



GLOBAL DATA ALLIANCE

**PRESENTATION TO OECD
CDEP DRAFTING GROUP ON
TRUSTED GOVERNMENT
ACCESS TO DATA**



OVERVIEW

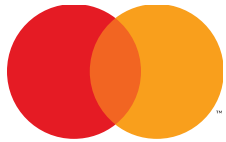
- Introductions
- About Cross-Border Data Transfers
- Digital Trade Restrictions, including Data Localization Requirements & Data Transfer Regulations
- Rationales for Data Localization Requirements & Data Transfer Regulations
- Int'l Agmts and Negotiations re Data Transfers

ABOUT THE GLOBAL DATA ALLIANCE

- The Global Data Alliance is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the transfer of data around the world to innovate and create jobs.
- Amid rising digital protectionism, a multi-sector voice is needed to support sensible and responsible cross-border data policies around the world.
- The Global Data Alliance provides that voice.
- Administered by BSA | The Software Alliance, the Global Data Alliance supports policies that help instill trust in the digital economy.

GDA MEMBERS

Global Data Alliance members include [BSA members](#) and the following:





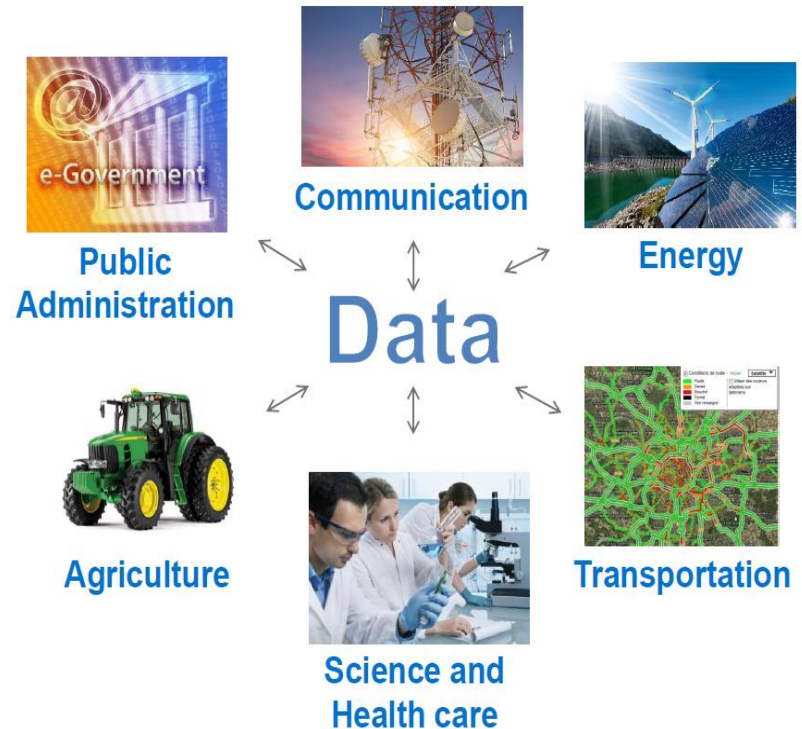
About Data & Data Transfers

ABOUT DATA & DATA TRANSFERS

- What is a Data Transfer?

- “Cross-border data transfers” refer to the movement or transfer of information across IT networks.
- Companies of all sizes rely on data transfers.
- This includes companies with int’l customers or operations.
 - Any communication to a person / device in another country
 - Financial transactions
 - R&D collaboration
 - M2M and IOT transactions

- In all sectors — from farming, fisheries, and mining; to aviation, hospitality and other services; to the manufacturing industries, data transfers are critical to innovation, job creation, and productivity, safety, and environmental responsibility.



ABOUT DATA & DATA TRANSFERS

Data Transfers are Critical to:



A country's global connectivity and its access to the international marketplace and supply chains;



The ability of companies of all sizes to use software-enabled technologies, including cloud computing, data analytics, and digitally connected industrial processes, to create jobs, boost productivity, and reach new markets; and



The workforce's ability to remain productive through teleworking, virtual collaboration, and online training, as well as remotely delivered health care and other services.

The protection of privacy, security, and regulatory compliance.

- In finance, the ability to transfer and analyze data in real-time across borders is critical to efforts to combat financial fraud, money laundering, or other illicit financial transactions.
- In cybersecurity, global access to real-time data are necessary to monitor traffic patterns, identify anomalies, and divert of potential threats.
- In IP and other criminal enforcement, data transfers are critical to developing insights on source countries, distribution hubs and networks, and end-user markets, implicated in the distribution of dangerous or adulterated counterfeit products, commercial scale piracy, and other illicit activities.

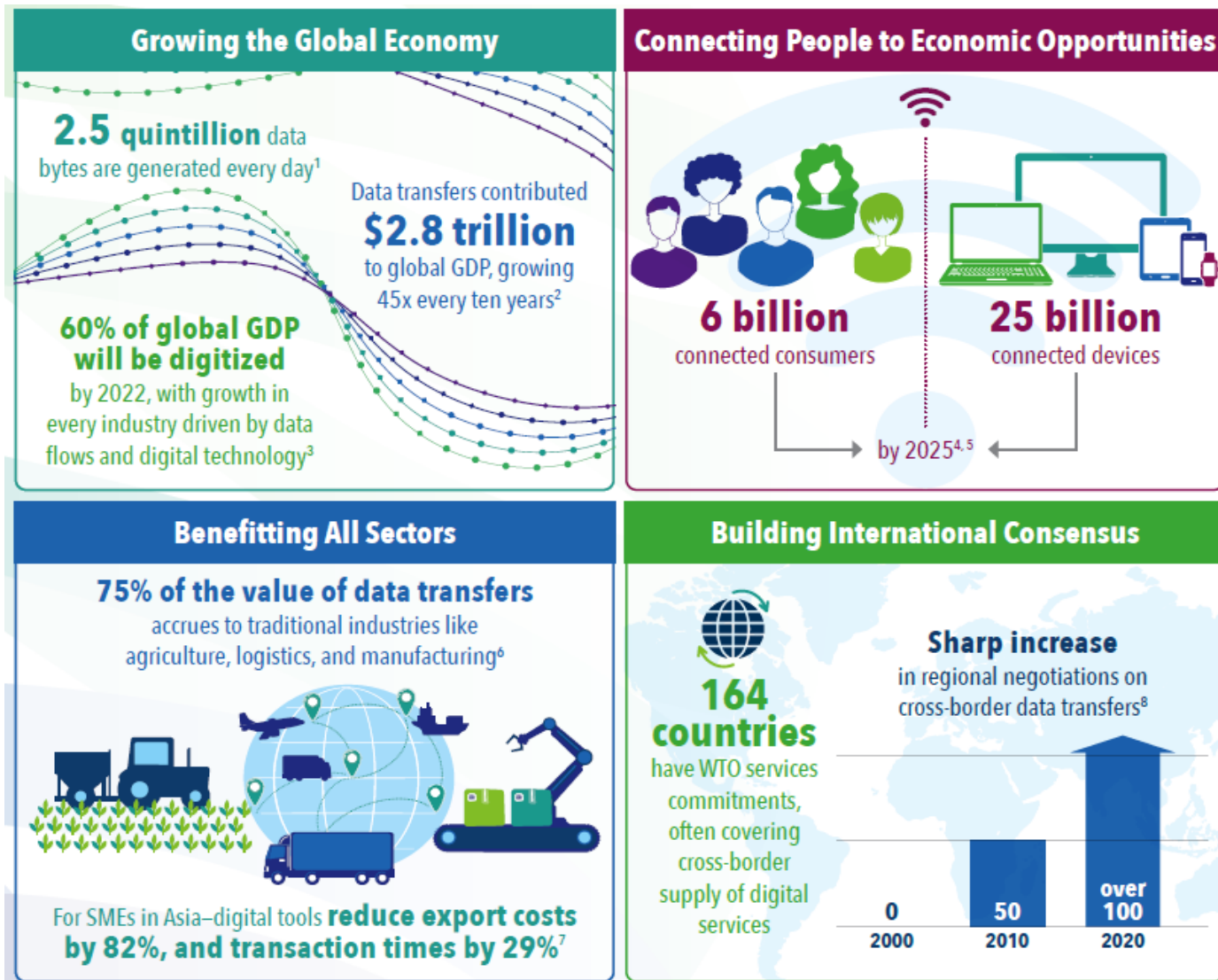
ABOUT DATA & DATA TRANSFERS

Data Transfers are Critical to:

- Research and development (R&D) and innovation. R&D depends upon access to globally sourced research data from laboratories across the world, as well as collaboration, joint research, and the exchange of ideas and knowledge among teams of inventors, designers, authors, and other creators and innovators in different countries.
- Artificial intelligence-based innovation, which depends upon analysis of data sets consolidated across borders to identify insights and patterns that can aid R&D teams in the development of novel solutions to scientific and technical challenges.
- Safety testing and marketing licensing / approvals for new aircraft, vehicles, medical devices, machine tools, and robotics, etc.
- Operation, servicing and support of such connected devices, which often depend upon satellite or other cross-border data communications (e.g., IoT software applications in the aerospace, automotive, and agricultural machinery sectors) for their operation.

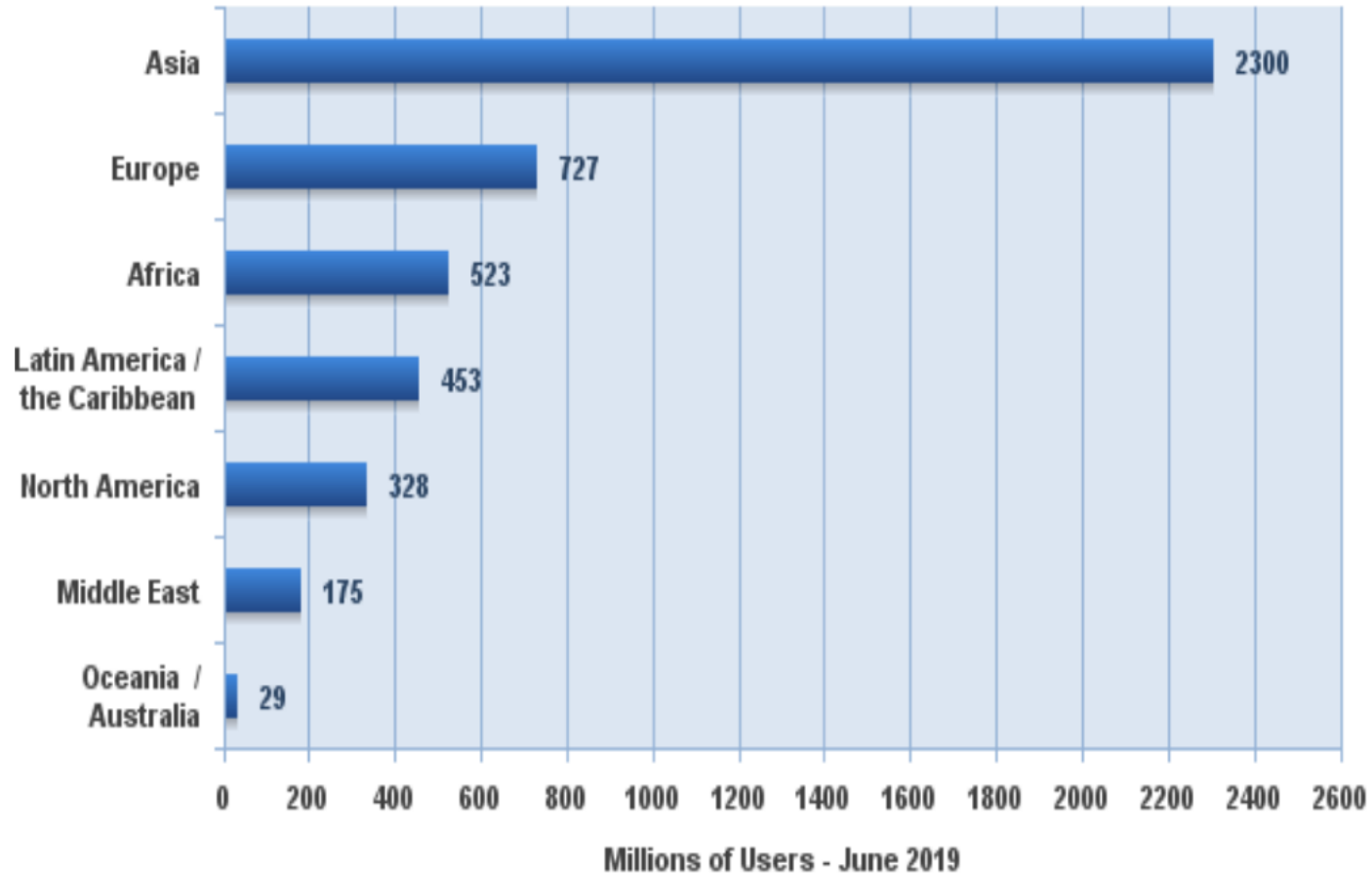
ABOUT DATA & DATA TRANSFERS

Cross-border Data Transfers – Facts & Figures



ABOUT DATA & DATA TRANSFERS

Internet Users in the World by Geographic Regions - Mid-Year 2019



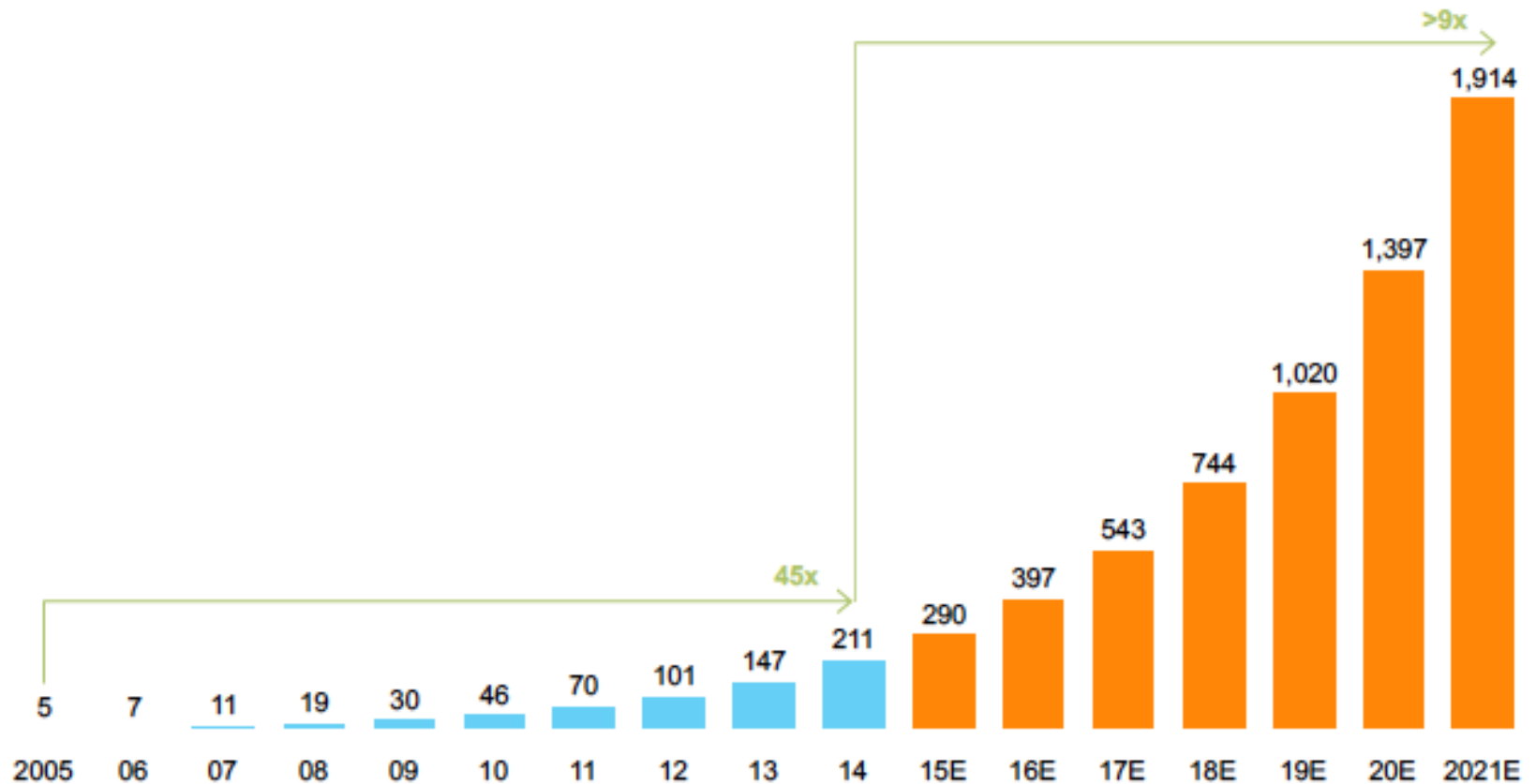
Source: Internet World Stats – www.internetworldstats.com/stats.html

ABOUT DATA & DATA TRANSFERS

Cross-border bandwidth has grown 45 times larger over the past decade—and may grow another nine times larger by 2021

Used cross-border bandwidth, global
Terabits per second

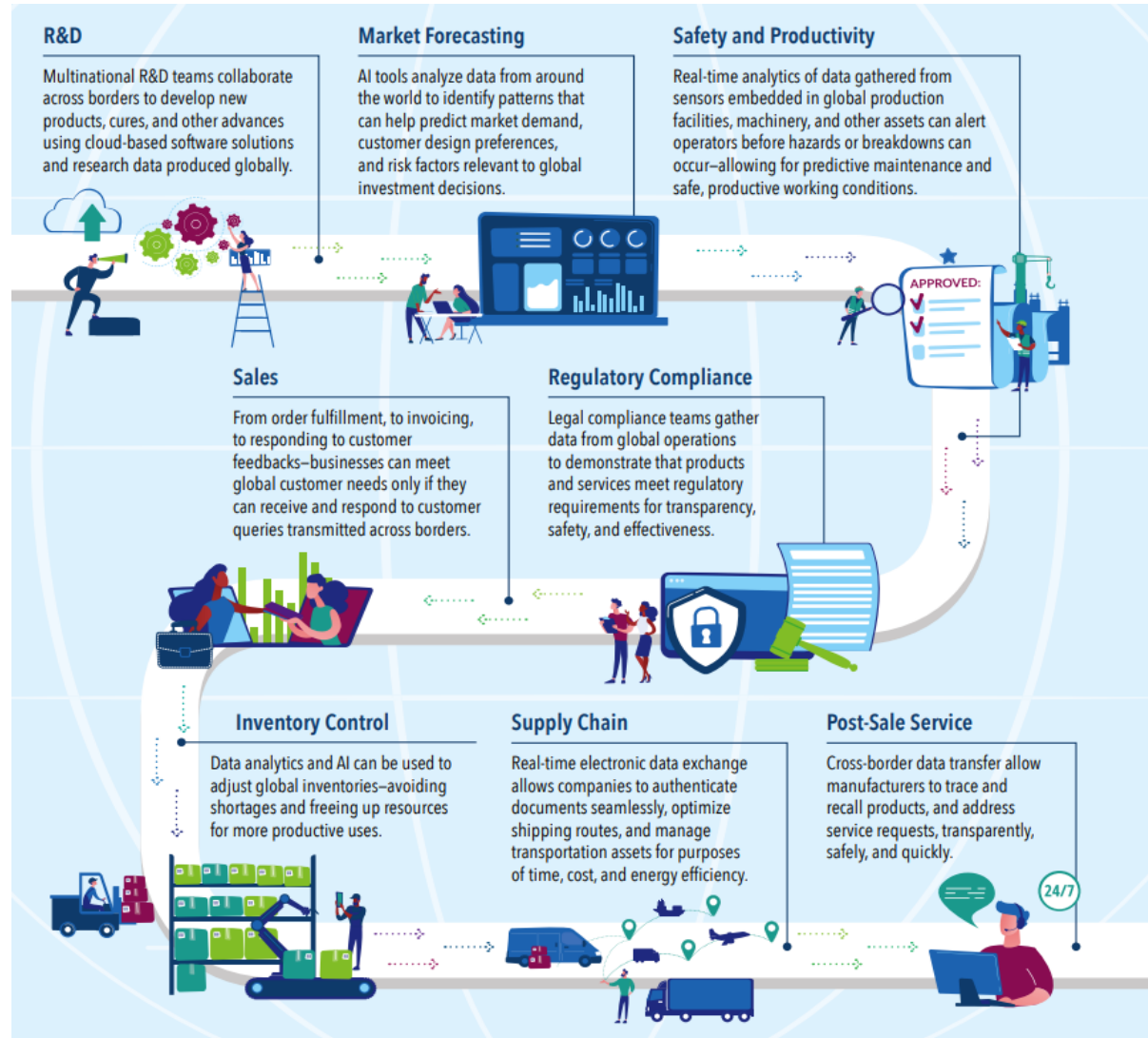
Actual Forecast



Source: Telegeography – McKinsey Global Institute Analysis

ABOUT DATA & DATA TRANSFERS

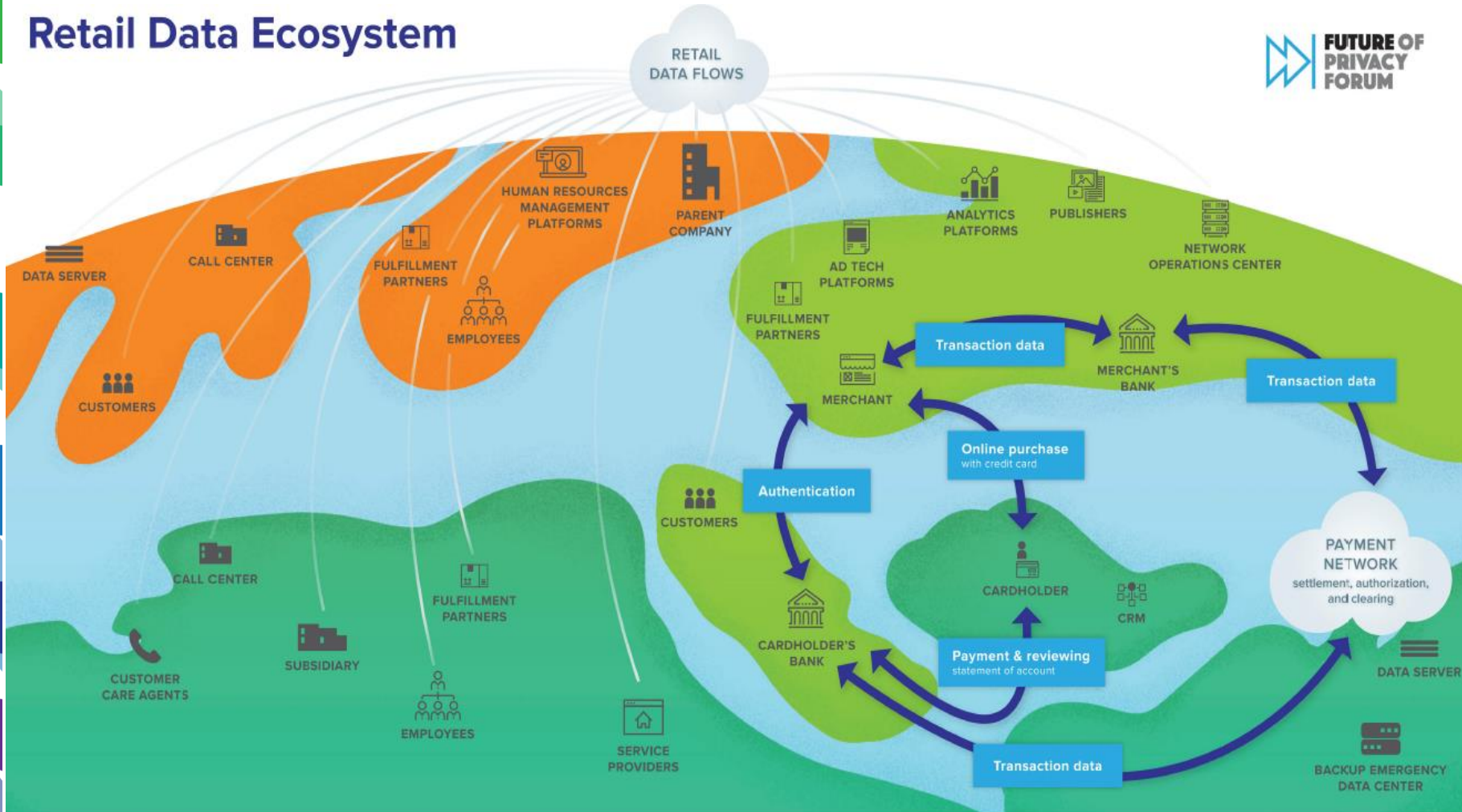
Data Transfers at Every Stage of the Value Chain



ABOUT DATA & DATA TRANSFERS

Data Transfers in the Retail Supply Chain

Retail Data Ecosystem





Data Localization Requirements

Data Transfer Restrictions

DATA LOCALIZATION MANDATES

DATA TRANSFER RESTRICTIONS

- National policies on cross-border data transfers and data localization are – alongside economic profile, level of internet and broadband access, and level of computer literacy – important determinants of the ability of economies to realize the promise of the digital 21st century and to respond effectively to the economic impacts of the COVID-19 pandemic.
- The types of cross-border data policies that can undermine that ability take many forms.
 - Some policies expressly require data to stay in-country.
 - Some policies impose unreasonable conditions on sending data abroad or prohibit such transfers outright.
 - Some policies require the use of domestic data centers or other equipment, or the need for such data centers to be operated by local vendors.

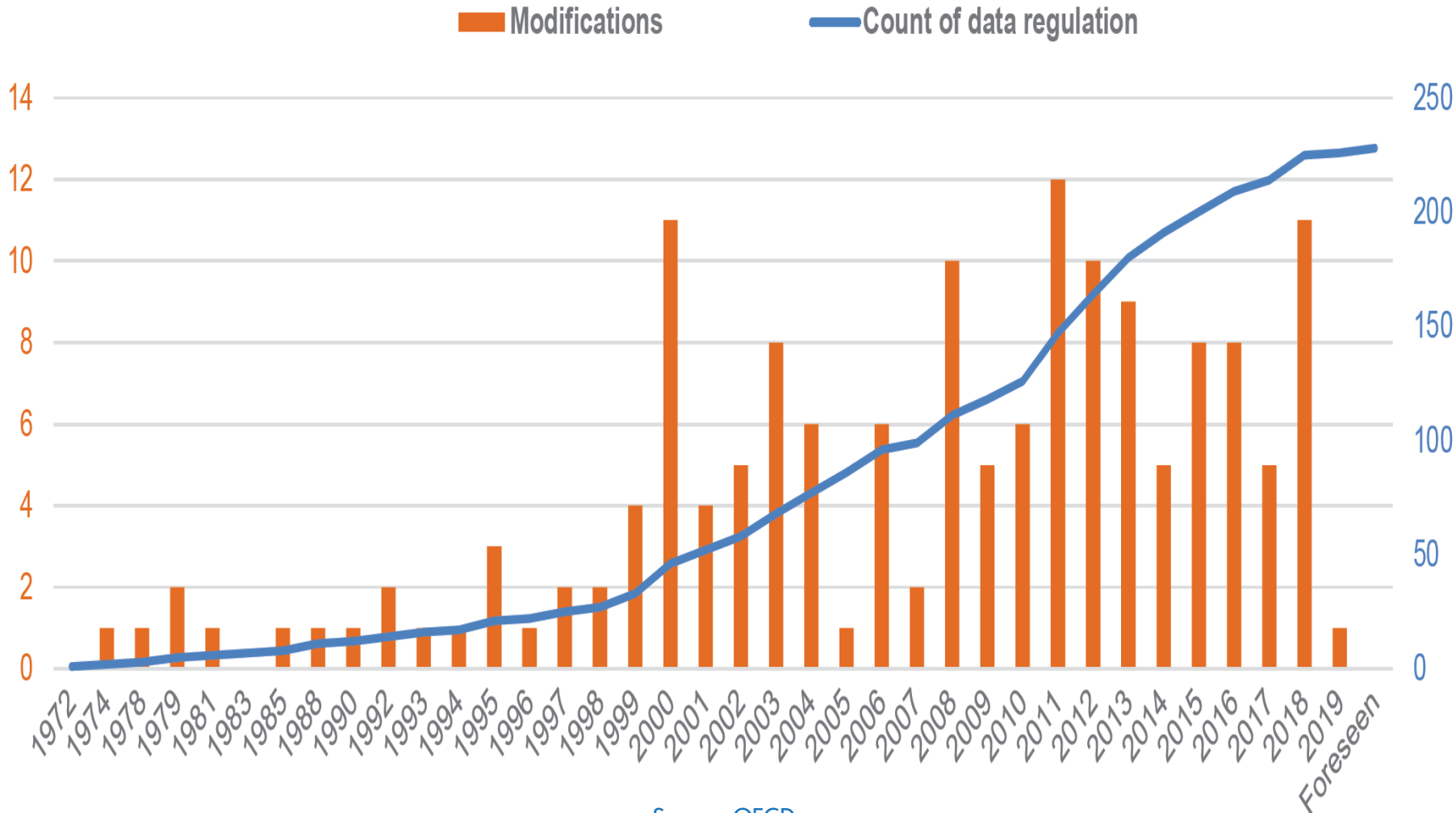
DATA LOCALIZATION MANDATES

DATA TRANSFER RESTRICTIONS

- Some measures cite privacy, security, or regulatory access as their underlying purpose, but often the measures are designed in a manner that also suggests alternative, protectionist purposes. For example, these measures may:
 - Reflect a choice of policy tools that are significantly more trade-restrictive than necessary to achieve the stated public policy goal;
 - Constitute unnecessary, unjustified and/or disguised restrictions on data transfers across borders, or may be more restrictive of data transfers than necessary; or
 - Treat cross-border data transfers less favorably than domestic data transfers.

DATA LOCALIZATION MANDATES DATA TRANSFER RESTRICTIONS

- Data regulations have grown by over 800% since 1995.

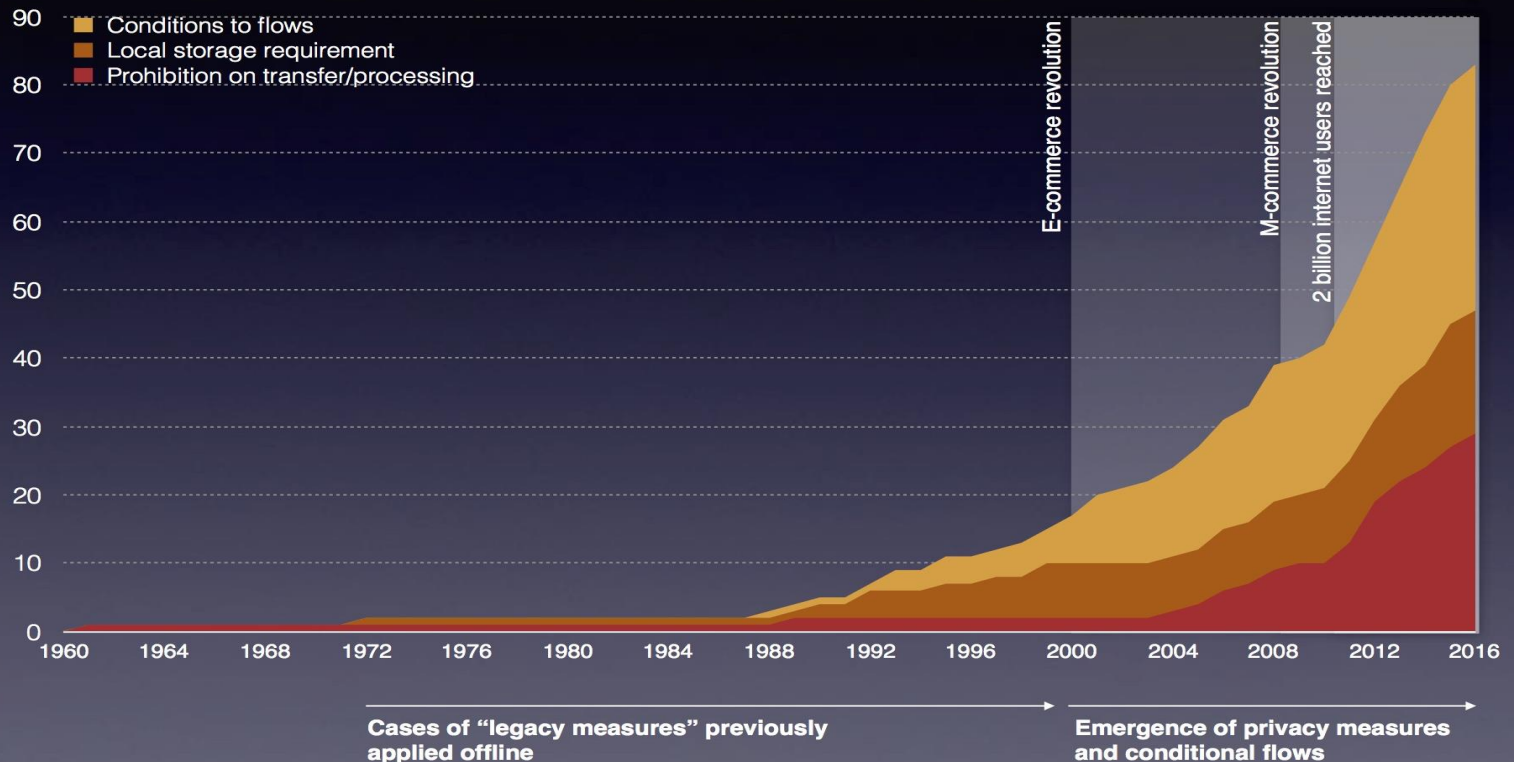


Source: OECD

DATA LOCALIZATION MANDATES DATA TRANSFER RESTRICTIONS

Localization mandates and transfer restrictions comprise the bulk of data regulations

Data localisation and data restriction measures in the world are increasing



DATA LOCALIZATION MANDATES

DATA TRANSFER RESTRICTIONS

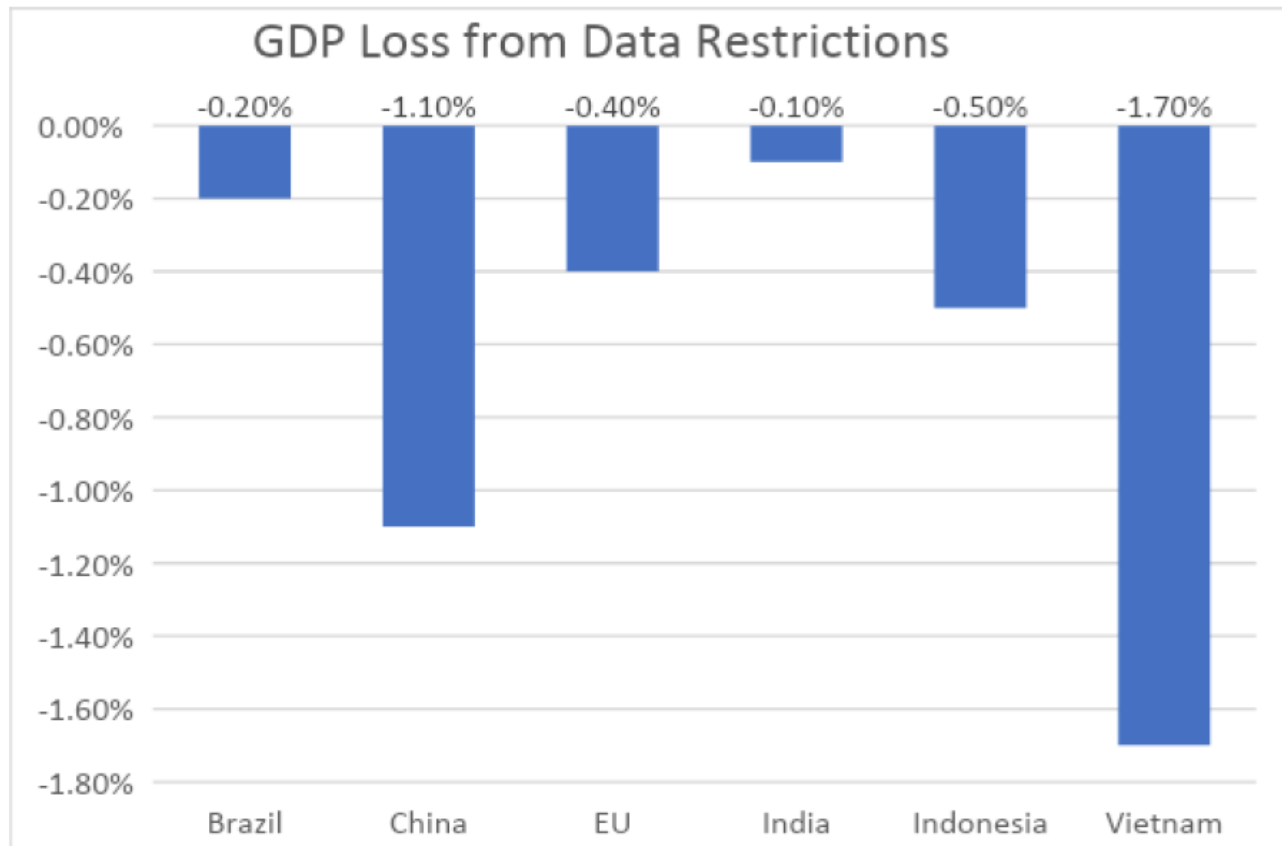
Economic Costs of Data Localization and Data Transfer Restrictions

- A 2021 GSMA study conducted in three developing regions (in South America, South-East Asia and Africa) indicates that data localization measures on IoT applications and M2M data could result in:
 - 59-68% of their productivity and revenue gains;
 - Investment losses ranging from \$4-5 billion;
 - Job losses ranging from 182,000-372,000 jobs.
- The World Bank's 2020 World Development Report found that, "restrictions on data flows have large negative consequences on the productivity of local companies using digital technologies and especially on trade in services."
 - "Countries would gain on average about 4.5 percent in productivity if they removed their restrictive data policies, whereas the benefits of reducing data restrictions on trade in services would on average be about 5 percent."
- A 2020 World Economic Forum study found that, "approximately half of cross-border [services] trade is enabled by digital connectivity[, which] ... has allowed developing countries and micro, small and medium-sized enterprises (MSMEs) to export through greater visibility, easier market access and less costly distribution."
 - "Developing countries ... accounted for 29.7% of services exports in 2019."
- 2019 AlphaBeta Study estimates that digital tools helped MSMEs across Asia reduce export costs by 82% and transaction times by 29%

DATA LOCALIZATION MANDATES DATA TRANSFER RESTRICTIONS

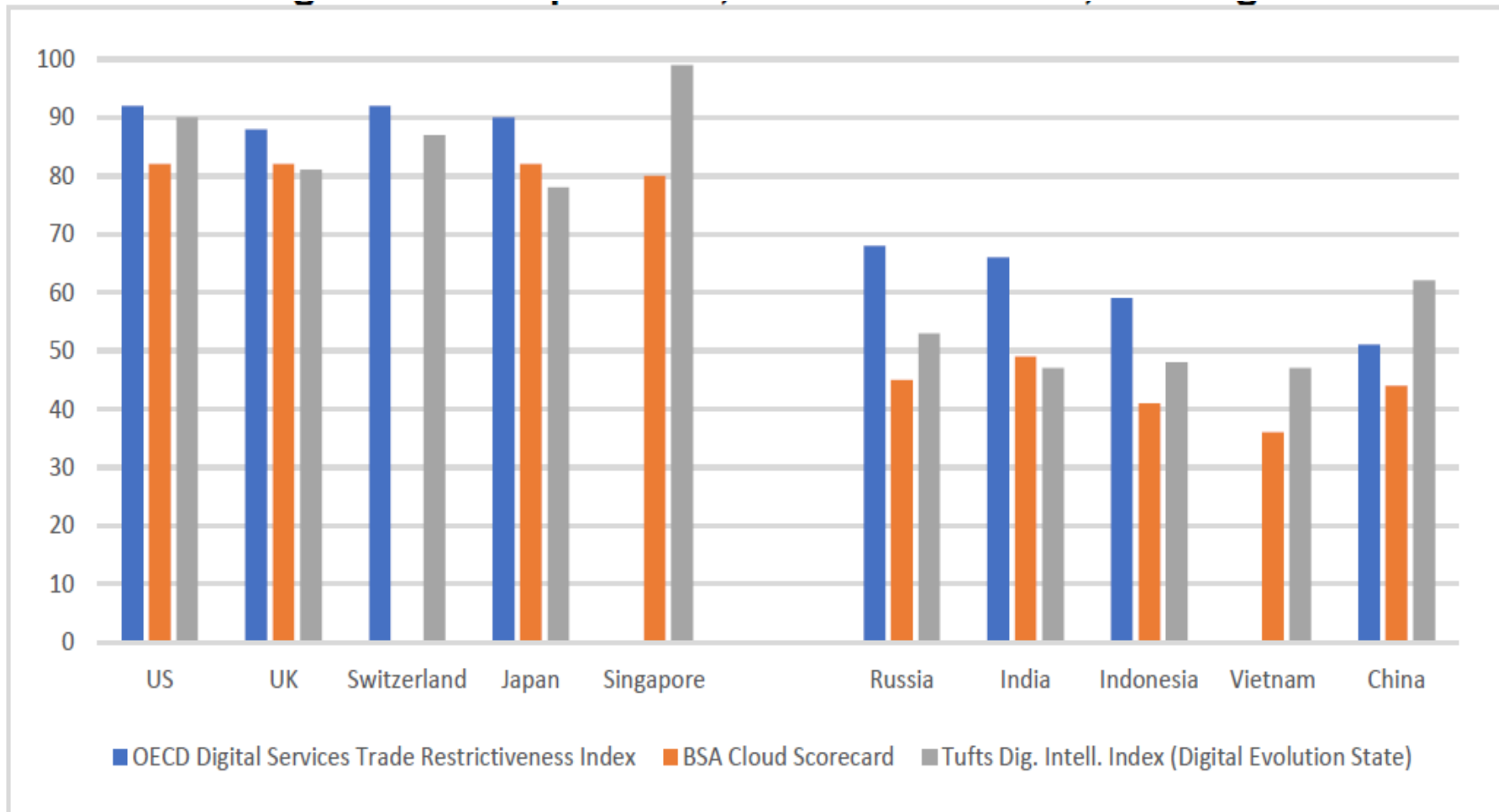
Economic Costs of Data Localization and Data Transfer Restrictions

- Cross-border data restrictions or localization mandates limit the GDP and economic opportunities, according to an ECIPE study.



DATA LOCALIZATION MANDATES DATA TRANSFER RESTRICTIONS

- Measures of digital trade openness



DATA LOCALIZATION MANDATES

DATA TRANSFER RESTRICTIONS

Examples of Data Localization and Data Transfer Restrictions

Some markets, including China, Egypt, India, Indonesia, Nigeria, Pakistan, Russia, Saudi Arabia, South Korea, UAE, and Vietnam, have adopted, or have proposed, significant data-related restrictions.

- Among several Chinese measures that restrict the ability to transfer data across borders, the draft 2017 Critical Information Infrastructure Protection regulations — as further elaborated in 2020 guidelines — would effectively require all cloud computing services providers (CSPs) to store data in-country. China's draft Personal Information Protection Law appears to contain stricter data localization requirements and data transfer restrictions than even China's 2017 Cybersecurity Law.
- India has imposed data localization requirements, including through India's Directive on Storage of Payment System Data issued by the Reserve Bank of India in 2018, which imposes data and infrastructure localization requirements. India has also proposed stringent localization and transfer restrictions in its draft Personal Data Protection Bill, and Non-Personal Data Governance Framework.
- South Korea's Cloud Security Assurance Program (CSAP) requires use of local data centers for a broad range of cloud services.
- The proposed implementation regulation for Indonesia's Government Regulation 71/2019 and OJK Regulation 13/2020 contains data localization requirements.
- Vietnam's 2018 Cybersecurity Law and draft implementing regulations impose data localization requirements.
- Egypt, Nigeria, Pakistan, Saudi Arabia and UAE, each issued measures or proposals that raise questions from a cross-border data policy perspective.
- A range of EU measures also impact cross-border data flows with third countries.

DATA-RELATED MEASURES (NOT ALL RESTRICTIVE)

- **Australia**
 - [Senate Select Committee on Financial Technology and Regulatory Technology](#)
 - [Privacy Act Review](#)
- **Brazil**
 - Implementation of Data Transfer Provisions in [Brazilian General Data Protection Law](#) (LGPD)
 - Guidelines on Government Procurement of Cloud Services
 - National Cybersecurity Strategy
- **Canada**
 - [Personal Information Protection and Electronic Documents Acts](#)
- **China**
 - [Cybersecurity Law](#)
 - [Cybersecurity Classified Protection Scheme](#)
 - [Guiding Opinions on Implementing CCPS and CII Protection Scheme](#)
 - [Administrative Measures for the Multi-level Protection Scheme of Information Security](#)
 - [Data Security Law](#)
 - [Personal Information Protection Law](#) (draft)
 - [Global Data Security Initiative](#)
 - [Unreliable Entities List Regulation](#)
- **Egypt**
 - [Data Protection Law](#) (summary)
- **EU**
 - [EU Data Strategy](#)
 - [EU Trade Policy Review](#)
 - [European Court of Justice Ruling On “Schrems II”](#)
 - [EDPB Recommendations on Supplementary Measures](#)
- **India**
 - [Personal Data Protection Bill](#)
 - National E-Commerce Policy
 - Non-Personal Data Governance Framework
 - [Directive on Storage of Payment System Data](#)
 - [Data Security Council of India Annual Report](#) (Working Group on Cloud Computing)
 - [National Telecom M2M Roadmap](#)
 - [Guidelines for Government Departments On Contractual Terms Related to Cloud Services](#)
 - National Cybersecurity Strategy
- **Indonesia**
 - Regulation 71 on Operation of Electronic Systems
 - Personal Data Protection Bill
 - E-Commerce Regulation
- **Japan**
 - [Amended Act on the Protection of Personal Information \(APPI\)](#)
- **Mexico**
 - [Use of Cloud Computing Services by Electronic Payment Funds](#)
- **Nigeria**
 - [Draft Data Protection Bill](#)
- **Pakistan**
 - [Personal Data Protection Bill](#)
- **Saudi Arabia**
 - [Cloud Computing Regulatory Framework](#)
 - [IoT Regulatory Framework](#)
 - [National Data Governance Interim Regulations](#)
- **South Korea**
 - [Act on the Development of Cloud Computing and Protection of its Users](#)
 - [Cloud Security Assurance Program](#)
 - [Regulation on Supervision of Electronic Financial Transactions](#)
 - [Credit Information and Protection Act](#)
 - [Personal Information Protection Act](#)
 - [Act on Promotion of Information and Communication Network Utilization and Information Protection \(Network Act\)](#)
- **United Arab Emirates**
 - Draft Retail Payment Services Regulations
- **United Kingdom**
 - [UK National Data Strategy](#)
 - [UK Telecom Security Bill](#)
- **United States**
 - [National Trade Estimate of Foreign Trade Barriers](#) (Section 181 of the Trade Act of 1974)
 - [Trade Promotion Authority](#)
- **Vietnam**
 - [Cybersecurity Law](#) and implementing regulations
 - [Personal Data Protection Draft Decree](#)



Rationale for Data Localization and Data Transfer Restrictions

RATIONALES CITED FOR DATA LOCALIZATION MANDATES & TRANSFER RESTRICTIONS

Several grounds are frequently cited as the basis for imposing data restrictions.

- **Security:** Some argue that localization and data transfer restrictions are necessary to ensure cybersecurity. Such restrictions often undermine security.
 - Cross-border data transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data.
 - Companies may choose to store data at geographically diverse locations to reduce risk of physical attacks, to enable companies to reduce network latency, and to maintain redundancy and resilience for critical data in the wake of physical damage to a storage location.
 - How data is protected is much more important to security than where it is stored.
- **Privacy:** Some argue that these restrictions are necessary to protect privacy – i.e., to ensure that companies process and use data consistent with a country’s data protection laws. This is not the case.
 - Organizations that transfer data globally typically implement procedures to ensure that the data is protected even when transferred outside of the country. These may include, where relevant, adequacy decisions, certifications, codes of conduct, Binding Corporate Rules (BCRs), and Standard Contractual Clauses (SCCs).
 - Where differences exist among data protection regimes, governments should create interoperability mechanisms to bridge those gaps in ways that both protect privacy and facilitate global data transfers, taking into account widely accepted privacy principles and industry best practices.

RATIONALES CITED FOR DATA LOCALIZATION MANDATES & TRANSFER RESTRICTIONS

- **Government Access:** Some claim that data localization and data transfer restrictions are necessary to ensure that regulators and law enforcement authorities have access to data relevant to conduct investigations.
 - The location of the data, however, is not the determining factor.
 - Responsible service providers work to respond to lawful requests for data consistent with their obligations to their customers and to protect consumer privacy.
 - If the service provider has a conflicting legal obligation not to disclose data, law enforcement authorities have several options: International agreements — including Mutual Legal Assistance Treaties (MLATs) or Agreements (MLAAs), multilateral treaties, and other agreements, such as those authorized by the United States Clarifying Lawful Overseas Use of Data (CLOUD) Act — can establish foundations for mutual legal assistance and reciprocal transfers of law enforcement data.
 - Courts may also issue requests to authorities abroad for the transfer of data through letters rogatory.
- **Data Sovereignty / Data Mercantilism / Digital Protectionism:** Policies associated with both data-related trade barriers and other domestic preferences or measures discriminating against foreign products, services, enterprises or technologies.
 - Data mercantilism is premised upon the view that cross-border data restrictions or data localization mandates offer protectionist economic benefits.
 - Such policies may be grounded in assumptions that cross-border data restrictions and data localization measures will foster the creation of jobs and “local champion” enterprises, and increased domestic innovation, investment, and GDP growth. However, these assumptions are not supported by economic evidence.
 - This premise is refuted by extensive economic evidence. (See slides above).



Int'l Agreements & Negotiations re Data Transfers

INT'L NEGOTIATIONS RELATING TO DATA TRANSFERS

- *GDA Cross Border Data Policy Principles*

PRINCIPLE 1

Countries should maintain the longstanding presumption favoring the seamless and responsible movement of data across borders

PRINCIPLE 2

Any rules impacting cross-border data transfers should be developed and maintained in accordance with good regulatory practices

PRINCIPLE 3

Any rules impacting cross-border data transfers should be non-discriminatory

PRINCIPLE 4

Any rules impacting cross-border data transfers should be necessary to achieve a legitimate objective and not impose greater restrictions than necessary

PRINCIPLE 5

Countries should support the use of accountability models aligned with international best practices to foster responsible data transfer practices

PRINCIPLE 6

Countries should work together to create trust-based frameworks that are interoperable and support the seamless and responsible movement of information across borders

INT'L NEGOTIATIONS RELATING TO DATA TRANSFERS

GDA Backgrounder on Int'l Data Negotiations

APEC

- Cross-Border Privacy Rules System (CBPRs)
- Digital "Post-2020 Vision"
- Internet and Digital Economy Roadmap
- Privacy Framework

Australia

- Australia-Singapore Digital Economy Agreement (DEA)
- Australia-EU trade negotiations
- Australia-Kong Kong FTA

Brazil

- EU-MERCOSUR trade negotiations

CPTPP

- Comprehensive and Progressive Agreement for Trans-Pacific Partnership

European Union

- EU adequacy (EU-US, EU-Canada, EU-Japan, EU-UK)
- EU trade negotiations (EU-Thailand, EU-Indonesia, EU-UK, EU-New Zealand, EU-Australia)

Japan

- Japan-US Digital Trade Agreement (DTA)
- Japan-UK Comprehensive Economic Partnership Agreement (CEPA)

OECD

- OECD Privacy Framework Review
- OECD Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

Singapore

- Digital Economy Partnership Agreement (DEPA)
- Singapore-Australia Economic Partnership Agreement
- Singapore-Korea trade negotiations

United Kingdom

- UK-Japan CEPA
- UK-Australia trade negotiations
- UK-EU trade negotiations
- UK-New Zealand trade negotiations
- UK-United States trade negotiations

United States

- United States-Mexico-Canada Agreement (USMCA)
- US-Japan Digital Trade Agreement
- US-Kenya trade negotiations
- US-UK trade negotiations
- US-Singapore Joint Statement on Financial Services Connectivity
- US Trade & Investment Framework Agreement talks

World Trade Organization

- WTO Joint Statement Initiative on Electronic Commerce and Digital Trade

Other Negotiations and Agreements

- Regional Comprehensive Economic Partnership
- The Pacific Alliance
- The African Continental Free Trade Area
- G7 Workstreams on Data Governance and Cross-Border Data Flow
- G20 Workstreams on Trade and Digital Economy

INT'L NEGOTIATIONS RELATING TO DATA TRANSFERS

- GDA Dashboard of Trade Rules on Data Transfers

● Yes ● No ● In Part

	CPTPP (AU, BN, CA, CL, JP, MY, MX, NZ, PE, SG, VN)	US-Mexico- Canada Agreement	Japan-US Digital Trade Agreement	Digital Economy Partnership Agreement (CL, SG, NZ)	Australia-Hong Kong FTA
Core Discipline: Contains affirmative disciplines on data transfer restrictions and data localization mandates	●	●	●	● ¹	●
Treatment of Exceptions: <i>Permissible derogations limited to measures that:</i>					
(1) <i>are necessary to achieve a legitimate public policy objective</i>	●	●	●	●	●
(2) <i>are not applied in a manner that would result in arbitrary or unjustifiable discrimination or a disguised restriction on trade</i>	●	●	●	●	●
(3) <i>do not impose transfer restrictions greater than necessary</i>	●	●	●	●	●
Prohibits Discrimination against Cross Border Data Transfers²	●	●	●	●	●
Coverage of Personal Data Transfers	●	●	●	●	●
Coverage of Non-personal Data Transfers	●	●	●	●	●
Coverage of Financial Services	● ³	●	●	●	●
Limits on Exceptions Premised on Privacy Grounds	●	●	●	●	●
Limits on Exceptions Premised on Grounds Other Than Privacy	●	●	●	●	●
Are Disciplines Enforceable?	●	●	●	●	●

¹ DEPA reaffirms and cross-references the Parties' existing data transfer and localization commitments from other international agreements.

² The USMCA and JUSDTA both prohibit Parties from differentiating between domestic data transfers and cross-border data transfers in a way that discriminates against foreign service providers.

³ The CPTPP (the Comprehensive and Progressive Trans-Pacific Partnership) does not extend the prohibition on data localization mandates to the financial sector, but it does extend provisions on cross-border data transfers to that sector.

INT'L NEGOTIATIONS RELATING TO DATA TRANSFERS

US-Mexico-Canada Agreement Article 19.11

Cross-Border Transfer of Information by Electronic Means

1. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.
2. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:
 - (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
 - (b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.

Footnote: A measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party

INT'L NEGOTIATIONS RELATING TO DATA TRANSFERS

Japan-UK Comprehensive Economic Partnership Agreement Art. 8.84

1. A Party shall not prohibit or restrict the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
2. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective, provided that the measure:
 - (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
 - (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.
3. This Article does not apply to: (a) government procurement; or (b) information held or processed by or on behalf of a Party, or measures by a Party related to that information, including measures related to its collection.

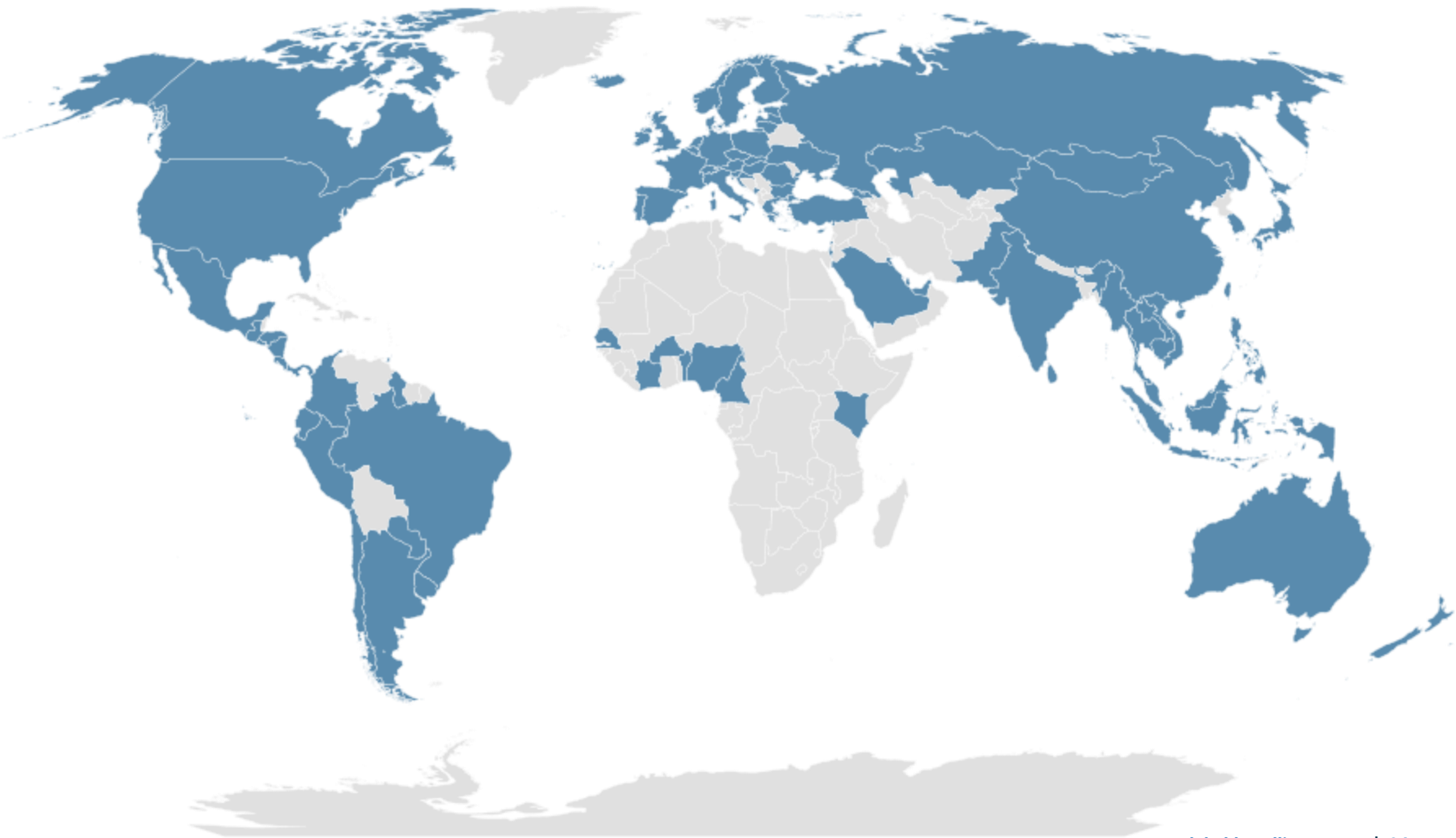
INT'L NEGOTIATIONS RELATING TO DATA TRANSFERS

The Regional Economic Partnership Agreement's [Electronic Commerce chapter](#) permits overbroad exclusions and derogations. RCEP data transfer and data localization commitments:

- **Are Limited to Each Party's Services and Investment Commitments**
 - The RCEP purports to limit RCEP obligations on data transfers and data localization to specific services-related commitments undertaken by the Parties. This means that data transfer and data localization obligations would only arise to the extent that a Party has 'scheduled' specific commitments in particular services sectors.
 - In practice, this approach would allow a trading partner to block data transfers in any sector in which it had not made a services commitment.
 - For example, if the trading partner had not made commitments relating to support services for aircraft repair and maintenance services, the trading partner could prevent inbound or outbound machine-to-machine transfers of data necessary to safe and reliable operation, predictive maintenance, operational diagnostics, or other product support that is critical to air carrier operations.
- **Allow for Derogations that a Party "Considers" Necessary**
 - The RCEP obligation permits a Party to derogate from the data transfer and data localization obligations to adopt or maintain "any measure inconsistent with paragraph 2 that [the implementing Party] considers necessary to achieve a public policy objective."
 - No past agreement – at the WTO or in the free trade agreement context – has expressly authorized a Party to disregard an obligation touching on data transfers or data localization on wholly subjective grounds.
- **Are Subject to a New National Security Exception of Unprecedented Breadth**
 - While prior trade agreements contain "national security" exceptions, the RCEP national security exceptions are particularly open-ended – drafted more broadly than national security exceptions found in the WTO Agreement or prior FTAs. The RCEP text in question states as follows:
 - "Nothing in this Article shall prevent a Party from adopting or maintaining ... any measure that it considers necessary for the protection of its essential security interests. Such measures shall not be disputed by other Parties."
- **Lack Any Binding Review Mechanism**
 - The entire RCEP Electronic Commerce chapter is exempted from binding dispute settlement.

INT'L NEGOTIATIONS RELATING TO DATA TRANSFERS

- 86 Countries are currently engaged in the WTO Joint Statement Initiative e-commerce negotiations



INT'L NEGOTIATIONS RELATING TO DATA TRANSFERS

Multi-Industry Statement for WTO JSI

- Urges WTO negotiators to
 - Prohibit unnecessary or discriminatory data localization mandates and data transfer restrictions
 - Support interoperability and transparency among legal frameworks
 - Apply rules across all economic sectors
 - Adopt frameworks to protect personal information



Multi-Industry Statement on Cross-Border Data Transfers and Data Localization Disciplines in
WTO Negotiations on E-Commerce

January 26, 2021

“To enhance certainty and economic opportunity, any agreement should discipline **unnecessary or discriminatory** data localization mandates and data transfer restrictions. Any agreement should also be guided by principles of transparency and **interoperability** among legal frameworks; should apply **across all economic sectors**; and should require all countries to adopt or maintain legal **frameworks to protect personal information.**”