data. This suggests that if it is to succeed, the multilateral exercise will need to recognise the boundaries to convergence that must be managed in one way or another in order to reach agreement. The question then will be whether a modest multilateral agreement is worth much. The argument made here is that the existence of a multilateral agreement is of considerable systemic importance because it provides a focal point for inclusive joint action in an area that will only become more crucial in international economic relations. Absent a multilateral locus, the damaging fragmentation of the digital economy is likely to be more intense. If governments become more disposed to cooperate and converge in the future, they will have a base upon which to build.

4.1 How Far do PTAs Cross Reference or Rely on WTO Provisions?

There can be no doubt that some of the more comprehensive PTAs seek to "regime shift" in the absence of relevant progress or provisions at the WTO. A separate question is whether PTAs rely on WTO disciplines by cross-referencing them. It would appear that the majority do not in order to lock in binding provisions. References to the WTO are nevertheless fairly commonplace, particularly in the case of PTAs involving the EU, Canada, and Singapore. When references to the WTO are made, they

[565] See, for example, Monteiro, J. Teh, R. (2017) Provisions on Electronic Commerce in Regional Trade Agreements. WTO Working Paper ERSD-2017-11. https://www.wto.org/english/res_e/reser_e/ersd201711_e.htm
[566] Trade Agreements Provisions on Electronic Commerce and Data, University of Lucerne.
[567] Much of the discussion that follows, and the sample data referred to, is based on a thorough analysis made possible by the TAPED database, undertaken by Burri, M., Polanco, R. (2020) Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset. Journal of International Economic Law. 00, 1-34.

are often general statements of applicability. Agreements involving Colombia, South Korea and the United States tend to affirm that WTO commitments are applicable to the degree they are relevant to e-commerce. Other agreements affirm WTO commitments in an overall sense.

In effect, there are many commitments in WTO agreements that are relevant to e-commerce. The Agreement on Trade Facilitation (ATF) is a good example, where streamlined trade administration procedures seek to reap the benefits of greater efficiency. A further consideration is that if a significant disagreement were to arise between PTA signatories, and the matter could be shown to involve an alleged WTO infringement, then a case could in principle be brought to dispute settlement under the WTO.

4.2 Commitments to Non-Discrimination in PTAs

Any commitments to MFN in PTAs apply only to signatories, which suggests that for bilateral agreements such references are neither here nor there. Third parties are in any case protected by WTO obligations. Where there are more than two parties to a PTA, MFN obviously matters. The case with NT is different since that is about how bilateral parties to a PTA treat one another with respect to their own products and service suppliers. Of the 78 PTA agreements in the TAPED database referred to above, only 35 of these include national treatment and 32 of them include MFN. Most of these are binding commitments.

As pointed out earlier, infringements of non-discrimination would in principle be justiciable under the WTO Dispute Settlement Understanding. When the WTO's dispute settlement system was working better than it does today, there were a number of instances where parties to a PTA preferred to use WTO dispute settlement to adjudicate a dispute, even if it would have been feasible to use the dispute settlement arrangements written into the PTA.

As discussed in the next section, in the WTO's e-commerce negotiations conversations about possible departures from the non-discrimination rule have been a continuing backdoor feature of the negotiating process. The clear implication is that there will be a trade-off between the ambition of the agreement and the way in which MFN is treated. The 2018 Brazil-Chile PTA recognised that this debate was going on and agreed to jointly evaluate those discussions in order to decide on how to treat non-discrimination in relation to the content of electronic transmissions.

4.3 Status of the WTO E-Commerce Import Duty Moratorium under PTAs

Provisions banning import duties were found in 76 agreements in the TAPED database. This meant that trading conditions were more certain for such downloadable products including software, music and e-books. Some PTA provisions simply acknowledge the existence of the moratorium, while others affirm its continuation. Others still declare an intention to make the moratorium permanent. This is the most commonly occurring reference to import duties on transmissions found in PTAs. Some PTAs involving the EU assert that digital trade involves services, and services are not subject to import

duties. In referring to digital transactions involving a physical transaction at the consumer end, certain PTAs decree that import duties can only cover the carrier medium and not the content.

The way these provisions are written reveals considerable variation among PTAs. However, in terms of the substantive content of PTA provisions, there is much common ground reflecting opposition to the idea of raising revenue through import duties on electronic transmissions. This means considerable alignment of positions both inside and outside the WTO.

4.4 Promoting Facilitation of E-Commerce Measures Under PTAs

To some degree or other, most trade agreements, including PTAs typically contain provisions aimed at facilitating trade. In the case of digital provisions in the PTAs under consideration, the articulation of facilitation objectives is varied. References are made, for example, to the creation of a favourable framework for global commerce, and the need for clear, transparent, and predictable domestic regulations. This applies both to their design and their administration. Most provisions of this nature are non-justiciable, in other words, of a best-endeavours nature. This tends to make them less contentious and potentially less influential in shaping outcomes. On the other hand, this is where the notion of trust comes in. As discussed above, the existence and influence of trust depends crucially on the degree of like-mindedness among parties to an agreement in regard to desired outcomes. Some PTAs refer directly to the need to create trust and confidence through appropriate regulation. In addition, some 45 PTAs make specific mention of small and medium-sized enterprises and their needs. This is also an area where best-endeavours provisions dominate.

Linked to facilitation is the notion of paperless trading, whereby all documentation associated with trade is made available electronically and can be used as the electronic equivalent of a paper version. Savings resulting from the enhanced efficiency of such arrangements are likely to be considerable. DEPA relies on paperless signatures for the parties to sign on. More recent PTAs press for the use of international standards and methodologies, such as those of the World Customs Organization. In some PTAs, adhering to international practices is an obligation. Fifty-six of the agreements in the sample contain paperless trading provisions and other cost-reducing approaches.

Electronic authentication also enhances efficiency. This arrangement provides for mutual recognition of technologically created digital certificates and signatures. Sixty-eight PTAs in the sample include provisions relating to electronic signatures. Over time, provisions on electronic signatures have become more binding, with emphasis either on allowing appropriate authentication and recognition arrangements or mandating their development. A range of other areas where the objective is to reduce trade and transaction costs include electronic contracts, electronic invoicing, electronic payment systems, and unique consignment numbers. The relevant provisions in PTAs tend to rely on commitments to policy objectives rather than the explicit specification of standards. Where the latter is a feature, however, reference is often made to the 1996 UNCITRAL Model Law on Electronic Commerce.

For the most part, policies aimed at facilitation appear to be relatively uncontentious. This is because they are essentially flanking measures, contingent upon commitments relating to basic elements of

the digital ecosystem. The most important of these are the provisions that determine whether and under what conditions data flows are permitted across national frontiers.

4.5 Data Flows

Early references to information crossing borders tended to be more aspirational than mandatory. Since the negotiations of the TPP/CPTTP (2017-18) and the Pacific Alliance (2015), provisions on data flows have become more formal. These agreements require that information be allowed to flow across borders by electronic means, including personal information when it is for the conduct of business by a covered person. This obligation is conditioned by the right of governments to "adopt or maintain measures to achieve a legitimate public policy objective, provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and does not impose restrictions on transfers of information greater than are required to achieve the objective."[568]

Language similar to this has been used in many other PTAs. The USMCA added more language regarding restrictions on cross-border data flows. It states that a restriction on cross-border data flows is not considered to achieve a legitimate public policy objective if it results in different treatment of data flows in a manner that affects the conditions of competition in the domestic market, and the restriction arises solely because the data flows in question are cross-border.

4.6 Data Flow Content and the Impracticality of Rules of Origin

It is worth noting that in contrast to a rules of origin regime involving goods that physically cross the border under preferential trade arrangements, it would be exceedingly difficult to apply rules of origin to the content of digital trade flows. This is related to the earlier discussion in Section 2.9 on the WTO Moratorium in respect of import duties on digital transmissions. While it might be challenging enough to identify taxable inputs into digitised products with physical equivalents, an added layer of difficulty arises if duty exemptions are to be allowed depending on the origin of particular inputs. Any government attempting to apply a rules of origin regime on digital trade across borders would have to identify the physical equivalent inputs making up a product, their taxable value, and their geographical origin. If governments seek to differentiate the terms of access to their markets on the basis of PTA relationships, they are likely to seek alternative means of discrimination which would be costly, distorting, and impractical.

Taking account of these realities, and the intrinsic difficulties of relying on such measures of discrimination, a different way of thinking of PTAs might be as stepping stones to digital convergence rather than constructs for favouring selected trading partners. Seen in this light, PTAs could more easily be envisaged as part of a convergent movement towards a multilateral agreement.

[568] Article 14.11 paragraph 3 of the TPP/CTPP text.

4.7 Data Localisation Restrictions

Increasingly, PTAs contain provisions on data localisation and/or the location of computing facilities. Most of these provisions are binding in nature and seek either to ban or to limit data localisation requirements. However, many stipulations are also accompanied by language allowing deviations from these data flow restrictions on public policy and national security grounds. A practical question is how far data localisation requirements are disruptive in practice, considering the relative ease with which data can be replicated. The answer would seem to reside in the question of how far data localisation requirements are tied to data flow restrictions.

In practice, data localisation requirements can vary in terms of their restrictiveness. They may simply prohibit certain categories of data from being stored in another jurisdiction. The prohibition may also extend to the processing of domestic data abroad. A softer control would be that there must be a local copy of domestically generated data, but the data may also be stored abroad.

4.8 Privacy and Data Protection

Some 82 of the PTAs included in the sample used by Burri and Polanco (2020) from the TAPED dataset contain provisions on privacy, usually under the rubric of data protection. In one form or another, data protection has become a standard trade-related provision in most PTAs of any depth. While just over one-third of the PTAs surveyed in the Burri and Polanco (2020) analysis were classified as “soft”, it seems that the treatment of data protection has also moved increasingly towards more binding obligations. The evolution of data protection provisions in PTAs also reflects to a degree the continuing efforts at accommodation between the United States and the European Union on this issue, starting from quite contrasting positions.

Several features shaping data protection provisions are worth mentioning. First, PTAs are increasingly developing differentiated rules for sectors, especially telecommunications and financial services. Second, in addition to key provisions on such matters as content, usage, and collection methods, PTAS also often include a range of ‘flanking’ activities. These may include such elements as information and experience sharing, research and training, dialogue and consultations, and technical assistance. This tendency is a reflection of the reality that the relevant provisions are highly varied among PTAs.

Third, data protection and privacy provisions can take the form of the introduction of new standards. The measures concerned may relate to data collection and processing, particular administrative procedures, or non-discrimination clauses. Finally, more binding policy tools can include explicitly-stated principles, equivalence understandings relating to outcomes, or the institutionalisation of standing bodies under the agreement that work on developing norms and guidelines, reviewing existing arrangements, and ruling upon or otherwise disposing of any issues as they arise. Some of these efforts seek to rely on standards already developed. These include such provisions or guidelines as the OECD recommendation to its Council on Guidelines Governing the Protection of Privacy and

Transborder Flows of Personal Data[569] and the APEC Privacy Framework.[570] In sum, existing approaches to data protection in PTAs are quite different from one another in many instances and constitute a rather complex collection of stipulations and urgings.

What is the relevance of this brief summary review of the jungle of digital provisions in PTAs to the possibility that governments could fashion a more full-blown approach to multilateral co-operation in digital trade? Even where principles are enunciated in trade agreements, such as the free flow of data, they are subject to exemptions and exceptions of various kinds. This is likely not only to be in the case of public policy preferences and various forms of protection from competition but also in relation to non-discrimination. The question is whether these kinds of departures from principles can be negotiated and made subject to prior commitments in a multilateral agreement – in justiciable form or otherwise – or whether they are going to be the fodder for further fragmentation. Success in avoiding further fragmentation depends on how a balance might be struck between open international data flows and the protection of legitimate public policy objectives.

Some PTAs are instructive in this regard, as is the accumulated experience of the WTO and its forerunner, the GATT. It remains to be seen how successful the WTO will be in fashioning a multilateral agreement on digital trade. Such an agreement will have to adequately balance the economy-wide value of relatively unimpeded international data flows with appropriate protection of public policy objectives. The prospects for the WTO in this domain are taken up in the next Section.

4.9 Multilateralism: Addressing Convergence and Divergence

The brief review above, along with the discussion in Section 3, reveals multiple efforts over the last few years to forge international agreements on digital trade. Nearly all the preferential efforts to establish rules in the area have been part of broader preferential trade agreements, usually incorporating a digital trade chapter in a more comprehensive PTA. In the absence of any multilateral template, the agreements tend to vary a little in architectural approach, but on the face of it less so in relation to content. Formulations have often been borrowed from WTO agreements.

Analyses such as those by Burri and Polanco (2020),[571] Drake-Brockman et al. (2021),[572] Elsig and Klotz (2021),[573] or Lippoldt (2022),[574] for example, show that while digital economy rulemaking in PTAs is somewhat fractured and complex, formulations of many provisions are similar, and in parts identical. The CPTPP, USMCA, United States-Japan, United Kingdom-Japan, Australia-Singapore, and DEPA, for

[569] OECD (2013) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[570] APEC Secretariat (2005) APEC Privacy Framework. https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

[571] Burri and Polanco, Op cit. fn. 56.

[572] Drake-Brockman, J, Gari, G., Harbinson, S., Hoekman, B., Nordas, H.K., Stephenson, S. (2021) Digital Trade and the WTO: Top Negotiating Priorities for Cross-Border Data Flows and Online Trade in Services. Jean Monnet IIISA Network Working Paper no. 11-2021 September.

[573] Elsig, M. and Klotz, M. (2021) Data Flow-Related Provisions in Preferential Trade Agreements: Trends and Patterns of Diffusion, in Burri, M. (Ed.) (2021) Biga Data and Global Trade Law. Cambridge University Press. Pp. 42-62.

[574] Lippoldt, D. (2022) Regulating the Digital Economy: Reflections on Trade and Investment Nexus. CIGI. February. https://www.cigionline.org/articles/regulating-the-digital-economy-reflections-on-the-trade-and-innovation-nexus/

instance, are sometimes the same, similar or quite convergent when it comes to cross-border data transfers, non-discrimination, public policy exceptions, privacy, source codes, consumer protection, cybersecurity co-operation, and data localisation. The RCEP, on the other hand, is something of an outlier in some areas, including language on stronger security exceptions relating to free data flows and data localisation.

If the formulation of provisions regulating data flows in the digital provisions of PTAs point in the direction of likely convergence, the picture appears a bit differently when it comes to an examination of particular measures. These, it may be argued, reflect something of the actual application of provisions in the agreements. A recent report by Evenett and Fritz (2022)[575] has documented thousands of digital policy interventions in G20 countries since 2008. They observe a notable uptake in measures since 2017, consistent with growing awareness of the growth of the digital economy and the reality that government policy lags behind marketplace realities. Some policies used with greater frequency, such as increased foreign investment screening and the growth in the use of subsidies, are relevant beyond the confines of the digital economy. Others of the kind referred to earlier in this section include such matters as data governance, content moderation, user rights, business obligations, and digital taxation. This Report concludes that policy fragmentation is on the rise and provides systematic evidence of the tendency in a significant number of policy domains.

Opinions as to the balance between policy divergence and convergence, and the imminence of the threat to future efforts at international policy convergence vary. More granulated analysis would be required to determine where the greatest difficulties reside in enhancing policy co-operation. But there can be no doubt that an important challenge remains if the considerable benefits available from the development of the digital economy are to be realised. The more inclusive such efforts in terms of country coverage, the greater the potential rewards. The following section assesses progress and prospects for multilateral co-operation in the digital trade domain.

[575] Evenett, S. J. and Fritz, J. (2022) Emergent Digital Fragmentation: The Perils of Unilateralism. A Joint Report of the Digital Policy Alert and Global Trade Alert. CEPR Press. https://www.hinrichfoundation.com/

5. MULTILATERAL AGREEMENT ON DIGITAL TRADE

5.1 Multilateral Efforts to Build an Integrated Global Digital Ecosystem

The discussion that follows is based on the WTO's ongoing efforts to craft an agreement on e-commerce agreement. The WTO is not the only place that a multilateral deal could be put together although it's an obvious candidate considering its mandate, the work that is underway, the numerous cross-references to WTO obligations in PTAs, and the accumulated experience of the institution. On the other hand, particular issues like taxation may be better dealt with elsewhere, as is the case at present with the OECD and taxation. If the WTO does succeed in pushing forward with its work on e-commerce, it will be essential to work with other agencies and organisations. There are many technical issues that must be tackled in the digital trade ecosystem. The WTO has some history of success in working with other agencies in the past, notably in the area of standards.

A short review of decision-making in the GATT/WTO is necessary in order to appreciate the context in which negotiations are being undertaken in the WTO on the Joint Initiative on E-Commerce. The GATT and the WTO have for many years maintained a system whereby decisions must be taken by consensus. A consensus is defined as the absence of any objections from those members present at the time a decision is taken. The consensus rule for decisions was designed to ensure that all parties were disposed to joint action under any approved agreement or commitment. While this approach tended to foster a sense of inclusiveness, it also meant that decisions could take longer to reach, while some were rendered impossible to reach, even when the opposition was highly minoritarian.

Over the last twenty-five years or so, adherence to consensus decision-making has started to wane. Early manifestations of this emerged in the immediate aftermath of the Uruguay Round in the area of services. Negotiations on two key service sectors – telecommunications and financial services – were incomplete by the time the Uruguay Round ended and then entered into force in January 1995. The continuation of these negotiations took place among a subset of the membership, and the eventual results were adopted by those members who agreed to do so. These negotiations were considered part of the Uruguay Round and did not require a separate mandate. In telecommunications, the results were regulatory in nature and took the form of a template, as discussed in Section 2.

In the case of financial services, also discussed above, the outcome was the Understanding on Commitments in Financial Services, under which the signatories assumed a series of additional commitments. In 1996, the technique of arriving at an agreement among a subset of parties was extended to information technology. The Information Technology Agreement involved a negotiation amongst those members who wished to further reduce their tariffs in information technology products.

While the subset of WTO members that adopted any of these agreements were required to assume additional obligations, nothing was required of the rest of the WTO membership that did not participate in the agreement. But those members were still able to benefit from the obligations

assumed by the others – in other words, to enjoy possible additional benefits arising from the agreement in question. This was on account of MFN.

Because the agreements among subsets of members did not seek any reciprocity from non-signatories, this tended to produce a situation in which an agreement would only fly if enough significant actors in the markets concerned signed on. This is why these agreements became known as "critical mass" agreements. Critical mass agreements would only succeed if enough countries were part of them to ensure an adequate level of reciprocity. In systemic terms, one implication of the reciprocity imperative is that these kinds of agreements need to be promoted and carried through by large economies. This can be seen as a systemic weakness, in the sense that maintaining MFN fractures the membership, but at the same time it kills off veto power among naysayers who refuse to engage. For many reasons not addressed here, the WTO has mostly lost its negotiating function over the last two decades or so. In the meanwhile, frustration has grown with what was widely seen as the stifling effect of the consensus principle. In the eyes of many, consensus was becoming the equivalent of a veto that could be used at will, either simply to stop things happening or to extract a concession elsewhere from those determined enough to push for a new agreement.

5.1.1 The birth of the Joint Initiative on E-Commerce

At the 11th WTO Ministerial Meeting held in Buenos Aires in 2017, subsets of members became active again in promoting negotiations in a number of subject areas that would not require a consensus decision to initiate. Moreover, nor would they need a consensus decision to complete if the results of the negotiation could be inscribed individually by participating members in their schedules of concessions.[576] These negotiations were referred to as Joint Statement Initiatives (JSIs) or Joint Initiatives (JIs). JIs were launched in e-commerce, investment facilitation for development, a working group on micro, small and medium-sized enterprises, and on advancing ongoing discussions on domestic regulation in services trade. All of these joint initiatives shared a commitment to MFN. Some of them envisaged negotiations, while others were more exploratory on the matter, or more likely to focus on soft law outcomes.

The Joint Initiative on E-Commerce was subscribed to by 71 WTO members, including China, the EU and the United States. The negotiation phase of the JI on E-Commerce was launched in January 2019. Currently, 86 WTO members are participating, representing over 90 per cent of global digital trade. There is no critical mass challenge here. On the contrary, the fact that so many countries are involved, with such different approaches to digital trade policy, represents a challenge in finding a landing zone for a robust and relevant multilateral agreement. The participation of the three digital giants – China, the European Union and the United States – is more than merely illustrative of the challenges of policy diversity. Yet at the same time, this initiative presents an opportunity. It can explore the reach of convergence at the global level. At the same time, it is a useful platform for governments to understand better their differences as a precursor to finding ways of lessening them. In that sense,

[576] Under the WTO agreements, each member maintains listings (schedules) of product-specific commitments both in goods (tariff schedules) and in services (schedules of specific commitments).

this negotiation may be able to extend the frontiers of convergence, even if only in relatively modest ways.

Two important elements of impetus for promoting the launch of the Joint Initiative on E-Commerce are worth mentioning. First, the Work Programme on E-Commerce launched in 1998 was not perceived as a negotiating exercise in the late 1990s and has not moved in that direction in the meantime. Second, there has been growing awareness that the WTO was being left behind by the onward march of information technology in its multiple guises and applications. As noted previously, the GATS covered some of the relevant ground, as did the 2017 Agreement on Trade Facilitation. But, the focus of these agreements was not digital trade and the plethora of policies and regulations relevant to digital exchanges across borders.

The JI on e-commerce is engaged in developing an e-commerce text, and all WTO members are entitled to participate in these digital trade negotiations and to receive all written material pertaining to the negotiation process. The initiative is jointly co-chaired by the Geneva Ambassadors of Australia, Japan and Singapore. The negotiations proceed through the exchange of textual proposals among members. Discussions take place both in plenaries and in small groups dedicated to specific topics.

Issues raised by members' submissions are discussed under six main themes: enabling electronic commerce, openness and electronic commerce, trust and digital trade, cross-cutting issues, telecommunications, and market access. These themes are divided into various subsectors and the subsectors in turn are divided into more specific topics. The latest version of the consolidated text was issued in September 2021. It summarises all the negotiating proposals under each topic, using square brackets to denote alternative proposals and no brackets where the language is either agreed upon or uncontroversial. Under some topics there is only a placeholder. In order to give an idea of the structure of the negotiations, Table 2 provides a listing of the subsectors and topics under each sector. This is a working structure and listing that has not been agreed. Ultimately, nothing is agreed until everything is agreed.

5.2 Progress in the Negotiations

These negotiations take place behind closed doors, and the state of play at any given time is not divulged publicly. This is intended to facilitate progress and avoid the difficult task of negotiating on multiple fronts simultaneously. Ultimately, the results will be subject to public scrutiny and decided upon according to domestic approval procedures, usually involving a legislative authority. In the meantime, however, in light of the complexity of the issues under negotiation, some participants have expressed concern about a lack of transparency, bearing in mind that small groups frequently meet in parallel. Attaining an appropriate balance in the conduct of such negotiations among numerous parties is a perennial challenge.

In December 2021, just prior to the COVID-driven postponement of the 12th WTO Ministerial Conference (MC12), the Trade Ministers of Australia, Japan, and Singapore, as the co-chairing

members of the JI, issued a statement reporting on progress.[577] The Ministers reported "substantial progress" in the negotiations and identified eight articles where "good convergence" had been achieved. These included online consumer protection; electronic signatures and authentication; unsolicited commercial electronic messages; open government data; electronic contracts; transparency (subject to the final scope of provisions and architecture); paperless trading; and open internet access.

The Ministers also referred to the consolidation of text proposals in other areas, including customs duties on electronic transmissions, cross-border data flows, data localisation, source code, electronic transactions frameworks, cybersecurity, and electronic invoicing. They further reported advanced discussions on market access. The Ministers also noted that "provisions that enable and promote the flow of data are key to a high standard and commercially meaningful outcome." The co-convenors undertake to arrange the work programme for 2022 to secure convergence on the majority of issues by the end of 2022.

Table 2: Sectors, Subsectors and Topics Under Consideration in JI on E-Commerce

ENABLING ELECTRONIC COMMERCE
A.1. Facilitating Electronic Transactions
(1) Electronic transactions frameworks
(2) Electronic authentication and electronic signatures
(3) Electronic contracts
(4) Electronic invoicing
(5) [Electronic payments services / Facilitation of e-payment]
A.2. Digital trade facilitation and logistics
(1) Paperless trading
(2) De minimis
(3) Unique Consignment Reference Numbers
(4) Customs procedures
(5) Improvements to trade policies
(6) Single windows data exchange and system interoperability
(7) Logistics Services
(8) Enhanced trade facilitation
(9) Use of technology for the release and clearance of goods
(10) Provision of Trade Facilitating and Supportive Services
OPENNESS AND ELECTRONIC COMMERCE
B.1. Non-discrimination and liability
(1) Non-discriminatory treatment of digital products
(2) Interactive computer services (limiting liabilities)
(3) Interactive computer services (infringement)

[577]WTO Joint Statement Initiative on E-commerce Statement by Ministers of Australia, Japan, and Singapore. (December 2021) https://www.wto.org/english/news_e/news21_e/ji_ecom_minister_statement_e.pdf

B.2. Flow of information
(1) [Cross-border transfer of information by electronic means / Cross-border data flows]
(2) Location of computing facilities
(3) [Financial information / Location of financial computing facilities for covered financial service suppliers]
B.3. Customs duties on electronic transmissions
B.4. Access to internet and data
(1) Open government data
(2) [Alt 1: Open internet access / Alt 2: Principles on Access to and Use of the Internet for electronic commerce/Digital Trade] [FN]
(3) Access to online Platforms / Competition
TRUST AND ELECTRONIC COMMERCE
C.1. Consumer Protection
(1) Online consumer protection
(2) Unsolicited commercial electronic messages
C.2. Privacy
(1) [Personal information protection / Personal data protection]
C.3. Business trust
(1) Source code
(2) ICT products that use cryptography

CROSS-CUTTING ISSUES
D.1. Transparency, domestic regulation and co-operation
(1) Transparency
(2) Electronic availability of trade related information
(3) Domestic regulation
(4) Co-operation
(5) Co-operation Mechanism
D.2. Cybersecurity
D.3. Capacity building
(1) Options for capacity building and technical assistance
TELECOMMUNICATIONS
E.1. Updating the WTO Reference Paper on Telecommunications Services
(1) Scope
(2) Definitions
(3) Competitive safeguards
(4) Interconnection
(5) Universal service
(6) Licensing and authorisation
(7) Telecommunications regulatory authority
(8) Allocation and use of scarce resources
(9) Essential facilities

(10) Resolution of disputes (11) Transparency E.2. Network equipment and products (1) Electronic commerce-related network equipment and products MARKET ACCESS Section F: Market access (1) Services market access (2) Temporary Entry and Sojourn of Electronic Commerce-Related Personnel (1) Goods market access ANNEX 1: SCOPE AND GENERAL PROVISIONS (1) Preamble (2) Definitions (3) Principles (4) Scope (5) Relation to other agreements (6) General exceptions (7) Security exception (8) Prudential measures (9) Taxation (10) Dispute Settlement (11) Committee on Trade-Related Aspects of Electronic Commerce

When MC12 finally took place in June 2022, a Ministerial Decision agreed to reinvigorate the Work Programme on Electronic Commerce,[578] based on the original mandate set out in the 1998 adoption of a Work Programme on Electronic Commerce.[579] Unsurprisingly, there was no mention of moving towards a negotiating phase in the Decision, leaving the Joint Initiative as the sole venue at this point for digital trade negotiations at the WTO. As Table 2 above suggests, a successful JI outcome has a distinct attraction unmatched by many other digital trade agreements in that it intends to adopt a holistic approach to the digital ecosystem. It would also encompass market access commitments in both goods and services.

[578] Ministerial Conference (2022) Work Programme on Electronic Commerce. Ministerial Decision. WT/MIN(22)/32. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN22/32.pdf&Open=True
[579] WT/L/274. Op cit. fn.22.

6. CONCLUSIONS

Legislative and regulatory actions on digital activity have multiplied in recent times, as have various vision statements, initiatives, and declarations. This is a clear reflection of the growing importance of the digital ecosphere, both nationally and internationally. As three major economic powerhouses – China, the European Union, and the United States – develop digital regimes, elements of convergence and divergence are bound to manifest themselves. These emerging nationally based regimes constitute the raw material for efforts to integrate the digital economy through digital trade agreements. Dozens of preferential agreements embodying digital trade rules have fashioned similarly if not identically worded provisions. Regionally based entities such as APEC, ASEAN, and in time the African Continental Free Trade Area (AfCFTA) can also support multilateral efforts.

As regimes regulating digital trade progress and become more complete, pressures to adopt divergent paths may emerge. If fragmentation takes hold, the integrative power of the digital economy could become the very instrument of economic and social disintegration. The direction of travel should be towards rendering regimes as compatible as possible under the umbrella of a multilateral agreement. Nevertheless, some divergence in digital trade regimes is both inevitable and desirable. Diverse preferences and priorities among countries must be respected and accommodated, not bulldozed. A certain degree of diversity can also be a source of resilience and competition. Governments will need to rise to the challenge of working with some differences in regulatory approaches to data flows and the broader policy environment that shapes digital trade. Where convergence is unattainable, managed divergence can be a viable alternative provided there is a sufficient degree of pre-commitment to the rules of the game, predicated upon a shared conviction that mutual gains are to be had from co—operation. Managed divergence is a far better outcome than a retreat towards policy autonomy.

Given the work carried out so far, the primary locus for engaging in continuing negotiations to forge a comprehensive, inclusive, non-discriminatory, and stand-alone multilateral digital trade agreement should be the WTO. Such an agreement should include market access commitments in services and goods as well as regulatory disciplines, along with a binding dispute settlement mechanism. The agreement should be flexible and enabling, with built-in mechanisms for revisiting provisions, facilitating deliberation, and a mandate for continuing negotiations. The provision of technical assistance is essential to supplement the efforts of dozens of countries seeking to participate more fully in the digital economy.

The WTO already has commitments in some of the relevant areas of regulation for a digital trade agreement, as well as market access commitments in services and goods. These can be taken across to a stand-alone digital trade agreement with considerably less need for additional negotiation. Negotiations should also be supported by other agencies and organisations with technical expertise.
All trade agreements in the digital sphere and elsewhere contain an exception clause to take care of overriding public policy concerns, be they about such matters as social preferences or values, national security, consumer protection and privacy, and cybersecurity. Governments do not try to negotiate away the primacy of public policy objectives. Rather, attention falls on ensuring that the measures

taken on these grounds are non-discriminatory, necessary, and proportional, and do not constitute a disguised restriction on trade.

The public policy exception is the one place, besides judgements on national security grounds, where measures can be taken at the sole discretion of a member on the presumption that the objective at hand is beyond challenge. These public policy exceptions have proven contentious at times. In order to build trust and ensure adequate accountability and transparency, provisions should be strengthened to secure against misuse or arbitrariness. Strengthened provisions could include requirements to pre-notify intended measures if the circumstances are not too time-sensitive, and in any event to notify them at the earliest opportunity. Parties should also be required to justify in writing the reasons for the measures and for their nature and extent. Such additions would contribute to greater confidence in the management of public policy imperatives.

On the issue of non-discrimination, MFN refers to equal opportunity, not to equal outcomes. Acceptance of this distinction is important. If regulatory structures are the same, then opportunity and outcome will be identical under MFN. However, even with workable equivalence criteria under an agreement with varied regulatory approaches on particular issues, there will be cases where equivalence is deemed absent among regulatory approaches. How, then, are MFN outcomes secured? The answer turns on the likeness between two situations. One party will receive unqualified MFN treatment (equivalence between outcome and opportunity) if regulatory approaches converge. But where convergence is lacking, outcomes may result in less access as a result of a regulatory equivalence test. Or access may be denied altogether. An outcome that is not the same for two parties could nevertheless be MFN-consistent on a determination of regulatory non-equivalence between two parties seeking access to the same market. One way of putting this is that it captures the difference between convergence and managed divergence.

Where these kinds of MFN-consistent outcomes offer less opportunity to different trading partners, they may create an incentive to negotiate away the lack of equivalence, as has proven to be the case with privacy-related regulatory design, notably between the European Union and the United States. This argument regarding equivalence and MFN-based access is about regulations and not the terms of sector- or product-specific market access. When it comes to market access in respect of particular products, reciprocity is deemed to have already been served in negotiations among parties to an agreement, despite the fact that the relevant commitments are not the same. In these circumstances, a denial of access on non-equivalence grounds would be considered a violation of MFN unless it was covered by a contingency trade measure such as an anti-dumping or countervailing duty to neutralise dumping or subsidisation.

Where there is a sufficiently high degree of unresolved divergence among parties to an agreement, a question may arise as to the level of ambition appropriate to a negotiated outcome. If the level of ambition is too high, a negotiation could drag on interminably, or simply collapse. Neither outcome is desirable if there is an agreement worth harvesting at a lower level of ambition. In a world of considerable policy variance among countries, it would be worthwhile to trade off ambition for a more modest success.

There are at least three reasons for doing so. First, if there is scope for rendering the digital ecosystem more supportive of trade, even though more modestly than hoped, there is an economic justification for securing the agreement. Second, the building of trust is a process and if a modest agreement is already in place that delivers a result, it is possible that this could facilitate stronger outcomes in the future. Third, where an agreement exists, it is likely that policy tendencies towards building further divergence in approaches to digital policies would be tempered.

In considering degrees of ambition in digital trade agreements, it is perhaps worth distinguishing between process convergence and substantive convergence. Securing co-operation in building the digital network for carrying out digital content exchange is likely to be less contentious than agreeing to convergence in relation to the content itself. Process convergence embraces a range of flanking digital trade disciplines. These might be considered to include such issues as consumer protection, electronic signatures and authentication, unsolicited commercial electronic messages (spam), open government data, electronic contracts, and paperless trading. These have reportedly proven to be among the issues closest to an agreement so far in the WTO e-commerce negotiations.

7. A SUMMARY OF KEY RECOMMENDATIONS

The recommendations summarised below represent a distillation of the main arguments elaborated in the paper in relation to the establishment of a multilateral digital trade agreement.

Broad coverage of a digital trade agreement is essential for effective inter-jurisdictional co-operation.

International agreements on digital trade aiming to maximise mutual gain among nations need to be extensive in coverage. They must go beyond regulation to cover sector-specific market access commitments in both goods and services, particularly where these are relevant to the digital economy. The access commitments may never be identical and convergence in access levels may be aspired to over time. But in the case of regulation, convergence is a default objective, with negotiated divergence being the fallback position that accommodates different values and priorities.

Non-discrimination should be the bedrock of international co-operation in digital trade relations, but clarity is required as to the meaning of non-discrimination.

An underlying principle of an inclusive (global) digital trade agreement is non-discrimination (MFN), to be applied among trading partners even in the case where public policy imperatives defy full regulatory convergence or market access. But we need to define MFN with care. It is about equality of opportunity but not necessarily equality of outcome in non-equivalent circumstances. Where adequate levels of equivalence are absent between partners, a lack of likeness prevails between products or production which means MFN does not apply, and this is preferably a negotiated outcome reflecting divergence.

A successful international digital trade agreement needs an overarching institutional persona.

A comprehensive and inclusive digital trade agreement needs the necessary coherence to bring together all its components under a single overarching structure. The World Trade Organization is already implicated in multiple aspects of rulemaking related to the digital economy. But it is not equipped to manage all of the complexities of the digital ecosystem. A variety of inter-governmental and non-governmental institutions with particular specialisations would need to be part of, and influential in, shaping an agreement.

Building a comprehensive multilateral digital trade agreement will take time, but progress should be 'banked' when possible. At the same time, preferential trade agreements can play a useful role in demonstrating what is possible while releasing constraints on those governments wishing to go further faster.

Governments will encounter difficulty in agreeing on a comprehensive multilateral digital trade agreement in terms of some of its provisions. In general, it is easier for them to agree on elements of regulation that embody public good elements by ensuring mutually beneficial outcomes. Such

elements include consumer protection, electronic signatures and authentication, spam, open government data, and electronic contracts. Other issues, particularly those that highlight divergencies in public policy imperatives and issues of competition. Governments should not set the bar of ambition too high too soon, but rather consolidate and implement elements of an agreement upon which to build subsequently. At the same time, preferential digital trade agreements can usefully inform a multilateral agreement and provide an opportunity for those governments who want to go further the opportunity to do so without having to bring all parties along. A further important consideration is that if governments 'bank' progress, they may be avoiding a further splintering of the digital ecosystem.

cerre Centre on Regulation in Europe

Avenue Louise 475 (box 10)
1050 Brussels, Belgium
+32 2 230 83 60
info@cerre.eu
www.cerre.eu
@CERRE_ThinkTank
Centre on Regulation in Europe (CERRE)
CERRE Think Tank