Putting Trust Back in Trusted Connectivity: A Call for More Congruence in Cross-Border Data Transfers

Priyadarshini D
Putting trust back in trusted connectivity: a call for more congruence in cross-border data transfers

ABSTRACT

The socio-economic benefits of cross-border data connectivity are significant. A fragmented regulatory landscape driven by lack of trust is, however, a crucial barrier. As leading trade partners and champions of digital connectivity, the EU and Asia could gain considerably by bridging the trust deficit and fragmentation to create one of the world’s largest regions for seamless data flows. Future action must therefore prioritize: (a) a detailed mapping of regulatory frameworks highlighting commonalities, compliances, and local nuances and imperatives driving Asian countries, for future discussions and policy-making; (b) an evaluation of the impact of regulatory tools such as adequacy decisions and data localization, and possible alternatives; (c) multistakeholder negotiations on the plurilateral e-commerce initiative at the World Trade Organization, which also includes countries that have expressed reservations; (d) the pursuit of “soft law” provisions alongside the negotiations for legally binding provisions; (e) the pursuit, in the immediate to short term, of interoperability mechanisms such as certifications or adequacy decisions; and (f) a holistic approach to policy that encompasses both hard and soft digital connectivity.

INTRODUCTION

Digital connectivity is a key driver of socio-economic growth. By 2023, around 29.3 billion networked devices are expected to connect machines, vehicles, infrastructure and buildings – more than users. Newer information and communication technologies such as 5G and the Internet of Things are poised to produce exponential levels of data. It is this data – and its movement across borders – that is fast becoming the bedrock of modern trade and commerce, socio-cultural interactions, governance and enforcement, and a critical input in emerging technologies like artificial intelligence that could carry significant societal ramifications.

Commercial cross-border data flows contributed more than trade in goods for the first time in 2014, accounting for nearly US$2.8 trillion of the global GDP of US$78 trillion that year.1 The surge of e-commerce, remote work, and the sharing of data for the development of Covid-19 vaccines demonstrate the benefits of cross-border data connectivity. They also underscore the importance of recognizing the link between soft, or data, connectivity and the underlying digital infrastructure such as mobile and broadband connectivity that facilitates them. In this milieu, as leading trade partners and significant contributors to world trade that have prioritized digital connectivity, the EU and Asia – the focus of this AESCON Policy Brief – could stand to benefit considerably from a deepened engagement on cross-border data flows.

Yet while there is general consensus on the potential of cross-border data connectivity to enhance shared and sustainable socio-economic prosperity and growth, there are vastly different approaches on how to regulate cross-border data flows. The Digital Economy Report 2021, issued by the United Nations Conference on Trade and Development (hereafter, UNCTAD Report),2 identifies three main approaches to regulating data. The Chinese model is driven largely by concerns about sovereignty over domestic data, as well as economic and national security considerations. The European approach is centred on the primacy of individual human rights, including privacy and the protection of personal data. The American approach is liberal and market-driven. The UNCTAD Report also recognizes a fourth approach – that of India’s – as being distinctive for seeking to apply data for domestic development.

Beyond these broad policy approaches, there also exist diverse regulatory frameworks and tools to control the transfer of data across borders. These range from unilaterally imposed conditions such as adequacy decisions and prior regulatory approvals for

1 James Manyika et al., Digital globalization: the new era of global flows, McKinsey Global Institute, 24 February 2016.
data transfers, to data localization requirements. The underlying motivation for these divergent approaches and restrictions is a lack of trust. A key driver for data localization, for example, is the opacity around collection, processing and the use of data by global digital platforms. Another is a ‘data divide’, where the gains of monetizing data have been captured by a few global digital platforms (mainly in the US and China) at the expense of ‘data providers’ that are located primarily in the developing world. The requirement for adequacy or equivalence is driven by uncertainty around the application of robust safety and security standards, particularly regarding personal data.

Significantly, there is no one-size-fits-all approach today. Importantly, countries’ responses involve both economic and non-economic dimensions of data, such as human rights, data sovereignty and national security. Ironically, perhaps, the range of policy and regulatory responses also represents an attempt to create trusted environments for individuals, countries and corporations to share data. The results of all this, however, are a fragmented landscape and barriers to data flows, which impede the realization of socio-economic opportunities and the benefits of a data-driven digitally connected global economy.

Against this complex backdrop, this AESCON Policy Brief considers the following questions in the context of cross-border data flows between the EU and Asia: how can data governance frameworks establish the necessary trust to enable the seamless movement of data across borders? And is it possible to achieve convergence or interoperability of different data-governance regimes while accommodating local imperatives or concerns?

In doing so, this policy brief highlights certain developments that indicate emerging areas of commonality or convergence. It also offers some recommendations arising from the discussions held at the session on ‘Norms and standards for trusted connectivity’ at the 2nd edition of the Asia-Europe Sustainable Connectivity Conference (AESCON). Given the interplay between soft and hard connectivity, this policy brief complements others in the series, which deal with digital infrastructures such as 5G technologies in greater detail.

**DATA CONNECTIVITY IN FOCUS – EUROPE AND ASIA**

Both the EU and many parts of Asia have made digital and data connectivity a priority under various bilateral and regional initiatives. The 2016 Master Plan on ASEAN Connectivity 2025 envisages a pan-ASEAN data-governance framework encompassing cross-border data transfers to improve data management among Association of South-East Asian Nations (ASEAN) members. As a first step, the plan recommends the mapping of data-management practices and approaches among ASEAN member nations. The Asia-Pacific Economic Cooperation-Cross-Border Privacy Rules (APEC-CBPR) system was established by APEC – a grouping of 21 member states including Japan, China, South Korea and the United States – and seeks to facilitate data flows among the participants through a government-backed voluntary certification mechanism. Certifications are issued to businesses upon compliance with the APEC Privacy Framework.

Another significant initiative is the concept of Data Free Flow with Trust (DFFT), championed by Japan as the host of the 2019 G20 summit in Osaka. The Osaka Leaders’ Declaration calls for respecting local and international legal frameworks, while promoting interoperability between them to enhance the free flow of data. In addition to Japan, around 24 countries and blocs – including China, the EU, South Korea, the US, Singapore, Thailand and Vietnam – have signed the declaration. Following the declaration, the G7 nations laid out a ‘G7 Roadmap for Cooperation on Data Free Flow with Trust’ – which was also endorsed by South Korea and Australia – for joint action in four key areas in 2021. These include identification of commonalities in regulatory approaches to cross-border data transfers, and building an evidence base on the impact of data localization measures and alternative policy responses to such measures. In addition to these regional or collective initiatives, various countries have also entered into bilateral free-trade agreements (FTAs). Examples include the Japan-India Comprehensive Economic Partnership Agreement and the EU-Japan Economic Partnership Agreement.

The EU, too, has taken several actions to enhance both regional and transcontinental connectivity. On the latter, the EU launched its EU-Asia Connectivity Strategy in 2018. Specific commitments to improve EU-Asia connectivity include efficient cross-border digital connection, bilateral, regional and international partnerships based on commonly agreed rules and standards, and sustainable finance. Following this, the EU also entered into bilateral Connectivity Partnerships with two Quad nations – Japan (in 2019) and India (in 2020) – and the ASEAN in 2020. On the side of hard connectivity, or the digital infrastructure that underpins cross-border data flows, more than one-hundred nations met at the Prague 5G Security Conference in 2019 to call for ‘trusted vendors’ in establishing 5G networks.

Furthermore, building on the EU-Asia Connectivity strategy and the bilateral connectivity agreements referred to above, the EU unveiled the Global Gateway initiative in 2021, earmarking €300 billion for investments around the world and with digital connectivity as one of its key priorities.

Clearly, and as visualized in Figure 1 and discussed in greater detail in subsequent sections, the landscape REGULATORY FRAMEWORKS

<table>
<thead>
<tr>
<th>Examples</th>
<th>Regulative Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is a global, legally binding agreement on cross-border data flows possible?</td>
<td>Multilateral</td>
</tr>
<tr>
<td>EU’s GDPR, APEC-CBPR system, Council of Europe’s Convention 108, and WTO’s Joint Statement Initiative on E-Commerce</td>
<td>Regional and plurilateral initiatives (binding)</td>
</tr>
<tr>
<td>Data Free Flow with Trust (G20 Osaka Track) and OECD Privacy Principles</td>
<td>Regional and plurilateral initiatives (non-binding)</td>
</tr>
<tr>
<td>EU-Japan FTA, EU-South Korea FTA, and Japan-India Comprehensive Economic Partnership Agreement (CEPA)</td>
<td>Bilateral arrangements</td>
</tr>
<tr>
<td>China’s Cyber Security Law, Japan’s Act on the Protection of Personal Information, South Korea’s Personal Information Protection Act, and India’s Data Protection Bill (in process)</td>
<td>National legal and regulatory frameworks</td>
</tr>
</tbody>
</table>

Figure 1: Fragmented landscape of national and international frameworks governing cross-border data flows

Source: Author’s own, for representational purposes only

---

5 AESCON was funded by the European Union, supported by the Asia-Europe Meeting, and organized by a consortium of think tanks in Europe and Asia, consisting of the Clingendael Institute (The Hague), the Kociuszko Institute (Kraków), Carnegie India (New Delhi), C21 (Bonn) and the Institute for Asian Studies (IAS/NU, Singapore). For details about the conference and videos of the various panel discussions, see www.aescon.org.
of national and international frameworks governing cross-border data flows remains fragmented and di-
verse, at varying levels. With an annual trade of €1.5 trillion, a combined contribution of 60 per cent of
global GDP, in addition to significant academic, cul-
tural and people-to-people linkages, both regions stand to gain considerably by bridging the trust defi-
cit and fragmentation of regulatory frameworks to create one of the world’s largest regions for seamless
transfer of data.

**TRUST IN CONNECTIVITY**

Unlike the General Data Protection Regulation (GDPR) in the EU, Asia has no common binding rules or stand-
ards that apply to the region as a whole for regulating data flows. While some Asian economies have put in
place a data-protection framework, others, including India, are still in various stages of enacting domestic
data-protection legislation. Few, like Afghanistan and Brunei Darussalam, simply do not have one. Some, as
noted, while there are parties to various international or regional frameworks, such as the OECD Privacy
Principles or the APEC Privacy Framework. For
instance, Australia, Japan, South Korea, Singapore, the Philippines and Taiwan are the only Asian partici-
pants in the latter.

Even among the G7 nations, which share democ-
raties of open and competitive markets, human rights and fundamental freedoms, approaches to
DFFT could differ. For instance, the EU seeks to imple-
ment rigorously data-protection measures under the
GDPR and adequacy decisions. Japan, in addition to con-
forming with the EU’s adequacy decision, also en-
genates in bilateral and regional trade agreements that
deal with data flows differently than the GDPR. Legal standards also differ. Asian countries largely share the overarching requirements for consent to be free, specific, informed and unambiguous - as is the case under the EU’s GDPR. But the standards or requirements could differ between countries. For in-
stance, while individual consent is a sufficient ground for transfer in Indonesia and Malaysia, India and China require prior regulatory approval, in addition to indi-
vidual consent, for specific types of data.7

As mentioned earlier, a key driver for contestations
around free flow of data is a lack of trust – for instance, on the adequacy or application of standards on data protection, privacy or international human rights, by other jurisdictions or private businesses. Another rea-
son - one that has been advanced by countries such as
India while arguing in favour of data localization8 - is the inability to access data for supervision and
law-enforcement purposes.9 Examples of data local-
ization mandates include the data localization direc-
tive issued by the Reserve Bank of India on financial
data in 2018, the draft Data Protection Bill (which in-
cluded a data localization mandate on personal data) that was awaiting passage in the Indian Parlia-
ment until recently, and the localization provisions in the
security-law of Vietnam.10 The EU, too, has soft localization mandates under the GDPR - that is,
cross-border data transfers are permitted subject to
compliance with conditions (unlike hard localization, which require local storage and prohibit transfers).
Economic motivations such as support to local indus-
try or employment have also been advanced for im-
posing restrictions on access and utilization of data by
countries like India.

These contestations are currently taking place in var-
ious forums, including among bilateral or regional
free-trade groupings, and at the World Trade Organiza-
(tion (WTO). At the WTO, while there has been progress
on the plurilateral Joint Statement Initiative (JSI) on
e-commerce, which was introduced by Australia, Japan and
Singapore, almost half of WTO members – mostly from
the developing world, led by India and South Afri-
ca - continue to stay out of the negotiations. Both India
and South Africa also refused to endorse DFFT. A key
reason for their refusal is that overarching global rules
may restrain their sovereign space to pursue domestic
objectives and policies, and fail to address existing in-
equities. For instance, India expressed its inability to
endorse DFFT on the basis that the concept was not well
understood, and that uninhibited data transfers fail to
address India’s concerns about access to data and the
exacerbation of the digital divide.11

Yet there are costs and consequences of such diverse and
divergent regulatory approaches and frameworks
on cross-border data flows. A fragmented governance
landscape imposes barriers to the movement of data
and enforcement of regulations, increases regulatory
complexity and uncertainty, and incurs costs on busi-
nesses and consumers. For example, several studies
measuring the impact of GDPR provisions find signif-
ificant costs associated with increased compliance,
especially for small and medium-sized enterprises, a
negative impact on firms’ productivity and employ-
ment, and a potential contraction of the EU’s GDP.
Another example is the estimated loss to India’s GDP
of up to 0.8 per cent of its domestic investments up
to 1.4 per cent because of data localization require-
ments.12

**CONVERGENCE FROM THE GROUND UP?**

Thus, a legally binding framework with common
standards and rules on cross-border or e-flows that
applies globally – or at least that encompasses the
EU and Asia – looks elusive at the moment. Yet there
may already be growing convergence or commonali-
ty, as representing the emergence of an international
architecture or architectures.13 One example of con-
vergence in legal provisions is the draft agreement of
the WTO’s JSI, which was released in 2020 and re-
stricts signatories’ ability to legislate domestically on
cross-border data flows, except for legitimate public
policy objectives and essential security interests. This provision is borrowed from regional trading agree-
ments such as the Comprehensive and Progressive
Agreement for Trans-Pacific Partnership (CPTPP) and
the Regional Comprehensive Economic Partnership
(RCEP). Adopting common legal texts across differ-
ent legal instruments helps to create similar, if not the
same, binding standards while clearly delineating so-
monic decision-making. In doing so, common legal texts
reduce the potential for conflicts or uncertainties in
regulatory frameworks. Although the EU is not a party
to RCEP or CPTPP, its support of the WTO JSI negoti-
ations could lend some familiar ground in relation to
the aforementioned regional trading agreements An-
other example of growing convergence in legal pro-
visions is the adoption of GDPR-like laws by 67 out of
120 non-EU countries as of 2018.14 Assessing the eco-
nomic costs and a state’s capacity for implementation
would, however, be key for the reasons discussed in
the previous section.

Beyond the adoption of common legal texts, there also exist interoperability mechanisms that aim to ease
cross-border data flows. Examples include the recent
adequacy decisions issued under the EU’s GDPR in fa-
vour of Japan and South Korea, and the certifications
issued under the APEC-CBPR system. Japan, too, has
issued an equivalency decision under its Act on the
Protection of Personal Information in favour of the EU.
In the absence of common standards and rules, such
interoperability mechanisms help countries to estab-

---

9 For a discussion on arguments advanced in relation to data localization, see Rishab Bailey and Smriti Parsheera, ‘Data localization mandates in existence, and most operate as regular conditions applicable to data flows, typically in relation to privacy.
11 The EU, too, has soft localization mandates under the GDPR - that is, cross-border data transfers are permitted subject to compliance with conditions (unlike hard localization, which require local storage and prohibit transfers).
12 Another example is the estimated loss to India’s GDP of up to 0.8 per cent of its domestic investments up to 1.4 per cent because of data localization requirements.
15 Rudra Chaudhuri, Fragmentation, the future geopolitics of data, Carnegie India, March 2022.
lish the necessary trust to allow data to flow across their borders. Japan could be an interesting example. Its domestic framework allows the flexibility to comply with both the GDPR, through the adequacy decision, and the APEC–CPBR system - both of which follow different approaches. Japan has also proposed DFFT and is party to various bilateral and regional trade agreements. How Japan navigates this diverse, binding and non-binding regulatory landscape going forward could prove to be an interesting case study for other countries.

**LOOKING AHEAD**

**Actionable steps:**

- Undertake a detailed mapping of regulatory frameworks highlighting commonalities, compliances, and local nuances and imperatives driving Asian countries, for future discussions and policy-making. The ASEM Asia–Europe Business Forum or the ASEM Economic Ministers’ Meeting could take the lead on this exercise.
- Evaluate the impact of regulatory tools such as adequacy decisions and data localization, and possible alternatives.
- Hold multistakeholder negotiations on the plurilateral e-commerce initiative at the WTO, which includes countries that have expressed reservations.
- In the immediate to short term, pursue interoperable frameworks such as certifications or adequacy decisions.
- Pursue a holistic approach to policy that encompasses both hard and soft digital connectivity.

Given the fragmentation of the regulatory landscape as discussed above, a detailed mapping of regulatory frameworks on cross-border data flows across the EU and Asia to identify commonalities could be useful. This could be particularly helpful in the context of Asia since, unlike the EU, which is represented by a single legislation (that is, the GDPR), Asia comprises countries and regional or geopolitical groupings with diverse interests, objectives and approaches to data governance.

This exercise could also map the interests, concerns and motivations driving the Asian countries, in order to offer a better understanding of local nuances and imperatives. In addition to forming the basis for discussions and future policy-making on common or interoperable frameworks, it could also help to clarify and ease compliance burdens. The ASEM Asia–Europe Business Forum or the ASEM Economic Ministers’ Meeting could perhaps take the lead on this exercise. An evaluation of the impact of regulatory mechanisms and restrictions such as adequacy decisions and data localization measures, and possible alternatives, would also be useful. For instance, localization mandates for law-enforcement objectives may be unnecessary if effective mechanisms replace the cumbersome processes such as today’s Mutual Legal Assistance Treaties (MLATs). This exercise could be particularly relevant, as the UNCTAD Report finds that current literature on cross-border data flows is framed around data as an economic resource, ignoring the non-economic dimensions, and is largely produced by the developed world. It also finds little hard evidence to support both extremes – that is, uninhibited data flows and hard localization of data. All of this calls for a dispassionate and balanced approach that addresses national priorities as well as the current inequities in distribution of gains from cross-border data flows.

Next, as a global multilateral forum, negotiations at the WTO on the JSI could prove to be an essential platform to prevent a fragmented landscape - particularly for developing countries, as all WTO members have veto powers. Given the largely plurilateral nature of the JSI at present, however, future efforts should prioritize and involve discussions with all stakeholders, especially the (developing) countries that have opted to remain outside the negotiations, and their civil society organizations. Such negotiations should respect the strategic interests and regulatory values of members, and avoid corporate capture at both the domestic and international levels. Moreover, any competition or divergence on digital trade (including cross-border data flows) must not derail coordination on other important matters, such as the security of supply chains through coalitions like the Quadrilateral Dialogue, or on technical standards through forums such as the Global Partnership on Artificial Intelligence. Additionally, ‘soft law’ provisions - that is, provisions that endeavour to hold non-binding regulatory consultations among national regulators – can also be considered in parallel on a range of issues involving digital trade, but not necessarily incorporated in the binding rules, such as privacy, to promote trust.

In the immediate to short term, however, given the fragmentation, interoperability mechanisms between different governance regimes, such as certifications or adequacy decisions, could be pursued. Finally, given the link between hard and soft digital connectivity, a holistic policy approach that encompass both would be essential to ensure that challenges associated with the former do not exacerbate those associated with the latter. Further, considering the digital and data divide, such an approach may also help developing countries to create the necessary capacity to participate in the digital economy and thus reap the associated gains.
ABOUT THE AUTHOR

Priyadarshini D is an Associate Fellow with the Technology and Society Program at the Carnegie Endowment for International Peace, India. Her research focuses on emerging issues at the intersection of law, technology, and finance. Carnegie does not take institutional positions on public policy issues; hence, the views represented herein are those of the author and do not necessarily reflect the views of Carnegie, its staff, or its trustees.

ABOUT THE AESCON POLICY BRIEF SERIES

This Policy Brief is one of a series that sprung from the Asia-Europe Sustainable Connectivity (AESCON) conference held from 22-24 March 2022. The five Policy Briefs present the main findings and policy recommendations from the various AESCON panels. The series is edited by Maaike Okano-Heijmans and Brigitte Dekker of the Clingendael Institute, and includes the following pieces:

▶ Multistakeholderism: the path to human-centred digital connectivity, by Maaike Okano-Heijmans and Vanshika Shah of the Clingendael Institute, The Hague

▶ Secure and resilient digital infrastructure: an agenda for Europe and Asia, by Michał Rakowski of the Kosciuszko Institute, Krakow

▶ Putting trust back in trusted connectivity: a call for more congruence in cross-border data transfers, by Priyadarshini D of Carnegie India, New Delhi

▶ Digital connectivity and opportunities for development cooperation between Asia and Europe, by Fabian Hohmann, Christina Stansell, Antonia Stock and Elisabeth Cager of the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), Bonn

▶ Linking digital trajectories: Asia and Europe’s opportunities in the digital economy, by Karthik Nachiappan of the Institute of South Asian Studies, Singapore