Of Binding Provisions and Trust Marks; Roadmap to a Global Legal Framework for the Digital Economy

Arnoud Willems* & Maryanne Kamau*

The digital economy is dynamic, fast expanding, and truly global. The legal framework that currently applies to the digital economy is either divided, fragmented, ad hoc*, out of date, or non-existent. Some legal initiatives quixotically aim at stopping cross-border data flows, reflecting consumer fears regarding privacy and security or government fears about losing tax revenue. The fragmented regulatory environment does not help companies 'scale up' digital technologies; in turn, this hampers innovation and global economic growth. In addition, some less digitally developed actors complain that current rules allow or even foster unfair competition.*

This article proposes a new and global legal framework for the digital economy: structured cooperation between states and companies under the administration of an autonomous body. States may resist giving up sovereignty, and citizens may fear erosion of their legal rights. However, uniform, consistent, and enforceable rules would benefit both states and citizens. Tax revenue could be fairly assessed and distributed, for example, and citizens and businesses would no longer face divergent privacy and security rules. Regulation would become more legitimate because both public and private stakeholders would participate in rulemaking, including smaller players and digital latecomers. Companies that subscribe to the framework would receive a global 'trust mark' that would boost consumer confidence. In sum, a global legal framework, as contemplated, would match the global character of activities in the digital economy.

1 INTRODUCTION

The digital revolution has permeated nearly all modern economic and social activities and altered the conduct of business and social interaction. Nowadays, approximately 12% of the global trade in goods is conducted online via e-commerce platforms,[1] while 50% of all traded services are enabled by information and communication technologies.[2]

* Arnoud Willems and Maryanne Kamau are lawyers with Sidley Austin LLP in Brussels. Any errors or omissions are the authors' own. The views expressed in this article are exclusively those of the authors. The article has been prepared for academic purposes only and does not constitute legal advice. Emails: awillems@sidley.com & mkamau@sidley.com.

1 J. Manyika, S. Lund, J. Bughin, , J. R. Woetzel, K. Stamenov & D. Dhingra, *Digital Globalization: The New Era of Global Flows* vol. 4 (San Francisco: McKinsey Global Institute 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows.

2 UNCTAD, *Information Economy Report, Trends and Outlook in Turbulent Times* (2009), http://unctad.org/en/docs/ier2009_en.pdf.

Willems, Arnoud & Kamau, Maryanne, 'Of Binding Provisions and Trust Marks; Roadmap to a Global Legal Framework for the Digital Economy'. *Legal Issues of Economic Integration* 46, no. 3 (2019): 225–246.

At the end of 2017, approximately 3.6 billion people in the world had an online presence.[3] Digitalization has also led to innovations such as cloud computing, blockchain, the internet of things (IOT), 3D printing, and artificial intelligence (AI). These innovations unlock the potential for both digital and brick-and-mortar companies to trade goods and services more efficiently.

In addition, the use of data has evolved from being a business asset to being critical to all aspects of human life. With the IOT and embedded systems, modern devices are increasingly digital and connected to the internet. The volume of data generated in the world is estimated to grow to 163 zettabytes by 2025.[4] Likewise, the world market for data is estimated to exceed USD 67 billion in 2021.[5]

Unfortunately, the legal framework for the digital economy has failed to keep up. The current unbalanced legal environment hampers business growth, puts consumers at risk, and creates dissensions amongst governments.[6] Some aspects of the digital economy, for instance the development and use of AI, have escaped regulatory control; there are no rules to cover them.[7] Where rules do exist, they are fragmented across countries and international bodies, are largely inadequate or too restrictive resulting in risks of abuse by some companies advancing business interests and countries pursuing protectionist policies.

The incoherence of the existing framework creates needless administrative burdens and compliance inconsistencies (risks) that lead to huge opportunity losses for businesses.[8] In the European Union (EU) for example, the European Commission (Commission) estimates that small online businesses incur extra costs of around EUR 9,000 to comply with the different national legal frameworks. Interestingly, the Commission estimates that regulatory coherence for the digital economy in the EU would push at least 57% of companies to start or increase their online sales to other EU countries.[9]

This article proposes reform of the regulation of the digital economy. Section two starts with a definition of the digital economy, without which no effective regulation is

---

3 Broadband Commission, *The State of Broadband: Broadband Catalyzing Sustainable Development ITU* (2017).

4 IDC white paper *Data Age 2025: The Evolution of Data to Life-Critical* (2017), https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.

5 Yohan Lecuyer, *The Data Rush: The 20th Century's Colourless Gold* (2018), https://blog.altima-agency.com/en/analytics_en/the-data-rush-the-20th-centurys-colorless-gold-analytics-experience-ux/.

6 *See* e.g. MNE Tax, *OECD Report Reveals Disagreement on Taxation of Digital Firms* (16 Mar. 2018), https://mnetax.com/oecd-interim-report-reveals-disagreement-among-nations-on-taxation-of-digital-firms-26655.

7 Although OECD Artificial Intelligence Principles were released on 22 May 2019, they do not impose binding rules on AI. *See* e.g. Politico, *US to Endorse New OECD Principles on Artificial Intelligence* (19 May 2019), https://www.politico.eu/article/u-s-to-endorse-new-oecd-principles-on-artificial-intelligence/.

8 International Chamber of Commerce (ICC), *ICC Contribution to the Intergovernmental Group of Experts on E-commerce and the Digital Economy, Consultation Fostering Development Gains from Domestic and Cross-border E-commerce in Developing Countries* (2018), https://cdn.iccwbo.org/content/uploads/sites/3/2018/04/icc-contribution-digital-economy-2018-1.pdf.

9 Digital Single Market Factsheet, https://ec.europa.eu/commission/sites/beta-political/files/dsm-factsheet_en.pdf.

possible. Section three highlights the weak points of the current (fragmented) legal framework: ad hoc and protectionist national regulation; 'silo-based' initiatives at the bilateral, regional, or plurilateral level; and unenforceable WTO efforts based on old trade-in-services concepts. Section four describes the legal and structural form that the proposed framework could undertake. Section five develops further several substantive areas that new digital rules could address: data localization, taxation, privacy, security, establishment restrictions, and intellectual property rights.

2 SCOPING THE DIGITAL ECONOMY: DEFINITION AND ECONOMIC IMPACT

2.1 Defining the digital economy

Without a coherent legal definition of the digital economy, it is impossible to determine how to apply any legal initiative. However, no agreed upon definition of the digital economy exists.[10] This has led either to a broad approach that encompasses all economic activities based on digital technologies[11] or to a narrow approach that focuses only on specific components of the digital economy such as e-commerce.[12]

This article considers the digital economy as a broad network of producers, suppliers and consumers of goods and services. This network is enabled by digital technologies and characterized by:

(1) infrastructure that supports digital connectivity, including both hardware (such as servers, data centres and optical fibre) and software;
(2) digital platforms providing an interface for interaction between users or between consumers and suppliers;
(3) e-commerce, including payment systems enabling trade in goods and services;
(4) digital services that are either necessary for or incidental to digital connectivity;
(5) electronic devices providing access to the digital world; and
(6) the generation and use of data.

---

10 R. Bukht & R. Heeks, *Defining, Conceptualizing and Measuring the Digital Economy*. Development Informatics Working Paper, 68 (2017).

11 EC, *Expert Group on Taxation of the Digital Economy* (Brussels: European Commission 2013), https://ec.europa.eu/taxation_customs/sites/taxation/files/resources/documents/taxation/gen_info/good_governance_matters/digital/general_issues.pdf.

12 OECD, *The Digital Economy* (Paris: OECD 2013), http://www.oecd.org/daf/competition/The-Digital-Economy-2012.pdf. *Cf.* The World Trade Organization Work Programme on Electronic Commerce defines e-commerce as 'the production, distribution, marketing, sale or delivery of goods and services by electronic means.'

2.2 Impact of the digital economy on global economic growth

Due to the definitional challenge highlighted above, measuring the digital economy using conventional tools has proven to be a daunting task.[13] However, some general conclusions can be drawn about the impact of the digital economy on the global economy. These conclusions are based on readily available data about some components of the digital economy mentioned in section 2.1.

In 2016, a World Bank study indicated that a 10% increase in broadband penetration in an exporting country results in a 1.9% increase in exports, while a similar increase in an importing country results in a 0.6% increase in bilateral exports.[14] McKinsey reported that cross-border data flows generated USD 2.8 trillion in economic value in 2014, a far greater effect on world gross domestic product (GDP) than trade in goods.[15] In a separate analysis examining the G8 and five other countries (Brazil, China, India, South Korea, and Sweden), the internet was reported to account for 3.4% of GDP and to have created a 10% growth in the productivity of small- and medium-size enterprises (SMEs).[16]

The 2017 United Nations Conference on Trade and Development (UNCTAD) Information Economy Report indicates that worldwide e-commerce sales in 2015 reached USD 25.3 trillion. As concerns the information and communications technology (ICT) sector, production of ICT goods and services accounts for 6.5% of global GDP. Interestingly, despite concerns about the impact of automation on global employment, the UNCTAD Report shows that the ICT service sector employed over 100 million people globally. This suggests that the digital economy is vital for job creation.[17] Evidently, the remarkable growth of the digital economy will make it a large part of the world's entire economy, a trend that should focus the attention of policy makers on the digital economy.

Despite the rapid growth of the digital economy, however, there is much uncertainty. Given the cross-border nature of activities in the digital economy, businesses face different national rules and encounter barriers to scaling up digital technologies. Global harmonization of these rules would help more businesses realize the benefits of the digital economy and rapidly facilitate growth.

Similarly, consumers and users are uncertain about whether their legitimate interests are protected. They argue that business interests should not prevail over the interests of consumers and other users interacting with digital technologies. The increased focus on

---

13 Bukht & Heeks, *supra* n. 10.

14 A. Osnago & S. W. Tan, *Disaggregating the Impact of the Internet on International Trade*, The World Bank (2016).

15 Manyika, Lund, Bughin, Woetzel, Stamenov & Dhingra, *supra* n. 1.

16 Olivia Nottebohm, James Manyika & Michael Chui. *Guest Column: Sizing the Internet Economy in Emerging Countries* (2012), https://www.mckinsey.com/mgi/overview/in-the-news/sizing-the-internet-economy-in-emerging-countries.

17 United Nations Conference on Trade and Development (UNCTAD) Information Economy Report 2017, https://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.

digital technologies by businesses exposes users to security risks, data exploitation and privacy violation risks, especially in the absence of an effective legal framework.[18] Policy makers need to focus their legislative attention towards a fit-for-purpose legal framework that balances growth of the digital economy and protecting public interests.

3 REGULATING THE DIGITAL ECONOMY: WHY REFORM IS NEEDED

The digital revolution has disrupted traditional economic activities and forged new opportunities that escape regulatory control, either because rules are lacking or because the existing rules are inadequate to govern aspects of the digital economy. As a result, the existing global legal framework has several weak points which call for reform.[19] Rules may be lacking or inadequate because regulatory initiatives are limited to the national level; because multilateral initiatives are imprecise and out of date; or because there are splits between digitally developed and undeveloped countries and between 'standard-setting' and 'standard-taking' actors in the system.

3.1 A FRAGMENTED LEGAL APPROACH TO THE DIGITAL ECONOMY

When regulation of the digital economy does take place, it is for the most part in the national legal order. Most countries subject digital economy actors to their existing laws to the extent that these laws apply. These national laws differ considerably per country. The only exception to this national approach is the EU's ongoing plan to create a digital single market. In 2015, the European Commission launched the digital single market strategy, which is aimed at harmonizing digital economy rules in the EU, removing regulatory barriers, and moving twenty-eight national digital markets to a single one.

In the international context, the legal framework regulating the digital economy is as fragmented as in the national level. Rules are negotiated using a 'silo-based format.'[20] As a result, different international fora – at the bilateral, regional, plurilateral or multilateral levels – take up legal initiatives focusing on different aspects of the digital economy. The multiplicity of platforms where discussions on rules are taking place (and the different scope of these discussions) prevents progress towards any kind of legal uniformity.

---

18 OECD, *Financial Markets, Insurance and Private Pensions: Digitalisation and Finance* (2018), http://www.oecd.org/finance/Financial-markets-insurance-pensions-digitalisation-and-finance.pdf.

19 *Global E-Commerce: Impacts of National Environment and Policy* 384 (Kenneth L. Kraemer, J. Dedrick, N. P. Melville & K. Zhu eds, Cambridge University Press 2006).

20 Huawei Europe, *Trade and the Digital Economy*, white paper (Oct. 2017), https://huawei.eu/sites/default/files/17.11.30%20White%20Paper%20Trade%20Rules%20and%20the%20Digital%20Economy%20Full%20EN%20Final.pdf.

Figure 1.1 Examples of International Fora and Initiatives Regulating the Digital Economy

International body	Applicable rules/regulatory initiatives
World Trade Organization (WTO)	Work Program on E-commerce
	General Agreement on Trade in Services (GATS)
	GATS Annex on Telecommunications
	Information Technology Agreement (ITA)
	Telecoms Reference Paper
	Understanding on Commitments in Financial Services
	Trade-Related Intellectual Property Rights Agreement (TRIPS)
	Ministerial Declaration on Duty-Free Moratorium on Electronic Transmissions
	Joint Statement Initiative (2017 and 2019)
Organization for Economic Co-operation and Development (OECD)	G20/OECD BEPS Project addressing the tax challenges of the digital economy
	Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data
United Nations Commission on International Trade Law (UNCITRAL)	Model Law on Electronic Commerce, 1996
	Model Law on Electronic Signatures, 2001
	Model law on Electronic Transferable Records, 2017
	United Nations Convention on the Use of Electronic Communications in International Contracts, 2005
	Working Group IV: Electronic commerce
Asia-Pacific Economic Cooperation (APEC)	Privacy Framework the Cross-Border Privacy Rules
World Customs Organization (WCO)	WCO Working Group on E-Commerce
International Telecommunication Union (ITU)	Recommendations of the Standardization Sector (ITU T-Recs)
	International Telecommunication Regulations
	Broadband Commission for Digital Development, 2010 (ITU and UNESCO)
	Connect 2020 Agenda for Global Telecommunication/ICT Development
World Intellectual Property Organization	Intellectual property rights relating to the digital economy
United Nations Conference on Trade and Development (UNCTAD)	eTrade for All

With the exception of the WTO, the initiatives in international intergovernmental fora are often espoused in the form of 'soft law': declarative statements, model laws, and guiding principles that cannot be enforced.[21] Although the WTO trade agreements do not contain specific rules for the digital economy, key components that intersect with trade are covered in the substantive rules of various agreements

[21] UNCTAD, *New Digital Era Must Ensure Prosperity for All, United Nations Says*, Information Economy Report (2017), http://unctad.org/en/PublicationsLibrary/ier2017_en.pdf.

like the Information Technology Agreement, (ITA),[22] the General Agreement on Trade in Services (GATS),[23] the GATS Annex on Telecommunications,[24] the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the WTO Trade Facilitation Agreement (TFA).[25]

However, WTO rules are outdated. Except for the TFA, these rules were developed before 1994; at that time, the current digital innovations did not exist or were not in wide use. WTO members realized the need to examine the 'cross-cutting' issue of the effect of e-commerce on global trade and created the Work Programme on Electronic Commerce in 1998.[26] To date, little progress has been made.[27]

This stalemate on the WTO negotiations has pushed countries towards bilateral, regional and plurilateral trade negotiations. It is estimated that as of September 2017, at least sixty-nine free trade agreements (FTAs) had an e-commerce chapter or specific provisions dedicated to e-commerce.[28] This number continues to grow in view of more recent accords such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), or the United States–Mexico–Canada Agreement (USMCA), which is pending ratification. The main issues covered in FTAs relate to broader trade discussions outside the WTO such as IP protection of digital products and prohibition on data localization. FTA provisions relating to e-commerce can be broadly categorized into market access, rules or facilitation commitments.[29]

3.2 Divided and conflicted rulemaking for the digital economy

The current approach to rulemaking for the digital economy needs rethinking; current legal initiatives are characterized by conflict and division and mainly have a local focus. First, the digital divide between the developed and developing world is a

---

22 *See* WTO Ministerial Declaration on the Expansion of Trade in Information Technology Products (16 Dec. 2015),https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=225713,133572&CurrentCatalogueIdIndex=0&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True.

23 *See* WTO case law on GATS. *Mexico-Telecoms, US-Gambling, China- Publications and Audio Visual Products* and *China- Electronic Payments*.

24 GATS Annex on Telecommunications, para. 5(a) and 5(c).

25 Art. 7.1 & 7.2 of the WTO Trade Facilitation Agreement, https://www.wto.org/english/docs_e/legal_e/tfa-nov14_e.htm.

26 Work Programme on Electronic Commerce, Adopted by the General Council on 25 Sept. 1998, and Geneva, http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm.

27 *See* Item 4 – Work Programme on Electronic Commerce – Review of Progress, Report by the Chairman, WT/GC/W/756 (17 Dec. 2018).

28 Wu, Mark. 2017. Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System. RTA Exchange. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB).

29 Amir Ebrahimi Darsinouei, *Understanding E-Commerce Issues in Trade Agreements: A Development Perspective Towards MC11 and Beyond*, Geneva. CUTS International, Geneva, 11 (2017), http://www.cuts-geneva.org/pdf/STUDY%20-%20E-Commerce%20Towards%20MC11.pdf.

vast and expanding one owing to infrastructure deficits, lack of access to online connectivity, and insufficient digital literacy.[30] This is the first split. Not surprisingly, these disparities reflect in the divergent priorities taken up by governments on policy making for the digital economy.

Second, countries appear to be split into either a standard-setting or standard-taking role regarding rulemaking. In efforts to shape the digital economy and secure their future as global powers, standard-setting countries have taken the lead and introduced rules.[31] These rules are meant to serve as model laws that standard-taking countries then align with. Such dominance by standard-setting countries locks out certain countries from weighing in on the discussions.

Third, as hinted at above, there are splits within the group of standard-setting countries. For example, countries like the United States adopt a liberal approach that promotes openness of the internet and the removal of global digital trade barriers through the conclusion of FTAs with digital trade provisions. While countries such as EU Member States advocate for greater government intervention to protect consumers and promote fair competition in the digital economy, other countries, like China, are considered to take a more controlling approach and prioritize domestic industrial policies over foreign trade.

Standard-taking countries that trade with all standard-setting countries thus face conflicting interests in determining the regime to align with. The choice of one over another could have serious political and economic ramifications. Using hypothetical examples, Aaronson and Leblond (2018) explore for instance, the conflict that would potentially arise for Canada and Mexico in choosing which regime to align with as they both have FTAs with the EU and the US. Similarly, countries in the African region would perhaps face a choice between the European or Chinese regime given their historical ties to Europe and the increasing presence of Chinese investments in their countries.[32]

In other words, without a proper global legal framework, control of economic activities in the digital world is left to a few standard-setting actors. The EU, for example, is making strides in creating a digital single market. In 2018, as part of this initiative, the EU adopted a data protection regime under the General Data Protection Regulation (GDPR) that is already being replicated in several countries. But one must assume that the EU (and other leading economies) will try to skew the conditions of the market in their favour.[33] To think otherwise would be delusional.

---

30 Huawei Europe, *Trade and the Digital Economy*, white paper (Oct. 2017), https://huawei.eu/sites/default/files/17.11.30%20White%20Paper%20Trade%20Rules%20and%20the%20Digital%20Economy%20Full%20EN%20Final.pdf.

31 S. A. Aaronson & P. Leblond, *Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO*, 21(2) J. Int'l Econ. L.(2018).

32 *Ibid*., at 25–26.

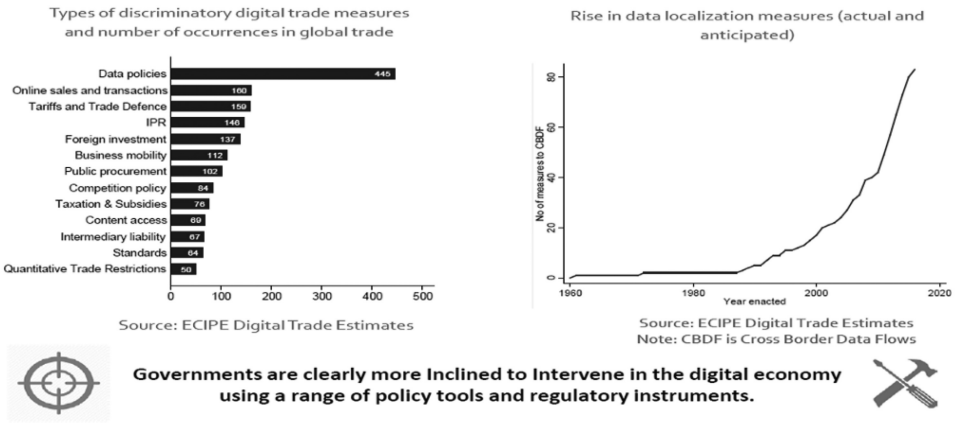
33 *Ibid*., at 2–3.

This echoes the discussion on standard-setting countries imposing their regulatory regimes for the digital economy on other countries. Naturally, countries where digital markets are established are keen on maintaining the advantages reaped from the digital economy through domestic regulations and/or trade strategies.[34]

Governments of some of these countries have mostly geared their legal interventions towards this objective. For example, several restrictive rules targeting data flows, foreign investment in domestic e-commerce, digital finance, and taxation, among others, have been introduced. These countries must realize that making new forays for coherent global rules should take just as much precedence as the focus on facilitating their own businesses to transform and adapt to the digital era and take advantage of digital connectivity.

It is also important for countries outside the controlling camp of rulemaking in the digital economy to avoid lagging even further behind as the rules in the digital economy evolve. As argued below, only a framework whose membership has critical mass can attract other powers interested in the first-mover advantages of setting the rules. This offers real political buy-in for states on either side of the digital divide to collaborate on the design of rules for a digital economy.[35]

Figure 1.2 Restrictive Regulatory Measures for the Digital Economy



Source: Huawei Europe, White Paper (October 2017) 'Trade and the digital economy'

34 *See* e.g. Henry Gao, *Digital or Trade? The Contrasting Approaches of China and US to Digital Trade*, 21(2) J. Int'l Econ. L. (2018).

35 E. O'Brien, *What Makes International Agreements Work: Defining Factors for Success*, Center on International Cooperation (2012).

3.3 WHY THE WTO IS NOT THE MOST SUITABLE ALTERNATIVE

Unfortunately, the soft law approach adopted by most multilateral initiatives does not offer enforceable rules or create legal certainty for the digital economy. The WTO, which has enforceable rules applying to a wide membership, is often cited as an appropriate framework to regulate the digital economy. The reform proposals at the WTO call for a recalibration of its existing rules and clarification of their application to the digital economy, which could steer the world towards common rules. However, progress at the WTO is questionable. The outcome of the Ministerial Conference of 2017 (MC11) illustrates that the current negotiation stalemate will not be resolved soon.

Proponents of using WTO rules to regulate the digital economy also argue that the rules, in their current shape, are sufficient to address trade issues related to the digital economy. While this might hold true for restrictions on data flows insofar as they affect trade in services, it is hard to imagine applying WTO rules to resolve issues relating to, for example, taxation of specific forms of digital income. The WTO is not apt to address the regulation of the digital economy in its entirety.

Recently, a group of WTO Members endorsed an initiative to begin negotiations for a plurilateral agreement on e-commerce at the WTO. This laudable initiative seeks to achieve a high standard outcome that builds on existing WTO rules with the participation of as many WTO Members as possible.[36] The scope and success of this initiative however, remains to be seen.

4 DESIGNING A MODERN LEGAL FRAMEWORK FOR THE DIGITAL ECONOMY

To be effective, any approach to designing a new legal framework for the digital economy needs to meet certain criteria. First, it would have to be holistic to create value for the entire digital ecosystem. Given the inherently cross-border nature of activities, a modern interoperable legal framework that functions seamlessly would be the most appropriate vehicle. Second, close public-private collaboration among governments, the business sector, and consumer associations would encourage the creation of a balanced, effective, and efficient environment for the digital economy.[37]

---

[36] WTO Joint Statement on Electronic Commerce, WT/L/1056 (25 Jan. 2019), http://trade.ec.europa.eu/doclib/docs/2019/january/tradoc_157643.pdf.

[37] International Chamber of Commerce, *Regulatory Modernization in the Digital Economy: Developing an Enabling Policy Environment for Innovation, Competition, and Growth*(2018), http://www.iccindiaonline.org/policy-statement-files/11.pdf.

4.1 Legal form: binding and enforceable

The digital economy needs legal certainty. The currently divided and conflictual legal environment cannot be improved by means of non-binding legal forms such as a memorandum of understanding or a declaration by like-minded countries. What is needed is a legally binding instrument that enables enforcement mechanisms (see section 4.2.2). Therefore, the language used in the rules created should match this binding nature. The language should not be tacit or hortatory.

4.2 Structural or operational form: an autonomous body administering public–private cooperation

In terms of institutional design, it is possible to envision a tripartite arrangement where governments and private companies interact under the administrative arm of an autonomous organization.[38] The arrangement would allow for state membership and provide governments with a forum to negotiate the appropriate universal rules and principles for regulating the digital economy.

Being the drivers of the digital economy, private companies would be eligible to participate as affiliate members. Their status would be similar to that of an observing nongovernmental body in many existing international agreements. Affiliate membership would be conditioned on meeting rigorous standards based on the rules for the digital economy agreed upon by Member States. Member States would drive the rule-making agenda within the organization but would have to consider input from affiliate members. For its part, the organization would assume an administrative role, exercising oversight and review powers over compliance by its Member States and affiliate members.

Such an arrangement would address many challenges facing the digital economy. Private sector involvement would foster the development of rules and policies that reflect business needs and are in line with technological developments. Private sector involvement would also lend some legitimacy to the legal framework within the digital sphere.[39]

---

[38] The Asia-Pacific Economic Cooperation (APEC) countries adopted a similar model under the Cross-Border Privacy Rules (CBPRs). The APEC CBPR system is a voluntary, self-regulatory initiative that facilitates privacy and protection of personal information flows among APEC economies. Companies trading in APEC member countries participate in the system and must develop and implement data privacy policies consistent with the APEC Privacy Framework.

[39] APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines (2011).

4.2[a] *Membership*

Participation in the proposed arrangement would give countries advantages tied to pioneering a legal framework for the digital economy such as, locking in key interests and having concerns considered from the outset. This would provide enough incentive to seek membership.[40] To drum up further support, carrot-stick incentives could be applied. The rights and benefits accruing to Member States under the relevant substantive provisions, discussed in section 4.3 below, could be limited exclusively to participating Member States to avoid free riders. Exclusivity, coupled with a proven record of success, could lure other states to join.

Member States could also agree on an internationally recognized trust mark, which affiliate members could use to indicate that they comply with the rules for the digital economy. One of the defining characteristic of trust marks is the involvement of a third party in the certification process who act as privacy, security and business reliability validators.[41] This would facilitate consumer trust, associate good business practice principles to the affiliate members, and ensure that these principles are applied widely. Member States could require companies seeking government contracts to have the trust mark certification in order to handle personal information and deliver digital products and services.[42] While the research findings on the actual effect of trust marks are notably scarce and inconsistent, it must be borne in mind that the potential advantages and disadvantages of a trust mark are conditional upon its design.[43]

4.2[b] *Enforcement*

Absent a proper enforcement mechanism, the proposed legal framework would merely be an addition to the list of toothless dogs in the realm of international law. The economic benefits and risks that attach to the digital economy require a functioning deterrent system that ensures companies and governments comply with the agreed rules. The enforcement model of the proposed legal framework could include the following mechanisms:

---

40 O'Brien, *supra* n. 35.

41 F. Alleweldt, S. Kara, N. Nahtigal, J. Trzaskowski, G. Fabisch, A. Fielder & P. Møgelvang-Hansen, *A Pan-European Trustmark for E-Commerce: Possibilities and Opportunities*. *Brussel: European Parliament* (2012). Directorate General for Internal Policies/Policy Department A: Economic and Scientific Policy, No. IP/A/IMCO/ST/2012–04.

42 Cf. UK government follows a similar model for its Cyber Essentials cyber security scheme, https://www.cyberessentials.ncsc.gov.uk/.

43 Alleweldt, Kara, Nahtigal, Trzaskowski, Fabisch, Fielder & Møgelvang-Hansen, *supra* n. 41.

4.2[b][i] Review and Policing

The implementation of the rules must be reviewed and policed. Subject to approval by Member States, these review and policing functions could be delegated to a board (the Board) that represents all Member States. The Board would ideally be composed of persons with considerable technical knowledge and experience in digital economy matters.

4.2[b][ii] Expeditious Dispute Resolution

The proposed legal framework would require a 'fit-for-purpose' dispute resolution mechanism. Such a mechanism would need to be expeditious to match the fast-paced nature of changes in the digital economy. Additionally, the mechanism would have to tackle violations by affiliate members and Member States. As such, the framework requires a system through which violation complaints are lodged, definitive binding determinations are obtained, and compliance with the determinations is enforced.

As concerns penalties for affiliate members who have committed violations, the withdrawal of trust mark certificates would help induce compliance. If further noncompliance after findings of violation occurs, affiliate membership could be revoked. For Member States, the WTO experience over the years has proven that governments respond to binding, enforceable international rules where their access to the rights and benefits of a global framework is tied to their observance and implementation of their obligations. This particularly holds true in disputes that were purely commercial in nature.[44] A reciprocal compliance model could be adopted for the digital economy: noncompliance with binding rules could be matched by countermeasures that allow other members to suspend their obligations towards the offending party.

4.2[c] *Voluntary Self-Regulation*

The proposed legal framework would require flexibility in enforcement to provide members with necessary protections. This flexibility can be achieved by encouraging self-regulation. Where members (affiliates or states) can regulate their conduct and maximize regulatory benefits such as consumer protection, all the while minimizing costs, the proposed legal framework could encourage such flexibilities.

---

[44] B. P. McGivern , *Seeking Compliance with WTO Rulings: Theory, Practice and Alternatives*, 36 Int'l L. 141, 156 (2002).

4.3 Addressing key substantive issues

Imagine that a new legal framework has been established for the digital economy, built around binding, enforceable rules, a supranational administrative organization, and a legitimizing public-private forum. What areas would the new rules focus on? This article develops on several key areas that pose significant challenges to the digital economy: data localization, taxation, privacy, security, establishment, intellectual property rights (IPR) and payment systems.

4.3[a] *Data Localization and Other Restrictions on Cross-Border Data Flows*

Governments have varied policy reactions to trade and use of data. Some of their concerns relate to privacy and security of personal data, national security interests, and economic standing of their digital economies at the global level. As mentioned above, these concerns have pushed some governments to impose measures that restrict the transfer and use of data outside their borders. These include data localization, bans on data transfer and conditional restrictions to the flow of data.[45]

Data localization refers to requirements to keep the collection, processing or storage of data within the jurisdiction where it was generated.[46] To comply, companies need to have local infrastructure in the jurisdictions imposing these requirements or contract out the infrastructure from local suppliers. These requirements have a rippling effect for any sector relying on data for the supply or delivery of goods and services. Local companies have to pay 30 to 60% more compared to cases where facilities outside their country's borders can be used for data.[47] Economy wide data localization laws are reported to drain between 0.7 and 1.1% of GDP from the economy. Any gains associated with data localization are too minute to outweigh the welfare losses made in the economy as a whole.[48] This defeats the 'global business models' that most suppliers apply to achieve efficiency and increases operational costs, rendering the global trade in goods and services more expensive for foreign suppliers, or worse still, nearly impossible.[49] There are

---

45 M. Ferracane, *Restrictions on Cross-Border Data Flows: A Taxonomy* (2017).

46 Building a European Data Economy, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* (2017), https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy.

47 B. O'Connor, *Quantifying the Cost of Forced Localization. Leviathan Security Group* (June 2015).

48 M. Bauer, H. Lee-Makiyama, E. Van der Marel & B. Verschelde, *The Costs of Data Localisation: Friendly Fire on Economic Recovery* (No. 3/2014). ECIPE Occasional Paper (2014).

49 Daniel Crosby, *Analysis of Data Localization Measures under WTO Services Trade Rules and Commitments. E15Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum* (2016).

at least thirty-four governments imposing either economy wide or sector-specific data localization measures.[50]

Governments often justify localization efforts by the need to protect the privacy and security of personal data. Information technology associations, however, argue that data security is a function not of where it is stored or processed, but of IT infrastructure security and the strength of the encryption techniques used.[51]

Knowing this, some countries have sought to use trade agreements to prohibit the use of data localization requirements as a condition for market access.[52] However, these provisions extend only to their bilateral partners. They do not solve the global phenomenon of data localization. The proposed legal framework for the digital economy could have binding provisions prohibiting data localization and other restrictions to the flow of data that would extend to a wider membership. These provisions could allow for limited exceptions for legitimate policy objectives. The legal provisions could also be subject to dispute settlement to ensure compliance and allow for jurisprudential interpretation of legitimate objectives.

Further, members could be encouraged to adopt other reasonable, less trade restrictive alternatives that safeguard their legitimate objectives while allowing data to flow across borders. These alternatives include data encryption tools; data protection and privacy regimes that balance trade objectives with data protection; information-sharing agreements for surveillance; and mutual legal assistance treaties that allow government access to data held on servers in different parts of the world.

4.3[b] *Taxation*

In a digital economy, businesses can generate income without having a physical presence in a country and can trade in intangible goods and electronically provided services. This fact challenges some fundamentals of taxation. The OECD has classified the tax challenges of the digital economy into four categories: (1) establishing the nexus between a jurisdiction and the tax liability arising, (2) treating transactions based on data, (3) characterizing income, and (4) collecting value-added tax.[53]

Faced with these challenges, some countries have taken up their own solutions for taxing the digital economy. India, for example, has taken the lead in taxing the digital economy through introducing an equalization levy on e-commerce transactions ('Google tax') without waiting for international consensus. Currently, it applies

---

50 N. Cory, *Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?, Information Technology and Innovation Foundation* (2017).

51 A. Chander & U. P. Le, *Breaking the Web: Data Localization vs. the Global Internet* 32–33 (2014).

52 *See* Art. 14.3 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Art. 15 of the Australia-Singapore FTA and Art. 9.10 of the Japan-Mongolia EPA.

53 OECD, *Addressing the Tax Challenges of the Digital Economy*, Action 1, Final Report, 99 (2015).

only to online advertisements, but plans are underway to increase the categories of digital products subject to the levy. This move is likely to spur others to take similar action.

In 2018, the European Commission proposed the implementation of a taxation system targeted at virtual businesses operating in the EU. The EU proposal takes a two-pronged approach. The first prong is a long-term solution in which corporate tax rules would be amended to have profits taxed where businesses have significant interaction with users on digital platforms. The second prong is a transitional solution in which an indirect tax would apply on the revenues from certain digital activities that are currently not taxed.[54] Although the proposals are currently stuck for lack of unanimous consensus among EU Member States, they have influenced similar discussions in France, New Zealand and the United Kingdom.[55] These discussions have also been brought up before the G20 and are likely to gain traction in leading economies.

The discussions on viability or need for such taxation systems fall outside the scope of this article. The article merely notes that the push to digital taxation will continue to gain traction in different parts of the world. This would add to the fragmented nature of digital economy rules if the solutions adopted are at the national level. A close inspection of the concerns raised reveals that the real issue is a dissatisfaction in the allocation of profit to countries where customers are located. Some countries provide the market for digital trade but do not collect taxes on transactions involving their tax subjects.

An alternative solution to the taxation challenge could be a global harmonized legal framework, created through public-private cooperation and administered by a supranational body. Under this framework, affiliate members could pay taxes for activities in the digital economy to a special body for redistribution to the relevant Member States. The taxation principles applied could be based on the standards agreed on in the OECD or newly negotiated rules that are cognizant of the need for a balanced approach.

This proposal would allow companies whose calls for the withdrawal of taxation initiatives have so far been disregarded to control the narrative and resulting outcome. Until proposals for digital taxes are effectively smothered, companies should also focus on alternatives that could minimize their exposure to risks. Instead of facing unilateral measures, or multiple tax and reporting obligations, companies would be subject to a unitary system.

---

54 European Commission, *Fair Taxation of the Digital Economy* (21 Mar. 2018), https://ec.europa.eu/taxation_customs/business/company-tax/fair-taxation-digital-economy_en.

55 Reuters, *Australia to Unveil Proposals for Multinational Digital Tax,* Financial Times, Digital giants face tax setback after G20 agreement (2019), https://www.ft.com/content/f00d2f70-8a6f-11e9-a1c1-51bf8f989972.

Taxation is complex. Asking governments to yield sovereign power and subject themselves to the will of a supranational body may seem unrealistic in the current political climate. In the alternative, Member States can adopt the application of OECD principles on taxation in the digital economy as a (mandatory) prerequisite for state membership to the proposed framework.

4.3[c] *Privacy*

Collection and analysis of personal data is a reality of modern life. Most jurisdictions recognize that privacy, even in the digital space, is a fundamental right, and have on this basis introduced rules on data privacy. Others consider privacy a consumer right and give consumers more freedom to individually manage their online privacy settings. Still other jurisdictions do not consider privacy an important concept requiring government intervention in the digital world. The lack of regulation is aimed at empowering local industries to take advantage of available personal data and enjoy large economies of scale.

Under most data protection rules, cross-border transfer of personal data is subject to certain conditions. These include proof that the recipient country has an adequate level of protection; that the data subject grants consent; or that a company uses binding corporate rules on privacy. This conditional regime is being adopted widely, as most countries anticipate that applying the same standards, as their trading partners will ensure they get adequacy decisions from them. This reflects efforts to balance protecting privacy while allowing cross-border data flows.

There are several international, regional, and national initiatives setting up data protection and privacy regimes. The most notable are the EU data protection regime under the GDPR[56] on personal data and the APEC Cross-Border Privacy Rules system (CBPR).[57] Both regimes enjoy wide membership. The proposed legal framework could borrow from existing regimes and take on a standard that does not interrupt or threaten the flow of data.

4.3[d] *Security*

With increasingly digitized economies and growing volumes of data in the global sphere, countries are vulnerable to cybersecurity risks and therefore need secure digital networks. Reportedly, there is a significant gap between data that requires security and data actually secured. The 2017 IDC white paper expects that by 2025,

---

[56] Regulation (EU) 2016/679 of the European Parliament and of the Council of the European Union of 27 Apr. 2016.

[57] APEC Privacy Framework (2005), https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.

almost 90% of all data created in the world will require some level of security, while only half will be secured.[58]

The risks attached to cyberattacks create a need for secure digital networks and technologies. The challenge attributed to cybersecurity is however paradoxical. On one hand, malicious cyber activities pose risks to businesses, governments, and public safety. Without cybersecurity, digital trade would be hampered because security and trust are a prerequisite. On the other hand, measures adopted to ensure cybersecurity may have a restrictive effect on trade.[59]

The proposed legal framework could require Member States to commit to strong regulatory cooperation on cybersecurity and focus on electronic signatures, encryption, and cooperation on cybersecurity. There is need for mutual recognition of authentication methods, acceptance of electronic signatures, and contractual freedom of parties to select authentication methods subject to performance standards and accreditation requirements.[60] The rules could also protect encryption products with exceptions allowing access for law enforcement purposes.

The framework could further contain rules addressing cybercrime, preferably taking a risk-based approach.

4.3[e] *Establishment*

The barriers to digital trade extend to placing certain requirements on companies in the digital sector with respect to establishment. These requirements include local presence through subsidiaries, branch offices/representation, or limiting foreign ownership as a condition for market access. These measures affect decisions on expanding in foreign markets, pursuing new customers, and monetizing products and services.

Several justifications have been put forward. First, governments highlight the need to ensure effective regulatory oversight and enforcement. Regulating foreign companies in the digital sector is problematic, especially for sensitive service sectors like health, finance and insurance. Proponents argue that without local presence, foreign businesses cannot be held accountable and can easily bypass domestic regulations and control. Second, having foreign companies serve a market offshore raises concerns for aggrieved customers who would have to litigate outside their own jurisdiction if any dispute occurs. Last, governments have introduced indigenous

---

58 IDC, *Data Age 2025: The Evolution of Data to Life-Critical,* white paper (2017), https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf.

59 Alberto Oddenino, *Digital Standardization, Cybersecurity Issues and International Trade Law* (2018), http://www.qil-qdi.org/digital-standardization-cybersecurity-issues-international-trade-law-forthcoming/#_ftn15.

60 Communication from Canada, Chile, Colombia, Côte d'Ivoire, the European Union, the Republic of Korea, Mexico, Paraguay and Singapore (JOB/GC/97/Rev.1) Work Programme on Electronic Commerce Trade Policy, the WTO and the Digital Economy.

innovation policies aimed at boosting local skills, technology transfers, and innovations tailored for the local economy.

Proposals for rules prohibiting local presence requirements subject to appropriate public policy exceptions have been made in the WTO Work Programme on E-Commerce by several countries: the EU, Canada, Chile, Colombia, Côte d'Ivoire, Korea, Mexico, Montenegro, Paraguay, Singapore, Turkey, Japan, and the USA. However, the 'appropriate public policy exceptions' have not been listed.

The proposed legal framework could include a prohibition on local presence requirements subject to limited exceptions. In any event, Member States can impose deposit requirements on foreign suppliers to cover any potential liabilities arising within the host country.

4.3[f] *Intellectual Property Rights*

Intellectual property (IP) is an essential enabler of digital trade. Modern trade is increasingly in bytes, ideas and services, thus pushing firms to invest heavily in knowledge-based capital. As a result, robust IP protection regimes are needed to ensure effective digital trade for products and services that are reliant on the protection of IP. However, with technological innovations, many IP infringements have become easier. These include pirating, circumvention of technological measures, trademark infringement by domain names, and cyber theft of trade secrets.

Infringements undermine business confidence and consumer trust in using the internet as a platform for international trade. Quantifying the level of infringement and economic cost in the digital space is difficult. The data available relies on estimates that may not reflect the actual global position.

The existing trade rules for IP (TRIPS) have difficulties addressing these infringements. First, these rules were established in a time when 'digital trade' was not a prominent feature of the economy, and they establish only minimum global IP protection standards. Second, although most countries have adopted laws implementing minimum standards on IP protection, infringements have risen to industrial proportions.[61] A recent OECD study on trade in counterfeited and pirated goods revealed that the volume of trade in counterfeited and pirated products could amount to as much as USD 509 billion (EUR 460 billion), representing close to 3.3% of world trade.[62]

---

[61] European Commission, *Strategy for the Enforcement of Intellectual Property Rights in Third Countries* (2005/C 129/03), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2005:129:0003:0016:EN:PDF.

[62] OECD/EUIPO, *Trends in Trade in Counterfeit and Pirated Goods*, Illicit Trade, OECD Publishing, Paris/European Union Intellectual Property Office (2019), https://doi.org/10.1787/g2g9f533-en.

The proposed legal framework could consider the existing global IP protection standards and build up specific provisions for issues directly relevant for the digital economy, such as intermediary liability and prohibitions on forced technology transfers as well as forced transfer of source code.

Intermediary liability refers to the liability that internet intermediaries such as internet service providers, search engines, social networks and online platforms incur for IP infringements conducted on their platforms. At the global level, this follows three models: (1) a strict liability model where intermediaries are liable for third-party infringements; (2) a safe-harbour model granting intermediaries immunity where some compliance is present on certain requirements; and (3) a broad-immunity model where intermediaries get broad or conditional immunity from liability for third-party infringements and exemption from content monitoring requirements.[63] Member States can adopt a hybrid liability model that considers the need for balance.

Forced technology transfers broadly refer to national policies aimed at forcibly increasing the transfer of foreign owned technology in a domestic market as a condition for investment at the expense of foreign innovations. These policies also raise significant trade concerns when laid as a precondition to establish or operate in a foreign market or when they grant less favourable treatment to foreign technology owners than domestic owners.[64] Recently, the EU launched a WTO challenge against China over forced transfer of technology. Although the WTO does not have specific rules on forced technology transfers, the EU invoked the specific commitments in China's Accession Protocol that prohibit such policies.[65] Since uniform WTO rules are lacking, the legislative framework could include prohibitions on forced transfers of technology.

Source codes are basic instructions written into a software program in human-readable text language which is then converted into machine code to enable computers understand and execute the software program. They are in a very basic sense, 'the source of a software program'. The current challenge that companies face is the loss of IP to foreign countries that impose forced transfer of source code requirements as a market access condition.

---

63 Centre for Internet and Society, India, *An Evidence Based Intermediary Liability Policy Framework* (2014), http://www.intgovforum.org/cms/wks2014/uploads/proposal_background_paper/Background_Paper_Towards_an_evidence_based_intermediary_liability_policy_framework.doc1.pdf.

64 OECD, Working Party of the Trade Committee, *International Technology Transfer Policies* (2019), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2018)8/FINAL&docLanguage=En.

65 Request for consultations by the European Union, *China - Certain Measures on the Transfer of Technology,* WT/DS549/1, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=250740,245753&CurrentCatalogueIdIndex=1&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True.

Recognizing that countries need to safeguard their national security interests, the legal framework could propose that instead of forced source code transfers, countries can impose export/import controls on encryption products. This would regulate trade of encryption products which might subvert security and the national order. Usually, export control rules on encryption technologies require companies trading in these items to seek approval but do not require disclosure of source code to regulators. Thus, the proposed legal framework could provide for the prohibition of forced technology and source code transfers or disclosures as a condition for market access.

4.3[g] *Payment Systems*

Online payment systems refer to the systems that support the use of payment cards (debit and credit), online and mobile payments, gift cards, and systems based on distributed ledger technologies such as blockchain to pay for goods and services offered. Transactions conducted through such means are faster and incur lower costs compared to paper-based alternatives, enabling companies to engage in trade efficiently.[66]

Online payment systems may be blocked either by issues affecting users (front-end) or payment service providers (back-end). The front-end issues often relate to the unavailability of the option to make/receive cross-border payments without undue restrictions. Notably, chapter 14 of the CPTTP on electronic commerce excludes financial institutions from the scope covered by that chapter. This by extension applies to electronic payment services.[67] Accordingly, to the extent that certain protections in chapter 14 of the CPTPP are only given to covered persons, electronic payment services could be excluded. The rules adopted in the proposed legal framework could ensure that financial institutions and electronic payment services are not carved out from the protections granted in the rules for the digital economy.

Back-end issues often trace back to a lack of interoperability in payment standards and issues relating to clearance and settlement of payments. Given the international sphere in which payment systems operate, the proposed legal framework could provide a necessary multilateral solution to the accessibility and interoperability issues facing payment standards.

---

66 H. David, W. Magnus, L. Ted & B. Göran, *What Does It Cost to Make a Payment?,* 2(2) Rev. Network Econ. 1 (2003).

67 Art. 14.1 of the CPTPP.

5 CONCLUSION

This article provides a sketch for a global legal framework for the digital economy. This sketch tailors to the global needs of operators in the digital economy, taking into account the legitimate concerns of both digitally advanced and less digitally advanced states. Structurally, the proposed legal framework could take up the form of a tripartite arrangement involving cooperation between governments and companies, administered by an autonomous body. The involvement of stakeholders in the design of the rules would lend legitimacy to the process and avoid new or ad hoc regulations with unintended effects that limit the digital economy's potential.

Beyond meeting legitimacy concerns, the suggested model would benefit companies and governments operating in the digital economy. Settling the issues around taxation of the digital economy, for example, would ensure predictability of tax rates and avoid double taxation, which is key for strategic actions and decisions. Moreover, a company's trust mark certification, demonstrating affiliation to a sustainable framework that provides harmonized global rules on privacy, data protection, and security, would be a valuable asset and provide for the trust needed for success in the digital economy.

The current rigid approach to the digital economy in the WTO, regional economic groupings, or at national level, will not yield desirable benefits. While the idea of a supranational body may seem ambitious, the focus here is not on reshaping the global order. Rather, the idea is to recalibrate existing regulatory trends and adapt them to fit a binding, enforceable, and global regime. By delineating a roadmap for such a legal framework, this article anticipates that governments and stakeholders will take up the challenge and start a discourse on global regulatory coherence in the digital economy.