Why a cross-track approach is necessary to steer the work of the CSTD Working Group on Data Governance

Anita Gurumurthy – IT for Change[1]

January 2026

The United Nations Commission on Science and Technology for Development (CSTD) Working Group on Data Governance, in line with the mandate in Para 48 of the Global Digital Compact, has approached the task of evolving follow-up recommendations towards equitable and interoperable data governance arrangements, through deliberations on four key tracks – (1) fundamental principles of data governance at all levels as relevant for development; (2) proposals to support interoperability between national, regional; and international data systems; (3) considerations of sharing the benefits of data; and (4) options to facilitate safe, secure, and trusted data flows, including cross-border data flows as relevant for development (all Sustainable Development Goals (SDGs)).

The discussions in the Working Group have generated rich insights across the four tracks. However, when treated primarily within track-specific silos, they risk obscuring the structural dynamics that cut across data governance debates. Questions on the principles of data governance, interoperability, equitable benefit-sharing, and governance of cross-border data flows are deeply interlinked and mutually constitutive. While they may be significant issues for policy in and of themselves, addressing them in isolation risks fragmenting governance responses and diluting their developmental implications.

Across tracks, certain political-economic tensions surface repeatedly. These are between:

- Economistic data frameworks and social-relational ethics of data (**individualistic and societal frameworks of data governance**),
- Technical interoperability and socio-cultural and economic premises of data ethics (technical standards for data interoperability and pluralistic visions of data governance), and
- The liberalisation of cross-border data flows and the differential abilities of countries to generate value in an interdependent global economy (**free data flows and data sovereignty**).

These tensions reflect the neocolonial dynamics of the global digital economy, with deep faultlines in the distribution of foundational digital capabilities and the socialisation of data value.

In line with the mandate of the Working Group, and in order to effectively address these tensions, we need a data governance approach grounded in a global political economy lens. As we argue through this submission, the frames of efficiency, growth, trade facilitation, or risk mitigation are not adequate to the task at hand.

[1] With contributions from team members - Nandini Chami, Shobhit S., Merrin Muhammed Ashraf, and Amoha Sharma.

A global political economy lens foregrounds questions of who generates data, who aggregates it, who gains from it, who controls its (re)use, who captures value, and how prevailing governance arrangements affect the ability of states and communities, particularly in the Global South, to pursue their autonomous pathways to digital self-determination and equitable development.

Our submission advances a cross-track synthesis attentive to the overall developmental dimensions of data governance. It seeks to explicate the structural linkages between key debates across tracks, assess positions adopted by other members and observers alongside our own – based on their submissions to the Working Group - and articulate coherent stances that move the ongoing discussions toward a more holistic and development-oriented framing of data governance at all levels. This submission is organised along the lines of the debates that we see as most critical to evolving a cross-track approach to key issues.

Please see Annexure 1, containing a summary of key inputs from select submissions across tracks to illustrate cross-track engagement with each of the three debates below.

Debate 1: Between individualistic and societal approaches to data governance

Across the four tracks, submissions highlight two sets of approaches towards data governance. On one hand are purely individualistic approaches that treat frameworks for personal data protection, privacy, and security as sufficient for the protection of human rights. On the other are more holistic approaches that move beyond the personal versus non-personal data distinction, recognising the societal and collective ethics of, and the strategic developmental interests of states over, the value generated from their data.

For instance, Canada's submission in Track 1 emphasises robust personal data protections, while cautioning against measures such as data localisation that might unduly restrict cross-border data flows. Within this approach, individual rights, consent, and trust-based regulatory frameworks are treated as the core safeguards needed to unlock the benefits of data innovation. Similar assumptions are reflected in submissions that view legal adequacy and mutual recognition of personal data protection frameworks as sufficient safeguards for interoperability and data sharing. The International Chamber of Commerce's submission in Track 2 treats interoperability as achievable through alignment of national frameworks on data protection, suggesting that once personal data safeguards are in place, data can circulate freely to generate economic value. Finland's submission in Track 3 similarly foregrounds individuals' control over their data as the key mechanism for enabling free flows of data and fair competition in the digital economy.

Other submissions challenge the adequacy of this individualistic framing. Iran's submission argues that societies, not only individuals, hold collective rights over the data they generate, and that such data carries a public interest dimension that cannot be reduced to personal data protection alone. Derechos Digitales advances a similar critique from the perspective of indigenous and community data, arguing that consent-based models are insufficient to protect collective knowledge systems and that governance must recognise collective guarantees that operate beyond individual consent.

These submissions demonstrate the inadequacy and limits of a data governance approach based on the premise of personal data protection in the free market of data flows as a sufficient guarantor of data rights. They also point to a more fundamental limitation of approaches that create a binary between 'personal data protection' and 'non-personal data governance'.

Data is an outcome of social relations, arising from collective activity and public systems, and its value is realised through aggregation and reuse. This makes the distinction between personal and non-personal data increasingly blurred for governance purposes, as persons can be identified even based on data that is not directly linked to them and public interest questions – such as if and whether some data may be alienable at all, how data as a public good may be legitimately claimed by public authorities, where group profiling may be necessary for purposes of affirmative actions – require to be tackled decisively. An individualistic governance approach to data fails not only to prevent the conversion of inalienable personal information into an alienable economic object,[2] but it also leaves the exclusive control that data collectors have over the social data they hoard untouched. ETC Group's submission highlights how this data-extractive dynamic in the digital economy (that cannot be addressed merely through a narrow focus on free, fair, and informed consent) enables the enclosure of aggregated societal data through platformisation, assetization, and secondary monetisation practices.

Some submissions, as noted in the Synthesis Report, urge the need to view data as an enabler of public value, and the importance of benefit-sharing arrangements that respect the rights of data-generating communities, including Indigenous Peoples.[3] Framings that look to privacy and consent mechanisms as a hold-all approach to addressing the governance challenges of data sidestep the critical question of equity and data justice for communities.[4]

The concentration of data capabilities and value has public interest and societal consequences that personal data protection frameworks do not address. While individuals may retain limited control over data through personality rights at the point of data collection, the economic value derived from aggregated data is disproportionately captured by platform owners and financiers, with producers and communities facing lock-in, exclusion, and limited capacity to benefit. ETC Group emphasises that unequal access to connectivity, tools, bargaining power, and skills means that data-driven innovation often reinforces existing asymmetries, and that data lock-ins undermine not only competition, but also community/societal autonomy.

The implications of this governance gap are also evident in the context of the track on cross-border data flows. Colombia's submission in Track 4 emphasises that in unlocking the economic and developmental benefits of cross-border data flows, data intermediaries can play a relevant role as technical and contractual guarantors who ensure data transfers comply with local and international privacy rules.

---

[2] Prainsack, B. (2019, February 14). *Logged Out: Ownership, exclusion and public value in the digital data and information commons*. Big Data & Society. https://journals.sagepub.com/doi/full/10.1177/2053951719829773.

[3] Chair's Summary, 4th Meeting of the UN CSTD Working Group on Data Governance.

[4] See UNICEF (Track 3) where UNICEF highlights "Data is often taken from people and communities. A consideration must be how benefits are returned to people and communities in return for data generation and data use. Part of this process is to understand what the needs and interests of the community are including permissible and desired data use, and benefits." Also see the submission by Anriette Esterhuysen, AfriSIG (Track 1) on the need for data justice, which calls for participatory governance, equitable access to data and mechanisms to address harm and exclusion.

However, Rethink Trade's submission cautions that such 'safe, secure, and trusted data sharing' arrangements in trade agreements are often skewed in favour of commercial interests and can undermine public interest and developmental objectives.

Box 1: An integrated agenda for individual and societal rights in data

- Addressing the limits of a consent-oriented, legal-contractual model of data governance requires a shift towards a public law framework that governs the data commons from a data justice perspective. Such a framework recognises that data generated through social relations and collective activity gives rise to societal and collective rights, alongside individual entitlements.

- At the global level, there is a need for international data solidarity - a vital principle that is based on a development-oriented data constitutionalism.

- A global data constitutionalism would encompass rights to safeguard against data harms, including data dispossession at societal scale, the rights of communities to representation and participation in datasets (which includes the right to opt-out), and the societal right to data self-determination, that is, the right of communities and nations to steward data pathways for democratic integrity, distributive justice and development gains.

- Traditional IP regimes need to be made fit-for-purpose for the digital economy, in order to prevent the enclosure of social data and data-derived intelligence. This includes narrowing trade secret protection in datasets by limiting the claims of dataholders to exclusive access.

Debate 2. Between technical standards for data interoperability and pluralistic visions of data governance

Across tracks, submissions engage with the question of interoperability by emphasising the role played by interoperable standards in impacting who can access, use, and benefit from data. While several submissions highlight the role of interoperable standards in enabling data sharing and countering platform lock-ins, others caution that interoperability, if pursued as an end in itself, can also facilitate extractive practices and deepen existing inequalities. The debate that emerged is therefore not regarding the importance of interoperability per se, but about whether it should be treated as a primary objective of data governance, or as a purpose-bound tool within pluralistic conceptions of data governance geared towards public value and equity.

Submissions across Tracks 1, 2 and 3 recognise interoperability as a foundational infrastructural feature that shapes how data flows across systems, institutions and borders, and who is able to access and benefit from these flows. ETC Group's submission in Track 2 highlights interoperability as a tool to avoid lock-ins and ensure that proprietary ecosystems do not undermine producer or community autonomy. UNESCO's submission in Track 3 further notes that governance arrangements, including interoperable standards, directly affect who can access, use, and benefit from data, and that interoperability can support public value creation across sectors.

Switzerland's submission in Track 4 complements these perspectives by emphasising that the benefits of data use enabled through interoperability extend beyond economic value to include transparency, improved public services, and citizen empowerment through digital self-determination.

At the same time, and as Derechos Digitales' submission in Track 2 recognises, while interoperability as a technical mechanism may be necessary to break monopolies, there are risks associated with legal interoperability arrangements that may result in a race to the bottom, entrenching the exploitation of Global South countries in the unequal international data order.[5]

What these submissions surface is an inherent tension – the need for a data regime in which interoperability of technical data standards (with its economic and non-economic benefits) does not lead to coercive harmonisation where a select few benefit at the expense of others. As noted in Linnet Taylor's submission in Track 2, the critical question is " what kind of interoperability",[6] underscoring that interoperability choices are inherently political, and require assessment of which data flows, to whom, and under what conditions.

Further, data interoperability is not an intrinsic public good. As a 2022 research study for the European Parliamentary Research Service highlights, proposals for interoperability and data-sharing under the European Union (EU) Data Act fail to challenge market structures that aid "centralisation, exploitation, and reduced autonomy for vulnerable communities."[7] The study points out that "interoperability, without challenging the commodification of data, could translate into the centralisation of data in companies."

What this means is that seamless data flows in fact reinforce data and value capture, creating de facto perpetual control for first-movers over aggregated societal data and data-derived intelligence. ETC Group's submission in Track 3 illustrates this dynamic in the context of agriculture, where value created along data pipelines is captured upstream by platform owners. In such contexts, managing data commons as a public good for permissionless innovation does not necessarily lead to democratic, social-purpose innovation trajectories.

What is evident is that interoperability of technical data standards cannot be conflated with unrestricted or seamless data flows, particularly across borders. Some submissions frame free cross-border data flows as an architectural necessity for innovation,[8] with regulatory interoperability positioned as a means to promote such flows.[9]

---

[5] See collective submission by Derechos Digitales, Research ICT Africa and Tech Global Institute (Track 2).

[6] See Linnet Taylor (Track 2).

[7] Lopez Solano, J., Martin, A., de Souza, S., & Taylor, L. (2022). *Governing data and artificial intelligence for all: Models for sustainable and just data governance* (Scientific Foresight Unit (STOA) Study, European Parliamentary Research Service, PE 729.533). European Parliament .https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU(2022)729533_EN.pdf

[8] See Carl Gahnberg (Track 1).

[9] See Canada (Track 2).

However, as reflected in Anita Gurumurthy's submission in Track 4,[10] most domestic, regional, and international measures supporting cross-border data flows have been designed primarily to facilitate market expansion for dominant digital services corporations. These measures often prioritise lowering business costs, expanding trade, and enabling global services delivery, while paying insufficient attention to distributional effects such as data control, value capture, and protections for data-generating communities. They also contribute to a growing public data deficit, limiting the capacity of public institutions, smaller firms, and community actors to innovate. Without a robust and nuanced data governance framework grounded in human rights and public interest norms, interoperability and data flows without guardrails risk reinforcing monopolies and entrenching existing inequalities.[11]

When interoperability functions as a proxy for unrestricted cross-border data flows, including through trade agreements, it ends up constraining governments' right to regulate data in the public interest. This compromises the ability of developing countries to access, use, and create value from their data resources for domestic development, trapping them in low-value segments of the global digital economy as raw data providers and digital services consumer markets.[12]

The contextual ethics of data and the consequent differences in national legal regimes for data also point to the fact that a one-size-fits-all global approach to interoperability is neither practical nor desirable.

We need to be cautious of approaches that frame interoperability primarily as the homogenisation of personal data protection standards, as they tend to ignore political, cultural, and economic differences across contexts and reinforce digital neo-imperialism. Anchoring everyone to an acceptable benchmark in consumer rights and privacy protections can drive standards to the lowest common denominator and ignore a whole gamut of data rights.[13]

---

[10] See Anita Gurumurthy (Track 4). Facilitation of safe, secure, and trusted data flows, including cross-border data flows (Submission to the UN Commission on Science and Technology for Development Working Group on Data Governance). IT for Change.
https://itforchange.net/sites/default/files/2735/Track%204-%20Facilitation%20of%20Safe%2C%20Secure%2C%20and%20Trusted%20Data%20Flows%2C%20Including%20Cross-Border%20Data%2 0Flows.pdf Also see Azmeh, S., Foster, C., & Echavarri, J. (2019). The international trade regime and the quest for free digital trade. International Studies Review, 22(3), 671–692. https://academic.oup.com/isr/article/22/3/671/5564378;
Bacchus, J., Borchert, I., Morita-Jaeger, M., & Ruiz Diaz, J. (2024, April 8). Interoperability of data governance regimes: Challenges for digital trade policy (CITP Briefing Paper No. 12). Centre for Inclusive Trade Policy.
https://citp.ac.uk/publications/interoperability-of-data-governance-regimes-challenges-for-digital-trade-policy

[11] Openness is not always a public good, and in fact, an "open by default" approach has accentuated risks of biopiracy or illegal commercialization of knowledge. See Anita Gurumurthy's presentation during the 4th Working Group meeting, titled "Governance Interoperability and Cooperation in Data Flows - Towards Trust And Accountability". Also see Eaves, D., Coyle, D., Vasconcellos, B., & Deshmukh, S. (2025). The economics of shared digital infrastructures: A framework for assessing societal value (IIPP Policy Report No. 2025/02). UCL Institute for Innovation and Public Purpose.
https://www.ucl.ac.uk/bartlett/sites/bartlett/files/2025-04/the_economics_of_shared_digital_infrastructures.pdf

[12] United Nations Conference on Trade and Development. (2021). *Digital economy report 2021: Cross-border data flows and development: For whom the data flow* (UNCTAD/DER/2021). United Nations.
https://unctad.org/system/files/official-document/der2021_en.pdf

[13] Bacchus, J., Borchert, I., Morita-Jaeger, M., & Ruiz Diaz, J. (2024, April 8). *Interoperability of data governance regimes: Challenges for digital trade policy* (CITP Briefing Paper No. 12). Centre for Inclusive Trade Policy
https://citp.ac.uk/publications/interoperability-of-data-governance-regimes-challenges-for-digital-trade-policy

Box 2 - A nuanced approach to interoperability

- Data governance frameworks should approach interoperability not as an end in itself but as part of a broader approach geared towards public value maximisation. Legal frictions or purpose constraints need to accompany technical interoperability of data. Such 'bounded openness' will ensure equity and public interest in data sharing arrangements. UNESCO's submission in Track 2 notes that collaboration does not require uniformity. Instead, it can be built on federated models, tiered access mechanisms, and data-sharing agreements that specify conditions, purposes, and safeguards for use. Similarly, as submitted by the United Nations Office for Digital and Emerging Technologies (UN ODET) under Track 3, governance arrangements should establish models of collaboration rooted in principles of fairness, reciprocity, and shared prosperity.[14]

- In global data commons emerging in various sectors such as health and agriculture, conditionalities should be instituted to safeguard equity in data reuse,[15] data traceability, and the flow of data value back into the public domain.[16] Guidelines on data sharing must give primacy to the interests of source communities to whom the data belongs.[17]

- A nuanced approach to interoperability in data governance is one that enables countries to maintain sovereignty over their data resources while participating in regional or global data ecosystems. For instance, the African Union (AU) Data Policy Framework advocates continental frameworks for interoperability that respect national data sovereignty while enabling regional flows.[18] This approach recognises that data ecosystems contextually differ in actor constellations, technology maturity, and regulatory risks,[19] and that uniform interoperability requirements can flatten these differences and unevenly distribute harms.

[14] ODET (Track 3) highlights that compensation mechanisms should go beyond monetary valuation to include capacity building, access to shared resources, and other benefits to better address today's uneven distribution of data infrastructure. Also see the submission by AfriSIG (Anriette Esterhuysen) to Track 3, wherein the importance of co-developing governance models that confront power asymmetries and distribute data's economic/social value equitably is highlighted.

[15] See the UN CEB Data Principles included in the Compendium of Data Governance Principles prepared by the Secretariat.

[16] Gurumurthy, A. (2025, August 25). Track 1: Data governance principles as relevant to development (Submission to the UN Commission on Science and Technology for Development Working Group on Data Governance). IT for Change. https://itforchange.net/sites/default/files/add/Track%201-Data%20Governance%20Principles%20as%20Relevant%20to%20Development.pdf

[17] See Anita Gurumurthy's presentation during the 4th Working Group meeting, titled "Governance Interoperability and Cooperation in Data Flows - Towards Trust and Accountability". Also see Matthew Canfield (Track 3); the submission highlights that agricultural data requires specific protections that involve greater commitment to participation of data originators.

[18] See Research ICT Africa (Track 2).

[19] See Hodapp, D., & Hanelt, A. (2022). *Interoperability in the era of digital innovation: An information systems research agenda.* Journal of Information Technology, 37(4), 407–427. https://www.researchgate.net/publication/358413970_Interoperability_in_the_era_of_digital_innovation_An_information_systems_research_agenda

Debate 3. Between free data flows and data sovereignty

Across the four tracks, submissions engage with cross-border data flows through two contrasting lenses. One set of submissions frames cross-border data flows as a technical or economic necessity for innovation and integration into global markets.

Regulatory diversity, localisation measures, and differentiated national approaches are often characterised as frictions that undermine scalability and competitiveness.[20]

Another set of submissions highlights that cross-border data flows operate within a global data economy marked by deep asymmetries in infrastructure, capital, institutional capacity, and bargaining power.[21] These submissions caution that cross-border data flows do not automatically produce equitable development outcomes, and that without attention to data sovereignty, regulatory autonomy, and value distribution, they can reinforce existing asymmetries. The debate, therefore, centres on how cross-border data flows should be governed, rather than on whether data should flow across borders.

Data generated through public services and other social and economic activity in the Global South often flows outward into infrastructures controlled by a small number of firms based in the North.[22] These firms possess the compute, capital, and proprietary systems required to convert raw data into high-value digital intelligence, which is then reintroduced into originating economies as platforms, analytics, or AI systems. Our earlier submissions highlight how most measures currently in place to support cross-border data flows entrench this one-way flow of value, consolidating capabilities and market power in a few jurisdictions while reinforcing dependency in the South. Such dynamics deepen the digital divide, particularly where countries lack the capacity to influence how their data is used, monetised, or reinvested.[23] Recognising regulation of cross-border data flows as a legitimate governance choice is therefore essential to shift attention from whether data should flow, to how flows are structured, who benefits from them, and how costs are distributed.[24]

Many submissions argue that predictable rules for cross-border data flows, harmonised through trade agreements, are necessary to support innovation and economic growth. These claims are often supported by aggregate growth projections under open data regimes, alongside concerns that regulatory fragmentation increases compliance costs and legal uncertainty.[25]

---

[20] See, for instance, ICC (Track 2) and NTT Data Group (Track 2). Similar concerns are echoed in Canada's submission (Track 4), which emphasises predictability and interoperability as enablers of economic participation.

[21] See Indonesia (Track 4) and Iran (Track 4), which underline the uneven capacities of states to participate in and benefit from cross-border data regimes. See Anita Gurumurthy (Track 4), which situates data flows within broader questions of power and development.

[22] See Anita Gurumurthy (Track 4); ETC Group (Track 3).

[23] See Indonesia (Track 4).

[24] See Anita Gurumurthy (Track 4); Linnet Taylor (Track 1).

[25] See ICC (Track 2) and Canada (Track 4), which stress legal certainty and reduced compliance costs, and references in WTO (Track 4) to OECD–WTO studies projecting aggregate GDP gains under open data regimesBRICS.

However, as pointed out in our earlier submissions and those of others,[26] trade-centric approaches prioritise market access and commercial efficiency over development, rights, and public interest considerations, particularly in a context where a small number of firms possess disproportionate agenda-setting power.

Embedding data flow commitments within trade agreements can thus constrain states' ability to regulate data use, adapt policies to technological change, or pursue alternative development strategies.

Instruments such as the World Trade Organisation (WTO) moratorium on customs duties on electronic transmissions are examples of how trade rules can lock in asymmetrical digital advantages while limiting fiscal and regulatory options for developing countries.[27] These concerns are amplified in the context of the decline of multilateral negotiations, where fragmented or bilateral arrangements further weaken the ability of less powerful states to defend development-oriented data governance choices.[28] From this perspective, cross-border data flows must not be treated as a narrow trade issue while ignoring their wider implications for democratic accountability, institutional capacity, and long-term development trajectories.

Further, several submissions promote "data free flow with trust" frameworks as a means of reconciling openness with safeguards such as privacy, security, and technical compliance to enable cross-border data flows.[29] While these safeguards are necessary, such frameworks narrow the governance challenge to risk mitigation and regulatory compatibility, leaving unaddressed questions of control, accountability, and value capture across the data lifecycle.

In response, in our earlier submissions, we have advanced a reframing of cross-border data governance towards "data flows with data rights", aligned with the BRICS Leaders' Statement on the Global Governance of AI.[30] This framing foregrounds substantive rights across the data lifecycle, including collective and societal interests that are not adequately protected through individual consent mechanisms or contractual/technical standards alone. It recognises that cross-border data flows must be purpose-bound, conditional, and subject to accountability.

A recurrent theme across many inputs from Global South stakeholders is the need to preserve policy space to govern cross-border data flows in line with national development priorities.[31] Regulatory autonomy enables states to stagger their integration into global data value chains, build domestic data and AI ecosystems, and adopt context-specific measures where necessary. Measures such as localisation requirements, conditional access rules, or sector-specific

[26] See Daniel Rangel/Rethink Trade (Track 4), which highlights that exceptions clauses to free data flows in digital trade agreements are modeled after the general exceptions in the GATT and the GATS, and hence, do not guarantee countries their right to regulate.
[27] See Anita Gurumurthy (Track 4).

[28] See Xiaowen and Mosi (Track 4).

[29] See Canada (Track 1), NTT Data Group (Track 2) and Microsoft (Track 2) where trust, interoperability, and compliance harmonisation mechanisms are foregrounded as sufficient to enable equitable data flows.

[30] See Anita Gurumurthy (Track 4).

[31] See Indonesia (Track 4) and Tanzania (Track 4), which stress the need to carefully consider integration, invest in domestic infrastructure, and build local data and AI ecosystems.

restrictions are not inherently illegitimate; rather, they are necessary tools that can support local development and resilience, especially where public institutions and domestic firms are still building capacity.[32]

Premature or uniform harmonisation can lock countries into governance models that privilege technological first-movers and foreclose alternative innovation pathways. As submitted in our earlier input, drawing from the principle of 'sovereign equality', all states should have the capacity to use data resources for local economic and social development that suit their vision of data economy, and to regulate cross-border data flows in their strategic interests by evolving national-level legislation and economic policy roadmaps.

Box 3 - Data flows with rights as the foundation of development sovereignty

- There is a need to recognise digital sovereignty and the right to development as baseline principles in the governance of data flows. This position draws on frameworks such as the BRICS Leaders' Statement on the Global Governance of AI, and is guided by the principles of 'data flows with rights'. A 'data flows with rights' approach recognises the indivisibility of human rights as a foundational norm for the governance of cross-border data flows. What this implies is that economic, social, and cultural rights in data, and data self-determination are as crucial to the governance of cross-border data flows as considerations of privacy, security, and freedom from dataveillance (first-generation rights).

- Drawing on the principle of 'sovereign equality', all states should have the capacity to use data resources for local economic and social development that suits their vision of development in digital society. Cross-border data flows, therefore, must be kept outside the purview of trade negotiations, which prioritise market access and harmonisation over public interest and regulatory autonomy.

[32] See Anita Gurumurthy (Inputs on the Synthesis Note for Track 4).

Annexure 1

A. Summary of key inputs relating to Debate 1

S No.	Track	Submission by	Summary of key inputs relating to Debate 1
1	Track 1	Canada	• The Secretariat should take account of the concept of Data Free Flow with Trust (DFFT), which aims to support open and free flows of data across borders while ensuring the appropriate privacy, security, and other safeguards are in place. The concept currently enjoys broad support across the G7 and G20 and underpins the OECD's policy and research on international data governance. • Canada balances these goals in its domestic frameworks by having in place strong, enforceable personal information protections for data held both by public and private actors, as well as guardrails for government collection, sharing, and use of personal information, without unduly restricting the cross-border flows of data or imposing data localisation requirements. Open and transparent communications about data management and governance practices could reinforce such measures by strengthening public trust. • Internationally, one way Canada supports the concept of DFFT is by seeking legally-binding commitments in free trade agreement (FTA) provisions that prohibit restrictions on cross-border data flows and data localisation requirements, while keeping a balance ensuring Canada and FTA partners can continue to pursue legitimate public policy objectives and protect key national interests such as security.
2	Track 2	International Chamber of Commerce	• A central barrier to progress is the false dichotomy between cross-border data flows and national control over data. These objectives are not mutually exclusive. Countries can safeguard their sovereignty and pursue their development priorities while enabling the seamless exchange of data that underpins trade, innovation, and security. Interoperability can be achieved through mechanisms such as mutual recognition and adequacy arrangements, which respect national legal frameworks while avoiding duplicative compliance burdens.

3	Track 3	Finland	• Today's data economy creates network effects favouring a few platforms able to collect and process the largest masses of personal data. These platforms are locking up markets, not just for their competitors, but also for most businesses who risk losing direct access to their customers. • By letting individuals control what happens to their data, we intend to create a truly free flow of data – freely decided by individuals, free from global choke points – and to create balance, fairness, diversity and competition in the digital economy
4	Track 1	Iran	[A couple of the principles highlighted as particularly important] • In addition to individual rights concerning the data they generate, societies also hold rights over the collective data they produce. This information is a public right belonging to the entire population of the country. • Data Sovereignty and the principles of international law: In the context of data governance, it is essential to ensure that digital sovereignty of countries over their data should be respected.
5	Track 2	Derechos Digitales	• Collective guarantees on data protection that are not dependent on consent should be advanced, including to protect data and knowledge from indigenous communities (and from other groups holding traditional knowledge), as well as their right to prior consultation.
6	Track 1	ETC Group	• Avoidance of lock-in: Interoperability and portability must be guaranteed so that proprietary ecosystems do not undermine producer or community autonomy • Unequal capability to benefit: Access to connectivity, tools, bargaining power, and skills is uneven, so data-driven value tends to concentrate with platform owners while producers and communities face lock-in and exclusion. Prioritise publicly governed digital infrastructure, enforceable portability and interoperability, and community data literacy and consent tools so local actors can participate on fair terms and capture value.

7	Track 3	UNICEF	• Data is often taken from people and communities. A consideration must be how benefits are returned to people and communities in return for data generation and data use. Part of this process is to understand what the needs and interests of the community are, including permissible and desired data use and benefits. Consequently, participation of individuals and groups, including young people and children, in decisions across the data lifecycle is important.
8	Track 1	Anriette Esterhuysen, AfriSIG	• Data practices can reinforce or disrupt existing power asymmetries and must therefore be designed to uphold dignity, equality, and the rights of all people. Data justice calls for participatory governance, equitable access to data, and redress mechanisms to address harm and exclusion.
9	Track 4	Colombia	• Data intermediaries [could] play a relevant role as technical and contractual guarantors that international transfers are carried out under secure and transparent conditions, ensuring compliance with local and international privacy rules. • The interaction of these mechanisms with development benefits is reflected in the possibility of boosting the digital economy, facilitating e-commerce, promoting technological innovation, and generating opportunities for inclusion and competitiveness for developing countries. However, these benefits only materialise to the extent that trust, minimum security standards, and regulatory frameworks that provide certainty to both users and economic agents involved in data management and processing exist.
10	Track 4	Daniel Rangel, Rethink Trade	• Certain interests have argued that adopting free flow of data rules in trade agreements is a way “to promote safe, secure, and trusted data sharing”. The problem is that trade agreements are often skewed in favour of commercial interests and, consequently, undermine public interest objectives, such as the protection of personal data.

B. Summary of key inputs relating to Debate 2

S No.	Track	Submission by	Summary of key inputs relating to Debate
1.	Track 1	ETC Group	• Avoidance of lock-in: Interoperability and portability must be guaranteed so that proprietary ecosystems do not undermine producer or community autonomy • Unequal capability to benefit: Access to connectivity, tools, bargaining power, and skills is uneven, so data-driven value tends to concentrate with platform owners while producers and communities face lock-in and exclusion. Prioritise publicly governed digital infrastructure, enforceable portability and interoperability, and community data literacy and consent tools so local actors can participate on fair terms and capture value.
2	Track 3	UNESCO	• Key governance arrangements, such as standardisation, financing models, intellectual property regimes, and data protection frameworks, directly affect who can access, use, and benefit from data. For instance, interoperable standards can enable broader data reuse and integration, supporting public value creation across sectors.
3	Track 4	Switzerland	• The benefits of data use go beyond purely economic value. Economically, interoperable and trustworthy data spaces improve efficiency, create new business models and strengthen competitiveness. Social benefits include greater transparency, better public services and citizen empowerment through digital self-determination. Indirect benefits arise from innovation and knowledge creation, such as advances in health research, environmental protection or mobility solutions. Considering all these dimensions ensures that data governance supports both prosperity and societal well-being.

S No.	Track	Submission by	Summary of key inputs relating to Debate
4	Track 2	Collective submission by Derechos Digitales, Research ICT Africa, Tech Global Institute	[From Derechos Digitales] ● We recognise and defend interoperability as a technical feature that allows different systems to communicate and information to be transferred from one to another. This is a key element allowing the advance of digital technologies since their origin and we defend it as a way to incentivise innovation and democratize access to knowledge, as well as a mechanism to break monopolies within the digital economy and to empower workers from the platform economy. A risk we foresee is for it to be deployed in a way that facilitates the exploitation of users' data among different parties without allowing them the exercise of informational self-determination. Thus, strong data protection mechanisms should be integrated in any deployment of interoperable systems, particularly by public entities entitled to exceptions to consent for the delivery of public services, to avoid undue data sharing. ● However, we have serious concerns about the idea of legal interoperability that is being pushed by some organisations and G7 countries, to facilitate compliance across jurisdictions and thus transnational data processing. We identify at least three risks of legal interoperability approach within data and AI governance: (a) it can result in a race to bottom for the minimum consensus possible in a divided and unequal world; (b) it can be used to push criteria defined by the economies that today are benefiting from data extraction and AI into Global South countries, further entrenching existing imbalances in the benefits of data economies; (c) it represents concerns around the infringement of diverse regulatory approaches and the national sovereignty of Global South countries.
5.	Track 2	Linnet Taylor	● Differing definitions of digital/data sovereignty are a big challenge: people are using the same words with very different meanings. Similarly, interests in accumulating data to feed AI models currently map onto economic power, as does the ability to do so. So the question, 'interoperability of what', is important. The AI economy should be considered in parallel with data governance, as it determines who will argue for what kind of interoperability. Bi-directional interoperability between private and public-sector systems can be important to building economic benefits, but also renders public systems vulnerable to extractive practices by commercial interests. It is therefore important to make it possible for public-sector actors to firewall data that should remain publicly controlled and not used to extract and financialise public-sector digital resources.

S No.	Track	Submission by	Summary of key inputs relating to Debate
6	Track 3	ETC Group	• Much of the value created along the data pipeline in the context of agriculture is captured upstream by platform owners and financiers through assetization, secondary monetization, and the creation of financial products such as carbon credits and ESG instruments.
7	Track 1	Carl Gahnberg	• Internet's resilience and openness depend on preserving it as a globally interoperable network of networks. RFC 1958 (Architectural Principles of the Internet, 1996) frames connectivity as the Internet's ultimate goal. Forced localisation, jurisdiction-based restrictions, and large-scale filtering run counter to fundamental principles of the Internet's architecture. They not only create inefficiencies but also erode the technical fabric that ensures security, trust, and openness can scale globally. • The IETF has long held that strong cryptography (notably end-to-end encryption, e2e) must be widely available and should not be weakened for the purpose of monitoring and surveillance. Encryption is an architectural expectation that must be upheld.
8	Track 2	Canada	• While promoting regulatory interoperability can reduce compliance burdens for businesses and stimulate innovation and economic growth, such benefits may initially accrue more readily to larger, more resourced companies who are better equipped to navigate complex legal transitions and invest in necessary internal compliance systems than SMEs. Therefore, efforts to enhance interoperability must foster inclusive environments that take SMEs' needs and circumstances into consideration so that the benefits of interoperability are broadly accessible throughout the economy.
9	Track 4	Anita Gurumurthy	• Most domestic, regional, and international measures currently in place to support CBDFs have been designed to enable global market expansion of dominant corporations. They do not pay adequate attention to the distributional effects of such free data flows, thereby overlooking a critical aspect of impacts on development. Such provisions, which seek to enable the operation of a frictionless global single market of digital services, will only benefit those countries with well-developed domestic digital economic sectors, and even within these countries, benefits will accrue to those "sectors and to people that are already privileged in terms of international market access or skills".

S No.	Track	Submission by	Summary of key inputs relating to Debate
10	Track 2	UNESCO	• Interoperability must be approached as a governance challenge, not just a technical one—requiring inclusive processes, shared principles, and trust-based mechanisms that protect rights while unlocking data's full public value. Collaboration does not require uniformity; instead, it can be built on federated models, tiered access mechanisms, and data sharing agreements that specify conditions, purposes, and safeguards for use. This enables countries to maintain sovereignty over their data and systems while participating in broader regional or global data ecosystem. Institutional sustainability depends on clearly defined data stewardship roles, inter-agency coordination mechanisms, and legal mandates that support interoperability as a public good.
11	Track 3	ODET	• Governance arrangements should establish models of collaboration rooted in principles of fairness, reciprocity, and shared prosperity. Compensation mechanisms should go beyond monetary valuation to include capacity building, access to shared resources, and other benefits to better address today's uneven distribution of data infrastructure. Underlining the urgent importance of talking about IP, appropriate governance mechanisms are key for tracking value derived from data used by LLMs and for determining how original contributors might be compensated and acknowledged.
12	Track 3	Anriette Esterhuysen, AfriSIG	Research ICT Africa: • Global collaboration is as important as regional collaboration and the international community and organisations need to advance better data benefit-sharing systems. Stakeholders must co-develop governance models that confront power asymmetries and distribute data's economic/social value equitably. Communities should have agency over how their data is collected, used, and deleted.
13	Track 2	Collective submission by Derechos Digitales, Research ICT Africa, Tech Global Institute	• The AUDPF proposes that interoperability should be promoted through AU-led continental frameworks that respect data sovereignty while enabling flows. This approach allows countries to retain control by applying differentiated safeguards depending on the sector and sensitivity of data.

C. Summary of key inputs relating to Debate 3

S No.	Track	Submission by	Summary of key inputs relating to Debate 3
1.	Track 2	Timea Suto, International Chamber of Commerce	• The most pressing challenges are regulatory fragmentation and divergent national approaches to data governance. Inconsistent rules, particularly around cross-border data flows, government access to personal data, and requirements for data localisation, create compliance burdens that disproportionately affect SMEs and reduce competitiveness. At the international level, risks also arise from overlapping or conflicting frameworks that increase costs and legal uncertainty, while at the regional level, approaches that prioritise sovereignty over interoperability may limit participation in global value chains.
2	Track 2	Masaru Dobashi, NTT Data Group Corporation	• Legal interoperability remains a major challenge. Rules for managing and using data differ across countries and are often difficult to interpret, which can hinder rapid service integration and limit scalability. • Interoperability challenges go beyond technical consistency. They include institutional and cultural differences, varying meanings and contexts of data—especially internationally—and barriers such as lack of trust and concerns over data sovereignty.
3	Track 4	Canada	• Canada seeks provisions in its free trade agreements to limit data-related barriers to cross-border digital trade, while ensuring Canada and trade-partners can continue to pursue legitimate public policy objectives and protect key national interests such as security.
4	Track 4	Indonesia	• Developing countries face key challenges in relation to cross-border data flows, including limited digital infrastructure, weak data protection laws, and concerns over data security and sovereignty. They often lack technical expertise and face high costs of compliance. Additionally, they have less influence in international policy-making, which can limit their ability to benefit fully from global data exchanges.
5	Track 4	Tahereh Jalili, Iran	• Developing countries face legal and regulatory challenges, security challenges, economic challenges and the data divide. Accountability mechanisms must be established to mitigate data misuse. • Existing mechanisms are incomplete and very few, and geared towards large corporations and developed countries.

6	Track 4	Anita Gurumurty, IT for Change	• Most domestic, regional, and international measures currently in place to support CBDFs have been designed to enable global market expansion of dominant corporations. They do not pay adequate attention to the distributional effects of such free data flows, thereby overlooking a critical aspect of impacts on development. Such provisions, which seek to enable the operation of a frictionless global single market of digital services, will only benefit those countries with well-developed domestic digital economic sectors, and even within these countries, benefits will accrue to those "sectors and to people that are already privileged in terms of international market access or skills". Shifts needed in policy frameworks: • Internationally, we need an integrated regime for CBDFs that simultaneously responds to its economic and non-economic dimensions of shaping data flows in a manner that facilitates the realization of human rights and structural justice in the global economy. Drawing from the principle of sovereign equality, all states should have the capacity to use data resources for local economic and social development, and to regulate CBDFs in their strategic interests by evolving national-level legislation and economic policy roadmaps. • The regulation of CBDFs should not be a trade policy issue, and selective aspects of such regulation cannot be negotiated through trade agreements, which prioritise profit imperatives over human rights values and are prone to industry capture. Challenges faced by countries regarding CBDFs: • Unequal value capture and one-way data flow • Expansive IP regimes • Restrictive trade agreements • Fiscal and taxation constraints • Privacy and national security risks arising from illegitimate foreign surveillance Suggestions: • Shifting from a DFFT to "data flow with data rights" policy stance • Recognition of the sovereign right of all countries to regulate data flows for strategic advantage • Infrastructure development • Fiscal measures to redistribute data value

7	Track 3	ETC Group	• Much of the value created along the data pipeline in the context of agriculture is captured upstream by platform owners and financiers through assetization, secondary monetisation, and the creation of financial products such as carbon credits and ESG instruments. • Governance arrangements that impact the benefits of data - standardisation and interoperability can widen participation if they are designed to prevent lock-in. Finance and market rules shape who captures value from data. Intellectual property and Access and Benefit-Sharing determine whether biocultural value is shared. Recent intergovernmental steps recognise that AI users of digital sequence information should contribute to a multilateral fund, establishing a precedent for redistributive benefit-sharing; extending these obligations to ecological and community- derived datasets would further align benefits with origin communities, guided by FPIC. Support for community-governed data institutions and cooperatives can align benefits with producers and local communities.
8	Track 1	Linnet Taylor	• (Emphasises) the importance of recognising legitimate claims to autonomy on the national or sub-national level and creating options for data to remain local and its value to others to be negotiated rather than enforced.
9	Track 4	Canada	• Canada seeks provisions in its free trade agreements to limit data-related barriers to cross-border digital trade, while ensuring Canada and trade-partners can continue to pursue legitimate public policy objectives and protect key national interests such as security.
10	Track 4	WTO	• According to a joint OECD-WTO study, measures that allow for the flow of data with appropriate safeguards are expected to have a positive impact on trade and GDP growth. While there are trade costs associated with data regulation, these are balanced by the trust benefits of safeguards that protect data when transferred abroad. Convergence towards this kind of balanced data regulation would deliver additional economic and trade benefits by reducing the fragmentation of data flow regimes. Indeed, the study finds that if open data regimes with safeguards were adopted by all economies, global exports would grow by 3.6% and global GDP by 1.77%. • The WTO moratorium on customs duties on - electronic transmissions, first adopted in 1998, has guaranteed a duty-free regime for electronic transmissions, contributing to the openness of the digital economy.

11	Track 4	Daniel Rangel, Rethink Trade	• Even when free data flows rules have exceptions, the language is modelled after the World Trade Organisation's general exceptions terms in the General Agreement on Tariffs and Trade and the General Agreement on Trade in Services, which do not guarantee countries' right to regulate (please see pgs. 26-27 of our report). So, if countries want to explore frameworks that support data transfers that are based on values first and then economic considerations, they should consider models like the Council of Europe's Convention 108+ or the African Union's Malabo Convention (please see pgs. 14-16 of our report). These instruments do enable the movement of data, but provided that recipient countries guarantee certain baseline protections.
12	Track 4	Tan Xiaowen and Li Mosi	• The first challenge countries face in relation to cross-border data flows is how to reconcile privacy concerns with the economic rights associated with the free flow of data. Second, the fragmentation of cross-border data flow regulations. Third, along with the decline of multilateral negotiations, developing countries' ability to participate in the discussion related to cross-border data flows is insufficient.
13	Track 1	Canada	• The Secretariat's compilation of governance principles should take into account the concept of Data Free Flow with Trust, which aims to support open and free flows of data across borders while ensuring the appropriate privacy, security, and other safeguards are in place.
14	Track 2	Ashutosh Chadha, Microsoft	• Achieving seamless interoperability encounters significant barriers at technical, organisational, legal, and political levels. Balancing cross-border collaboration with data sovereignty is a central tension. The concept of "Data Free Flow with Trust" (DFFT) proposes sharing data under mutual assurances of privacy, security, and respect for local laws.
15	Track 4	Tanzania	• Developing countries face challenges relating to deficits in technology know-how, infrastructure and digital literacy.