Towards a Multilateral Consensus on Data Governance

*Alan Ichilevici de Oliveira, Kateryna Heseleva, and Vincent Jerald Ramos**

18 May 2020

"Fragmented approaches to governance do more harm than good. Nations could and should take part in international agreements to converge data-related policies, but still preserve the nations' policy sphere and sovereignty to data governance."

Abstract: To recouple the benefits of increased digital trade with human and societal well-being on a global level, countries must achieve a consensus on how to regulate data. Past international discussions have shown that while countries have significantly varying approaches to data governance, consensus can still be reached on many issues. This *Policy Brief* highlights a feasible and multilaterally agreeable data governance framework that is anchored on two pillars: (1) promote interoperability; and (2) establish global governance rules and norms. Each pillar consists of more specific and actionable policy recommendations that follow through prior international work. We conclude with a recognition of the G20's role as a strong multilateral forum where this consensus can be reached. Indeed, this *Policy Brief* bridges the silos between data governance, international cooperation, and growth in pursuit of proposing a data governance framework that works for all.

Challenge

Data is increasingly becoming one of the most important resources of the 21st century, greatly affecting how industries, nations and societies develop. In 2019, there were about 4.13 billion internet users around the world, a 900 percent increase from the same statistic two decades ago. Goods and services flow across borders through digital platforms at an unprecedented rate.

However, approaches to data governance vary significantly across countries and, even in countries where data-related laws exist, enforcement mechanisms might not be in place (López González and Ferencz, 2018). This fact is reflective of a larger problem of regulation

*The authors are Master of Public Policy students at the Hertie School, Berlin. This Policy Brief was prepared in partial fulfillment of the requirements of the course G20 Policy Issues and Recommendations, Spring Semester 2020. The authors would like to thank Prof. Dr. Dennis Snower for his constructive feedback. Their views do not represent those of the Hertie School, or their other present affiliations. All remaining errors are theirs alone.

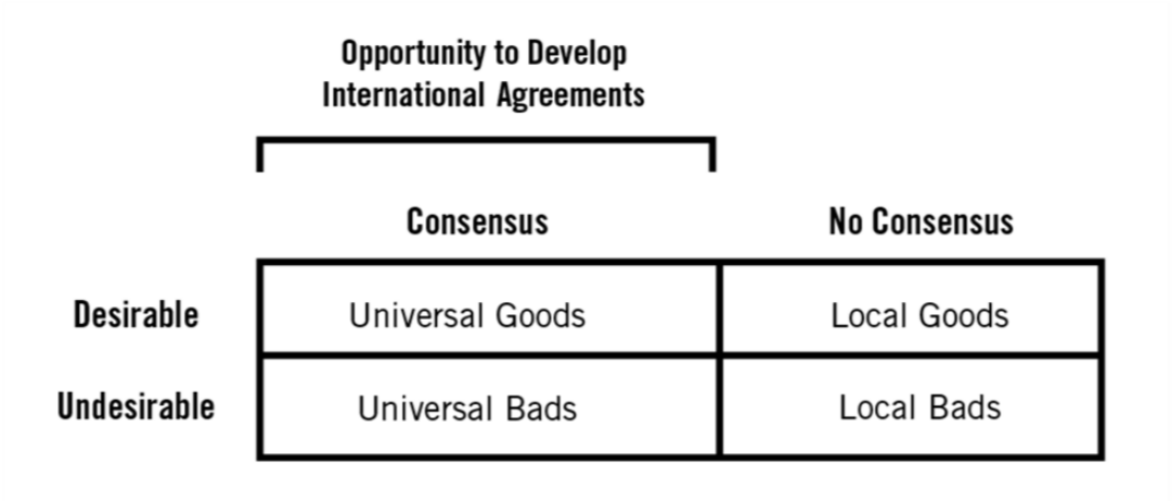

Figure 1: Typology of Internet Policy Goals. Source: https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust

in the digital economy. Government regulations on how data should be regulated, stored, transferred and processed are non-existent at worst and fragmented at best.

Such divergence in regulation ultimately leads to a divergence in standards and experiences in the Internet of Things (IoT). For instance, while some nations are treating privacy as a human right and making great efforts to preserve users' information and anonymity, other governments are enforcing strong state control and content censorship. Many nations demand data to be stored locally and impose limitations to data transfers outside their borders.

Understandably, governments want as much control over data for security and protectionism reasons. Nevertheless, fragmented approaches to governance do more harm than good. Nations could and should take part in international agreements to converge data-related policies, but still preserve the nations' policy sphere and sovereignty to data governance. By creating a governance framework which facilitates free data flows, while ensuring cybersecurity and trust, all nations would benefit and still decide how to regulate data. In doing so, nations would develop common solutions to address issues where there is a broad global consensus about desirable "universal goods" and undesirable "universal bads" (Cory, Atikson and Castro, 2019).

Finally, the discussion of data governance and the digital economy has indeed become abstract and complex. This Policy Brief attempts to go back to basics and ask more fundamental questions. What is our universal understanding of data? How can countries agree on data interoperability to maximally reap the benefits of digital trade? What global rules and norms should be put in place? From this point, countries can start recouping the silos between data governance, international cooperation, and growth.

PILLAR 1: Promoting Data Interoperability on a Global Level

In the absence of a universally accepted definition of interoperability as it pertains to data governance, Kerber and Schweizer (2017) broadly characterizes it as "the ability of a system, product or service to communicate and function with other (technically different) systems, products or services." The main benefits of interoperability are two-pronged– efficiency and security. Take two economic agents who want to exchange information via two technically different systems. With interoperability, transaction costs are reduced and data is more secure since agents would no longer need to invest in a new system just to "read" the new information. Agents would also no longer need the services of a third party who will convert the information into a format that is readable by their systems. This promotes efficiency through cost-savings and improves security through exchanging information directly. However, we recognize that promoting interoperability entails financial costs and risks on innovation and competition. Hence, following Kerber and Schweizer (2017), we likewise recommend a context-specific optimal degree of interoperability that achieves efficiency and security.

Indeed, any consensus on data governance should begin with a recognition that data is anchored in human identity. In the definitions of data in various national statutes and multilateral agreements, there seems to be one lacking element: identity. Simply put, data is a resource which contains information that is ultimately about people (Lovelock, 2018). Hence, it ought to be protected and handled properly by whoever is in possession. This definition, as it is, does not bring up any contestable aspects of "identity" such as human rights, data privacy, and freedom of information, which may be met with hesitation by some States. Therefore, we believe that such a definition of identity in data can be agreed upon by most, if not all, countries. Therefore, the foundation of the two specific proposals under this pillar is the recognition that data is anchored in human identity and should be safeguarded and traded with care.

Proposal 1: Support data flows through encryption

The whole discussion of interoperability matters because of the underlying assumption that agents (individuals, firms, countries, etc.) want to exchange data. Therefore, as data flows from one agent to another, there has to be a mechanism by which the information contained in the data reaches its desired recipient. With this mechanism in place, interceptors are unlikely to obtain and access secure data. Encryption is the key technology that agents use to ensure data security and confidentiality (GSMA, 2018). It is a precondition for data to flow with trust. Therefore, governments should support, and not undermine, encryption's role in securing data flow. Governments around the world have in different ways attempted to undermine encryption, including: requiring to license encryption with government agencies, imposing a government-mandated encryption standard, prohibiting end-to-end encryption which allows leakages and loopholes to be present, and advocating for backdoor government access. These policy measures defeat the purpose of encryption. Encrypted data with backdoors and leeways for government access are prone to interceptors and cybercriminals as well. We encourage governments to secure the data of their individuals, firms, and states

through encryption without interference.

Proposal 2: Protect data flows without constraints on domestic localization policies

Data localization– which implies that data collected from a country should be stored within the borders of that country, is arguably one of the more contentious provisions in the data governance debate. Think of it as a spectrum. Under extreme localization, data should be stored within the borders of a country and under no circumstances will it be allowed to be transferred elsewhere. On the other end of the spectrum, no localization, there is no regulation as to where collected data should be stored. Countries occupy significantly different points on the spectrum. India has advocated for relatively strong localization of personal data[1], whereas the US, Mexico, and Canada have recently adopted a provision that entirely rejects localization[2]. We propose a consensus on data protection that does not bound or limit a country's localization policy.

Are proposals that aim to protect data flows without binding countries' localization policies unlikely to be effective? The short answer is no. There have been successful multilateral attempts to promote and protect data flows without specific provisions on what the country's localization policies ought to be. One of which is the Cross Border Privacy Rules System of the Asia-Pacific Economic Cooperation (APEC CBPR)– a model framework for protecting personal data flows across the APEC region. It is a voluntary and accountability-based system which should be accepted by a country first, followed by a certification of an accountability agent that a firm or organization is compliant with the standards. CBPR's objective is not to impose a binding law or regulation on the protection of personal data but to facilitate data transfers that meets a certain threshold of data protection parameters (Sullivan, 2019).

The voluntary nature of the CBPR, as well as its explicit intention to balance the promotion of data transfers with protection of personal data, strengthens its appeals to countries regardless of their stance of localization. USA, Mexico, and Canada– all of which have rejected localization, are part of the CBPR. However, the Philippines and Australia, both of which have no explicit general positions on localization, are also part of the system. Therefore, can different countries with different localization regulations ever find a consensus for data protection? The answer is yes and the CBPR shows it's possible.

Related Policy Implementations

In this section, we proposed two specific recommendations to support and complement the promotion of interoperability on a global level. To operationalize this vision, we recommend a related policy recommendation for countries to explicitly recognize data protection and

[1] Article 40(1) of the 2018 draft of the Personal Data Protection Bill in India, to wit: *"Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies"*

[2] Article 19.12 of the US-Mexico-Canada Agreement (USMCA), to wit: *"No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."*

interoperability as objectives in its laws and regulations and appoint enforcement authorities. Further, we recommend countries to coordinate and form a voluntary and accountability-based mechanism for data flows and data protection, similar to the APEC CBPR.

PILLAR 2: Establishing Global Data Governance Rules and Norms

Japan's Prime Minister, Shinzo Abe, used the country's G20 presidency in 2019 as a spotlight to advocate for the creation of a set of international rules which would enable the free movement of data across borders. 'Data Free Flow with Trust', as this concept is known, promotes finding common ground for worldwide data governance and establishing a common legal framework. According to Koizumi (2019), "although the idea of free data flows is not new, the inclusion of 'trust' is". The innovation in this proposal relies on the fact that trust is placed centrally for the success of a global data governance framework. By developing and enforcing common data governance rules and norms, supported by efficient cooperation mechanisms and strong cybersecurity measures, data can flow in a secure environment. Hence, we build on Abe's contribution and recommend that domestic data governance become part of a global cooperation trust-based framework with adequate cooperation instruments allied to strong local law enforcement.

Proposal 3: Strengthen Law Enforcement and Cooperation Mechanisms

For a trust system to work, it is important that rules are followed and wrong-doers face the consequences of their actions. Firms doing business in a country should be held accountable to national laws regardless of where they store, process or transfer data. Hence, a clear and efficient legal framework should be established to facilitate access to data stored in other jurisdictions for legitimate investigation purposes. This way, companies would still be subject to national laws and would not be able to escape regulations by transferring data overseas. Similarly to international financial markets, where firms must comply with a country's local regulations even if they are operating from abroad or sending money to another country, so must be the case of companies using data acquired within a country.

For this to happen, cooperation procedures must be revised and enforcing mechanisms standardized. Many international cooperation treaties are outdated and excessively time-consuming. Conflicting national laws jeopardize the efficiency of cooperation mechanisms, and local agencies have significantly different enforcement capabilities, depending on their available resources and the legal systems they have.

Countries should negotiate a new multilateral agreement to establish the grounds for this framework to work. This includes settling matters of jurisdiction and establishing cooperation protocols while preserving countries' sovereignty. Regulations will inevitably be different in each country, according to governments' priorities and values. Still, an adequate cooperation protocol will allow the coordinated action of law enforcement bodies in case of businesses

violating national regulations and trying to escape consequences by storing or handling data abroad.

Proposal 4: Combine multilateralism with multistakeholderism

Even though cooperation among nations is a key element for global data governance success, governments are not alone in this process. The complexity of this issue surpasses multilateralism's limitations. A holistic approach is fundamental to develop global mechanisms of digital cooperation. By acknowledging the interdependence of stakeholders and sectors, the world can move together towards better digital solutions. The combination of multilateralism and multistakeholderism creates the proper environment for Global Data Governance.

By engaging all stakeholders to work on an agreed problem set, the global community can develop resilient political commitment around the topic of digital governance. Governments play a central role in this discussion, but they are not alone. The private sector, the academic community, the technical community and civil society must take part in developing the digital ecosystem.

Technological innovations, content production, cybersecurity measures, ethical implications, societal change, economic development, network management and privacy are some of the issues which must be taken into consideration in this discussion. Combining so many aspects and points of view is extremely challenging, but by getting everyone on the same page, solutions arise. It is possible to make the analogy to the climate debate: once the majority of stakeholders accepted that climate change is real and immediate action is necessary, the world shifted towards addressing the issue.

Proposal 5: Adapt digital assessment methodology

One of the obstacles for efficient multilateral data governance is the absence of quantitative methodologies to rely on during policy-making and to assess the effectiveness of implemented policies. One of the reasons behind that is that countries use different approaches to data collection and evaluation. Therefore, data collection is uneven and comparing evidence from different countries is challenging (The Age of Digital Interdependence, p. 23). Introducing common methodology will bring more clarity into discussions on data governance, enable even flow of data and ensure consistency into measures taken by G20 member states. The recommended methodology is digital assessment, which has been used by the EU institutions in order to relate human rights issues to existing digital technologies. Digital assessment questions may be formulated in the following way: 'Are there ICT influencing the way the problem is formed' or 'Are there visible trends on how digitalization can change the nature of existing challenges' (Lovelock, 2018, p. 48). This method can be also used to ensure that private data is collected in accordance with internationally accepted guidelines. The Organization for Economic Development and Cooperation (OECD) developed Guidelines on the Protection of Privacy and Transborder Flows of Personal Data that lays out principles of the lawful use and sharing of personal information for the public and private sector. These principles highlight that private data can only be collected with consent, the purpose for data collection should be specified and that personal data cannot be disclosed externally

without prior consent (Privacy, Data and Technology, 2018). Adopting digital assessment methodology will enable G20 member states to take advantage of opportunities to ensure human rights and social cohesion in the digital economy.

Proposal 6: Appoint a special committee on human rights in digital economy

In 2015, the UN Human Rights Council established a position of the Special Rapporteur on the right of privacy who concentrates on specific applications of human rights in data governance, examines and reports back the situation in every country (Donahoe, 2014). G20 can follow this example and appoint a special committee that will include academia, researchers, analysts, and representatives of non-governmental and international organizations, whose responsibilities will include developing relevant guidelines, providing G20 member states with actionable recommendations on enshrining human rights, especially right to privacy, in their respective domestic policies. The special committee will support G20 members in bringing the human aspect of data governance, ensuring multilateral agreement, and converging national regulations on fundamental human rights in the digital economy.

Related Policy Implementations

Several initiatives around the world work to establish and improve Global Data Governance. The Internet Governance Forum (IGF), for example, promotes an annual inclusive debate process between governments, the private sector, civil society, and the technical and academic communities. The International Consumer Protection Enforcement Network (ICPEN) connects the consumer protection law enforcement authorities of 64 member countries and promotes their cooperation. And the APEC Cross-border Privacy Enforcement Arrangement (APEC CPEA) promotes information sharing among Privacy Enforcement Authorities in APEC economies. Based on the models of IGF, ICPEN and APEC CPEA, we recommend that law enforcement cooperation mechanisms be strengthened and a multistakeholder approach is combined to the multilateral negotiations currently in place. Besides, the EC has also adopted digital assessment methodology that allows them to identify possible human rights related implications of information and communication technologies (ICT) in a timely manner and come up with solutions that are likely to be accepted by stakeholders (Lovelock, 2018).

Conclusion and the Role of the G20

This Policy Note presents two pillars where multilateral consensus on global data governance can be achieved moving forward. First, countries should promote interoperability on a global level to achieve security and efficiency but this commitment should not come at the expense of sacrificing the policy sphere and sovereignty of the signatories for this consensus. Second, countries should begin to recouple the fragmented approaches to data governance and establish global rules and norms to ensure that countries follow through their international

commitments, translate commitments to actionable policy reforms, continue to share best practices with the global community.

However, there needs to be an effective multilateral forum where this consensus can be advocated in the G20, an international forum of the world's largest economies, is one of the few avenues where multilateral consensus on data governance can be reached. The G20's legitimacy and gravitas in global data governance suits the transnational nature of the digital economy. Apart from connecting heads of governments in annual conferences, it connects ministers and senior officials through the Sherpa track, as well as non-state stakeholders through engagement groups. This is crucial as lack of trust and communication among key stakeholders creates obstacles to finding a multilateral consensus on data governance. In these forums, consensus on basic principles of data governance within the G20 is expected to ripple through domestic policies and data governance policies of countries can finally start to converge. This is the role that the G20 can see itself playing in consolidating a meaningful consensus on a data governance framework that works for all.

Literature Review

Asia-Pacific Economic Cooperation (APEC). APEC Cross-border Privacy Enforcement Arrangement (CPEA). From: https://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Cross-border-Privacy-Enforcement-Arrangement

Cory, N., Atkinson, R. and Castro, D. (2019). Principles and Policies for "Data Free Flow With Trust". ITIF. From: https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust

Donahoe, E. (2014). "Human Rights in the Digital Age". Human Rights Watch. From: https://www.hrw.org/news/2014/12/23/human-rights-digital-age.

GSMA (Global Systems for Mobile Communications Association) (2018). Cross Border Data Flows: Realising Benefits and Removing Barriers.

Hutt. R. (2015). "What Are Your Digital Rights". World Economic Forum. From: https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer/

Internet Governance Forum (2019). Towards a Global Framework for Cyber Peace and Digital Cooperation: An Agenda for the 2020s.

International Consumer Protection Enforcement Network (ICPEN). Who we are. From: https://www.icpen.org/who-we-are

Kerber, W. & Schweitzer, H. (2017). Interoperability in the Digital Economy. Journal of Intellectual Property, Information Technology, and E-Commerce Law. 8(39) para 2.

Klang, M. & Andrew, M. (2016). Human Rights in the Digital Age. Routledge.

Koizumi, M. (2019). Japan's pitch for free data flows 'with trust' faces uphill battle at G20 amid 'splinternet' fears. Japan Times. From: https://www.japantimes.co.jp/news/2019/06/27/business/tech/japans-pitch-free-data-flows-trust-faces-uphill-battle-g20 -

amid-splinternet-fears/

Kreutz, C. (2018). "Introduction to Digital Human Rights". Crisscrossed. From: https://www.crisscrossed.net/2018/11/08/Introduction-human-digital-rights/

Latonero, M. (2018). "Governing Artificial Intelligence: Upholding Human Rights & Dignity". Data&Society. From: https://datasociety.net/library/governing-artificialintelligence/

López González, J. & Ferencz, J. (2018). "Digital Trade and Market Openness", OECD Trade Policy Papers, No. 217, OECD Paris. http://dx.doi.org/10.1787/1bd89c9a-en

Lovelock, P. (2018). "Framing Policies for Digital Economy. Towards Policy Frameworks in the Asia-Pacific". United Nations Development Programme, Singapore. From: https://www.undp.org/content/dam/undp/library/capacity-development/English/Singapore%20Centre/FramingPolicies_DigitalEconomy_2018_NUS-UNDP.pdf

New Zealand Human Rights Commission. (2018). Privacy, Data and Technology: Human Rights Challenges in the Digital Age. Auckland. From: https://www.hrc.co.nz/files/5715/2575/3415/Privacy_Data_Technology_-_Human_Rights_Challenges_in_the_Digital_Age_FINAL.pdf

Office of the United Nations High Commissioner for Human Rights. (2018). A Human Rights-Based Approach to Data. Geneva, Switzerland. From: https://www.ohchr.org/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf

Organization for Security and Cooperation in Europe. (2018). Declaration on Digital Economy as a Driver for Promoting Co-operation, Security and Growth. Ministerial Council, Milan. From: https://www.osce.org/chairmanship/405920?download=true

Schwarzer, J., et al. (2019). The Digital Economy for Economic Development: Free Flow of Data and Supporting Policies. G20 Insights Policy Briefs.

Shull, A. (2018). "The Charter and Human Rights in the Digital Age". Centre for International Governance Innovation. From: https://www.cigionline.org/articles/charter-and-human-rights-digital-age

Sullivan, C. (2019). EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era. Computer Law & Security Review. doi:10.1016/j.clsr.2019.05.004

United Nations Conference on Trade and Development. (2019). Secure Identities Can Booth Inclusivity in the Digital Economy. From: https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2050

UN Secretary-General's High-Level Panel on Digital Cooperation. The Age of Digital Interdependence. From: https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf