5

Data as Capital and Algorithmic Input

Competition, Transparency, and Trade Rules

5.1 Introduction

The most important feature of platformization is scale. A platform can only provide value to users if it grows to a significant size.[1] When a digital platform reaches a certain scale, it gains access to more and more of its users' data. Of course, this feature is not even remotely novel, because larger factories have always been more efficient than smaller ones, even in the "old economy." However, datafication forces this economic logic to the extreme.[2] In this regard, companies in smaller countries are often disadvantaged vis-à-vis companies in larger countries, simply because of the constraints of smaller markets in terms of efficiencies of scale and volume of data.[3] The leading platforms – including Google, Facebook, Amazon, Baidu, and Alibaba – were launched in the US or China, where they could operate and reach the necessary scale in a large domestic market before they went global.[4]

More importantly, big tech companies have the ability to commoditize our data, which is the key ingredient of many digital services, including

The first two parts of this Chapter (5.1 and 5.2) were an abridged and revised version of Shin-yi Peng, "The Uneasy Interplay between Digital Inequality and International Economic Law" (2022) 33(1) European Journal of International Law 205–235.

[1] EMAG, "Digital Platform's Market Power" (September 30,2019) <https://ec.europa.eu/competition/information/digitisation_2018/contributions/emag.pdf>, at 2.

[2] European Commission, "Competition Policy for the Digital Era" ("EU Competition Policy") (May 20, 2019) <https://op.europa.eu/en/publication-detail/-/publication/21dc175c-7b76-11e9-9f05-01aa75ed71a1/language-en>.

[3] Communication from India and South Africa, "The E-Commerce Moratorium: Scope and Impact" ("E-Commerce Moratorium") WT/GC/W798 (March 10, 2020), para. 3.2.

[4] EMAG, supra note 1, at 3.

AI.[5] Many commentators have rightly pointed out that data is the single-largest lasting asset of these globally dominant companies.[6] Indeed, data is now becoming a form of capital.[7] The ability to collect, use, and apply data is a competitive parameter whose relevance is quickly increasing.[8] The data held by these leading platforms is particularly valuable due to the scale and scope of user data collected, which further provides these big players with strong competitive advantages, allowing them to dominate in the relevant market, create entrance barriers to potential competitors, attract more and more users, build richer and richer data sets, and reinforce their market power.[9] In short, control over data may effectively act as a market entry barrier.[10] Big platforms' control over our data strengthens their market position and makes it easier for them to enter new markets. In the case of Meta, as an example, access to data not only enables Facebook to tailor services, but also to use data to benefit other business lines, such as Messenger, WhatsApp, and Instagram.[11]

The reality of this battle is clear: Big platforms' business practices interlock a combination of forces to dominate the data market – presenting a new form of modern monopoly.[12] To some extent, the emerging phenomenon of leading platforms that appropriate and extract data for

[5] See generally Tom Taulli, *Artificial Intelligence Basics: A Non-Technical Introduction* (Apress 2019), at 36; Chris Skinner, *Digital Human: The Fourth Revolution of Humanity Includes Everyone* (UNKNO 2018), at 58–60.

[6] See, for example, Alex Moazed and Nicholas L. Johnson, *Modern Monopolies: What It Takes to Dominate the Twenty-first Century Economy* (St. Martin's Press 2016), at 99; "The Rise of Data Capital" (*MIT Technology Review Insights*, March 21, 2016) <www.technologyreview.com/2016/03/21/161487/the-rise-of-data-capital>.

[7] Richard Baldwin, *The Globotics Upheaval: Globalization, Robotics, and the Future of Work* (Oxford University Press 2019), at 216–217. As Baldwin quoted the comments of Eric Posner and Glen Weyl, "once we give our data to [the big tech] companies," they can "use it as much as they like." Such a practice is governed by the "data-as-capital" view. However, under the "data-as-labor" view, we maintain data ownership, and the big tech companies would have to pay us for the data we "create."

[8] EU Competition Policy, supra note 2; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs 2019), at 338.

[9] Australian Competition and Consumer Commission (ACCC), "Digital Platforms Inquiry – Final Report" (July 26, 2019) <www.accc.gov.au/publications/digital-platforms-inquiry-final-report>, at 57.

[10] See generally Lina M. Khan, "Amazon's Antitrust Paradox" (2017) 126 Yale Law Journal 710, at 785.

[11] EU Competition Policy, supra note 2, at 13, 115.

[12] Moazed and Johnson, supra note 6, at 99; Francesco Ducci, *Natural Monopolies in Digital Platform Markets* (Cambridge University Press 2020), at 24.

profit can be conceptualized as "data colonialism."[13] Overwhelming "economies of scope" empower these large incumbent platforms, giving them a strong competitive advantage.[14] Platformized transactions further enable the expansion of data capitalism, which works both domestically on a home country's populations, and also on a global scale. In this twenty-first century version of colonialism, big tech companies benefit from colonization all over the world. From this aspect, the North–South divide does not seem to matter as much as it usually does.[15] The US and East Asia account for 90 percent of the market for large-scale digital platforms, whereas Africa and Latin America's combined share comprises only 1 percent of the market.[16] These uneven, if not one-way, transnational data flows indicate that "data" – the input for AI and other technologies – has largely originated abroad for the benefit of big tech's data analysis.[17] Given the inordinate concentration of digital technologies in developed economies and a few Asian countries, most developing countries are becoming "net data exporters" that consistently supply valuable data without fairly benefiting from the digital economy.[18]

Against this backdrop,[19] this chapter explores two notable features of the platform economy: First, data has become capital. At the crux of the matter are questions regarding how to "decolonize" data, how public policy should evolve to promote competition in the digital market, and how data capitalism as a whole should be confronted.[20] More importantly, what role can international law assume in promoting competition

[13] See Nick Couldry and Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press 2019), at 83–85, 187–196; Sarah Myers West, "Data Capitalism: Redefining the Logics of Surveillance and Privacy" (2019) 58(1) Business & Society 20, at 24.

[14] Zuboff, supra note 8, at 128–137; Jonathan Haskel and Stian Westlake, *Capitalism without Capital: The Rise of the Intangible Economy* (Princeton University Press 2018), at 118–119.

[15] See María Soledad Segura and Silvio Waisbord, "Between Data Capitalism and Data Citizenship," (2019) 20(4) Television & New Media 412, at 412–419.

[16] E-Commerce Moratorium, supra note 3, para. 3.4.

[17] "Data" is an asset for value creation, and thus, control over massive volumes of personal data is the key to market power. Common concerns therefore emerge regarding the privacy risks posed by market concentration and the abuse of market dominance. See Section 6.3.1.

[18] E-Commerce Moratorium, supra note 3, para. 3.4.

[19] Also note that global digital platforms are among the "winners" of the pandemic in past years because their dominant role has been further reinforced as a result of the boom in e-commerce attributable to the lockdown. *Ibid.*

[20] EU Competition Policy, supra note 2, at 13.

in the digital market? Second, data has become input or feeds for platforms' algorithmic recommendations, which are at the heart of the datafied economy's business models. Problems arising from this phenomenon are potential unfair competition and the lack of algorithmic transparency and accountability. Big tech's datafication-enabled advertising, or, more generally, its overall business model, calls for deep thinking about how to appropriately regulate associated datafication practices. Recognizing that our behavioral data has increasingly become a commodity, the surveillance power of the digital platforms, left without proper constraints, will deepen the negative effect of datafication. What are the necessary steps toward holding digital platforms accountable due to their crucial roles in this datafied society? Are existing regulatory tools sufficient to provide domestic regulators with the information they need to ensure the adequate transparency of algorithmic systems in order to supervise how digital platforms moderate, rank, and recommend content to their users?[21] In particular, what is the interplay between international trade agreements and national algorithmic transparency requirements? These are the key issues this chapter seeks to address.

5.2 Trade and Competition Policy for a Platform Economy

5.2.1 When Winners Act Globally and Take All

Much like the persistently unequal distributions in the broadband networks, the upper layer of the Internet architecture – the platforms – is now facing threats posed by data capitalism. The digital economy is gradually being shaped by increases in market concentration on a global scale, the proliferation of anti-competitive practices by digital platforms, and the abuse of dominant market positions by platform monopolies.[22] Taken as a whole, "winner takes all" is a predictable phenomenon of the digital economy,[23] in which big tech companies do not "compete in the

[21] See Position by Algorithm Watch, "Input to the High Commissioner Report on the Practical Application of the United Nations Guiding Principles on Business and Human Rights to the Activities of Technology Companies" (February 2022) <www.ohchr.org/sites/default/files/2022–03/AlgorithmWatch.pdf>, at 7.

[22] EU Competition Policy, supra note 2, at 98–100.

[23] Cf., Herbert Hovenkamp, "Antitrust and Platform Monopoly" (2021) 130 Yale Law Journal 1952, 1970 (arguing that only a few platforms are natural monopolies, and that the market for digital platforms is rarely winner-take-all).

market," but, rather, "compete for the market" to displace each other.[24] In this context, competition policy must be tailor-made in order to ensure its effectiveness vis-à-vis dominant digital players, thereby safeguarding competition in the markets.[25]

In fact, big tech firms have increasingly been investigated for abuse of dominance and anti-competitive behavior all over the world, which offers plenty of food for thought about data capitalism. Many are in the midst of investigations by competition authorities, some are facing the scrutiny of the administrative courts, and several cases have been concluded.[26] For example, in its Apple Dating app case,[27] the Netherlands Authority for Consumers and Markets (ACM) found that Apple abused its dominant market position by imposing unreasonable terms and conditions on the services suppliers of the dating app in the App Store. In the view of the ACM, Apple enjoys a dominant position in the relevant market of the mobile operating system for dating app providers. "Having a dominant position is not illegal in and of itself. Abusing one, however, is," explained the ACM.[28] Due to the fact that Apple restricts dating app providers' freedom of choice, including banning them from referring within their own dating apps to alternative payment systems outside the app, the ACM came to the conclusion that Apple violated the Dutch Competition Act.[29] Similarly, in the Google Shopping case,[30] the European Commission concluded that Google, by favoring its own comparison shopping service, had abused its dominant position in the relevant market for online general search services. According to the commission's decision,[31] Google breached the EU

[24] OECD, "Big Data: Bringing Competition Policy to the Digital Era" DAF/COMP (2016) <https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf>, at 17 (explaining the features of the digital economy).

[25] *Ibid.*, at 14.

[26] See Henri Piffaut, "Algorithms: The Impact on Competition" (2022) 23(1) Business Law International 5, at 18.

[27] The Netherlands Authority for Consumers and Markets (ACM), "ACM Obliges Apple to Adjust Unreasonable Conditions for its App Store" (December 24, 2021) <www.acm.nl/en/publications/acm-obliges-apple-adjust-unreasonable-conditions-its-app-store>.

[28] *Ibid.*

[29] *Ibid.*

[30] European Commission Decision, "Google Search (AdSense)" CASE AT.4041 (March 20, 2019) <https://ec.europa.eu/competition/antitrust/cases/dec_docs/40411/40411_1619_11.pdf>.

[31] *Ibid.*, at 8.2. The Commission found that Google's own comparison shopping service was "prominently positioned at the top of Google's general results pages," and displayed in an eye-catching manner.

competition rules because it had "systematically given prominent placement to its own comparison shopping service."[32] Google appealed this decision, and the European General Court upheld the Commission's decision,[33] finding that Google's self-preferential practices constitute an abuse of dominance and have potential anticompetitive effects.[34]

Overall, these cases have led to emerging regulatory efforts with regard to digital platforms. In particular, these decisions underscore the difficulties in correcting *ex-post* negative effects on competition and the need to have *ex-ante* regulations in place to constrain big tech's behaviors and require platform transparency. The trend of rising inequality between those who provide the data and those who control the use of such data challenges our existing legal approaches to the problem of anticompetition. There is an urgent need to revisit the fundamental goals of competition law in the light of digital trade.[35]

5.2.2 *Emerging Competition Law for Data Markets*

5.2.2.1 Big Tech and Competition Policy

Today, competition authorities all over the world are considering the benefits associated with digital platform obligations.[36] One potential mechanism, among others, is to require leading digital platforms to share data with other services operated by their potential rivals, which may "enhance data access, resolve data bottlenecks, and contribute to a fuller realization of the innovative potential inherent in data."[37] In any event, all of the approaches require greater cross-border collaboration. Big tech companies act globally, and dominant platforms are global in scope. The impact of their market power can be more meaningfully addressed

[32] European Commission, Press Release, "Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service" (June 27, 2017) <https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784>.

[33] Judgment of the General Court, Google and Alphabet v Commission (Google Shopping), The Court of Justice of the European Union, Case T-612/17 (November 10, 2021) <https://curia.europa.eu/juris/liste.jsf?num=T-612/17>, para.168.

[34] *Ibid.*

[35] Couldry and Mejias, supra note 13, at 191.

[36] Ariel Ezrachi and Maurice Stucke, *Virtual Competition – The Promise and Perils of the Algorithm-Driven Economy* (Harvard University Press 2016), at 203, 205.

[37] ACCC, supra note 9.

through competition rules at the international level.[38] Compared with national regulations, competition disciplines at the international level would be more effective in defining the relevant (global) market, identifying the abusive market power (globally), addressing (cross-border) collusive practices and digital cartels, and reviewing mergers of (global) platforms. After all, the leading platforms operate on a global scale, and as such, efforts at the international level would be more commensurate with the scale of impact of digital platforms.[39]

In practice, the competition assessment will necessarily depend on the extent and type of data to be shared, the precise form of the data-sharing arrangement, the degree of transparency requirements, and the definition of the relevant market.[40] However, the gap in competition policies and enforcement among jurisdictions will likely leave any competition authority ill-equipped to effectively address the anticompetitive practices of the big tech companies, simply because data flows do not stop at borders.[41] In short, more and more countries are now focusing their regulatory attention on big tech. Recent regulatory progress toward defining "dominant platforms" and establishing ground rules to promote competition reflect a growing understanding that the platform economy requires tailored intervention. The dynamics of global data flows, however, make it legally challenging to enforce data competition policies without global regulatory harmonization. The lack of consistency among national competition laws demonstrates the need for a more consistent, streamlined system among competition regimes – either through greater international collaboration or the creation of additional cross-border disciplines for competition policy.

A number of new regulations and regulatory recommendations have been floated at both the national and the regional level. Among these, the Organization for Economic Co-operation and Development (OECD) policy papers point to the high concentration of data-driven markets, express caution regarding the absorption of new entrants through acquisitions by dominant incumbents, and call for competition rules that seek

[38] UNCTAD, "Digital Economy Report" (2019) <https://unctad.org/publication/digital-economy-report-2019>, at 19.

[39] *Ibid.*, at 147–148.

[40] Arne Hintz et al., *Digital Citizenship in a Datafied Society* (Polity 2019), at 63–68; Maurice Stucke and Allen Grunes, *Big Data and Competition Policy* (Oxford University Press 2016), at 168, 202.

[41] Stucke and Grunes, *ibid.*, at 338 (arguing that the competition policy gap leaves consumers and SMEs vulnerable).

to promote the efficient use and exchange of data.[42] The European Parliament, in addition to the adoption of the two landmark pieces of legislation on digital platforms – the DSA and the Digital Markets Act (DMA) – has also passed or proposed regulations including the Data Act, the Data Governance Act, and the Artificial Intelligence Act, which seek to provide an overall framework for data governance.[43] At the same time, examples in the Asia Pacific region include Australia's News Media and Digital Platforms Mandatory Bargaining Code, which was developed by the Australian Competition and Consumer Commission (ACCC) to address "bargaining power imbalances between the digital platforms and Australian news media."[44] Moreover, the ACCC has already conducted public consultations on policies that would provide for greater regulatory oversight of digital platforms with strong market positions, such as Google and Facebook.[45]

5.2.2.2 EU as Global Norm-Setter?

While various regulatory initiatives are still subject to policy debates, and certainly there are divergent views on how competition law should be restored to account for specific concerns brought about by datafication and data capitalism, the legal approaches share common elements:

- Relevant Markets and Market Power: All of the proposals address the need to clarify what constitutes the "relevant market" of a digital platform. To summarize, identifying relevant markets inside the ecosystem of "data" can prove particularly challenging, because big tech companies always assume multiple roles.[46] Competition authorities must identify a multi-side market and consider relevant data flows in the market.[47]
- Dominant Position and Anti-Competitive Practices: A closely related issue is market power assessment in the context of data access and data

[42] OECD, supra note 24, para. 87.
[43] At the time of this writing, an agreement between the European Council and the European Parliament on the Artificial Intelligence Act seemed possible by mid-2023.
[44] ACCC, News Media Bargaining Code (2021) <www.legislation.gov.au/Details/C2021A00021>.
[45] ACCC, "Digital Platforms Inquiry" (December 10, 2018) <www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry/preliminary-report>.
[46] UNCTAD, supra note 38, at 19, 39.
[47] OECD, supra note 24, paras. 30, 34, 45. See Section 5.2.3.3 for further discussion on this point.

control, which requires, among other things, specific criteria to assess the impact of a dominant market position. It is a generally shared view among competition authorities that when data is overly concentrated in the hands of big tech companies, it may provide these firms with a substantial competitive advantage against new entrants.[48] The misuse of data to maintain market power should be considered an anticompetitive practice that requires governmental intervention.[49] Most policy papers attempt to identify the types of anticompetitive conduct that are enabled through the control of data, including collusive practices and digital cartels.[50] As emphasized in several policy papers, the incentive for digital platforms to use data to collude with each other is enormous.[51] As a result, the need for competition authorities to adapt tools to address digital cartels is overwhelmingly strong.

- Mergers and Acquisitions: Another closely linked dimension is "data-driven mergers and acquisitions."[52] As evidenced by the Facebook/WhatsApp merger,[53] it is not uncommon for digital platforms to acquire other digital companies and start-ups, which increases the risk of monopolization of data.[54] Policymakers increasingly understand the need to examine the impact of mergers on data, the overall competitive implications of mergers and acquisitions involving digital platforms, and the new threshold for merger control in competition law.[55]

Against this backdrop, the EU's DMA sets a high global benchmark for regulating digital platforms.[56] Overall, the DMA addresses digital market "imbalances" in the EU, imposes tailored asymmetric *ex-*

[48] *Ibid.*, paras. 20, 64 (pointing out how market power may increase market entry costs).
[49] *Ibid.*, para. 64.
[50] *Ibid.*, para. 75; Stucke and Grunes, supra note 40, at 234.
[51] OECD, "Algorithms and Collusion: Competition Policy in the Digital Age" (2017). <www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf>, at 20–21, 29; Cf., Nicolas Petit, *Big Tech & the Digital Economy: The Moligopoly Scenario* (Oxford University Press 2020), at 252–256 (arguing that consumer protection regulation is the appropriate tool to address the harms inherent to big tech companies).
[52] UNCTAD, supra note 38, at 14.
[53] Stucke and Grunes, supra note 40, at 74.
[54] UNCTAD, *ibid.*, at 139; EU Competition Policy, supra note 2, at 110.
[55] EU Competition Policy, *ibid.*, at 113.
[56] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

ante rules on "gatekeeper platforms,"[57] provides a legal mechanism based on market investigations, and establishes harmonized rules prohibiting certain unfair practices among gatekeeper platforms.[58] In particular, the DMA establishes a set of defined criteria for qualifying a large digital platform as a "gatekeeper,"[59] with the underlying principle that digital platforms with a certain degree of market power should be subject to more stringent obligations than smaller players.[60] In September 2023, the EC has designated six gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft.[61] Within six months of being designated gatekeepers, digital platforms are obliged to comply with a number of "special obligations." More specifically, the DMA imposes obligations and prohibitions to limit gatekeepers' abilities to process and use personal data,[62] to negotiate certain conditions with business users,[63] and to restrict end users from switching between digital applications.[64] Note that the European Commission, based on market investigations, has the discretion to "update" obligations for gatekeepers to ensure the obligations are "up to date."[65]

Such an ambitious agenda reveals the EU's aim to be a global norm-setter in digital markets.[66] Expectedly, the DMA will assert significant regulatory control over digital platforms, both within Europe and beyond. The rules will bind global platforms, rendering them *de facto* global standards – more commonly known as the "Brussels Effect." As for big tech, the stakes are particularly high, because the EU is one of the world's largest consumer markets. They must accept the

[57] *Ibid*. The DMA will apply only to providers of "core platform services."
[58] *Ibid*. Gatekeeper platforms carry additional responsibilities, including the requirement to comply with a defined set of obligations to avoid certain unfair practices, to ensure interoperability with its platform, and to share data that is provided or generated by business users and their customers in their use of the platform.
[59] DMA, Article 3 (Designation of Gatekeepers). Infra note 105.
[60] Put simply, a platform that has a significant impact on the EU market, provides a core platform service, has a strong economic position, and is active in multiple EU countries shall be designated as a gatekeeper.
[61] European Commission, "Digital Markets Act: Commission Designates Six Gatekeepers" (September 6, 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328>. Infra note 106.
[62] DMA, Article 5(2).
[63] DMA, Article 5(3)(4).
[64] DMA, Article 5(6).
[65] DMA, Article 12 (Updating obligations for gatekeepers).
[66] The DMA was signed into law on September 14, 2022 and became applicable, for the most part, in May 2023.

EU's "terms of business" as the price of admission. To conclude, driven by economic and strategic rationales, the EU has been leveraging its economic muscle and vying for a leadership role in shaping the global rulebook governing digital platforms. The EU's intensified efforts to set international standards for the digital economy could be part of the solution tool kit to curb data capitalism.

5.2.3 *Calling for a WTO "Data Reference Paper?"*

5.2.3.1 Trade and Competition

At the multilateral level, competition was one of the so-called new issues under the WTO framework two decades ago, at which time members attempted to address how domestic and international competition policies interact with international trade.[67] To a certain extent, international economic law and competition policy are grounded in complementary principles.[68] While the former emphasizes free trade and prohibits discrimination between trading partners, the latter aims to preserve the freedom of business activities and control the anticompetitive conduct of private enterprises.[69] Much discussion has been carried out in relevant legal literature regarding the importance of competition policy to trade liberalization, which generally describes how international cartels affect international trade, how transnational abuses of a dominant position constitute trade barriers to goods or services,[70] and how anticompetitive vertical market concentrations exclude foreign suppliers from a market.[71] Indeed, the rationales underlying both trade and competition are arguably closely related. Nonetheless, to date no significant consensus on the convergence of the two areas has emerged.[72]

To illustrate, historically, the interaction between trade and competition policy has been an important element of both multilateral and

[67] WTO, Interaction between Trade and Competition Policy, <www.wto.org/english/tratop_e/comp_e/comp_e.htm> (visited May 25, 2020).
[68] Ernst-Ulrich Petersmann, "Competition-oriented Reforms of the WTO World Trade System-Proposals and Policy Options" in Roger Zach et al. (eds.), *Towards WTO Competition Rules* (Kluwer Law International 1999), at 65.
[69] International Trade Center, *Combating Anti-Competitive Practices: A Guide for Developing Economy Exporters* 10 (2012) < https://intracen.org/media/file/12106>, at 10.
[70] *Ibid.*
[71] *Ibid.*
[72] Philip Marsden, *A Competition Policy for the WTO* (Cameron May 2003), at 201–235.

regional trade negotiations.[73] The issue of competition policy, however, was dropped from the Doha Round of the WTO trade negotiations.[74] In brief, negotiating efforts to create a general agreement on competition policy under the WTO have been unsuccessful, and the Working Group on the Interaction between Trade and Competition Policy has been inactive since 2004.[75] At the same time, competition policy has been addressed in FTAs,[76] with an evident trend toward a dedicated chapter in recent years,[77] which to a certain degree implies a growing perceived need for common competition disciplines among countries.[78] Given such a trend,[79] the interface between international trade and competition policy is now primarily manifested by the incorporation of "basic competition principles" in the FTAs.[80] Most specifically use the terms "anti-competitive agreements" and "abuses of market power,"[81] while few mention "anti-competitive mergers," "merger control," and "merger review."[82] It should also be noted that approximately half of the FTAs contain competition provisions pertaining to cooperation and technical assistance.[83]

Notwithstanding those "WTO-plus" obligations at the regional level, key problems remain. "General competition policies," which prohibit or require broad categories of business behaviors defined in rather general

[73] Robert D. Anderson et al., "Competition Policy, Trade and the Global Economy" World Trade Organization Working Paper (2018).

[74] *Ibid.* The Working Group on Trade and Competition under the WTO has been inactive since then.

[75] *Ibid.*

[76] *Ibid.*, at 74.

[77] See, for example, CPTPP, Chapter 16 (Competition Policy); USMCA, Chapter 21.

[78] The USMCA's competition chapter, for example, adds provisions on limiting antitrust exemptions, nondiscrimination in enforcement, and comity. The chapter also includes a new article addressing procedural fairness disciplines.

[79] For more discussions on general competition principles under the FTAs, see OECD, "Regional Competition Agreements: Benefits and Challenges" (November 29, 2018) <www.ftc.gov/system/files/attachments/us-submissions-oecd-2010-present-other-international-competition-fora/regional_competition_agreements_united_states.pdf>. It has been observed that the competition policy chapters of the FTAs appear to be drafted with vagueness and ambiguity. Parties to the FTAs only agreed to minimum standards for the key elements.

[80] *Ibid.*

[81] OECD, "Competition Provisions in Trade Agreements – Contribution from Mexico" (December 1, 2019) <www.oecd.org/daf/competition/competition-provisions-in-trade-agreements.htm>.

[82] *Ibid.*

[83] *Ibid.*

terms, are not sufficient to address digital cartels and data monopolization. The digital sector needs specifically tailored regulatory disciplines. How can international economic law help to ensure that additional procompetitive regulations are put into place? The real question is this: How can we restore the relevance of international economic law in the digital economy? Could such a restoration be launched with the modernization of the WTO Telecommunications Reference Paper for the data-driven economy?

5.2.3.2 Telecom Reference Paper as a Model

While WTO members have to date failed to agree on competition rules, in the context of the post-Uruguay Round WTO negotiations on Basic Telecommunications Services, most WTO members have committed to the regulatory principles spelled out in the Telecom Reference Paper under the GATS,[84] which sets out specific obligations for competition.[85] In the absence of general competition rules under the WTO regime, the Telecom Reference Paper serves as a sector-specific competition agreement, through which anticompetitive practices can be challenged using the WTO dispute settlement system.[86]

The Telecom Reference Paper requires members to adopt and maintain competitive safeguarding rules to prevent abusive restrictions on bottleneck facilities, which may result in a *de facto* limitation on market access to basic telecommunications services.[87] It also prohibits discriminatory competition conditions within the markets and prevents anticompetitive practices among dominant suppliers.[88] Key provisions include the following:

- Relevant Market and Dominant Supplier: The Telecom Reference Paper defines "major supplier" as a supplier that has the ability to

[84] Telecom Reference Paper. See Section 1.4.2.

[85] David Luff, "Telecommunications and Audiovisual Services: Considerations for a Convergence Policy at the World Trade Organization Level" (2004) 38(6) Journal of World Trade 1059; Lee Tuthill, "The GATS and New Rules for Regulators" (1997) 21 Telecommunications Policy 783.

[86] Mitsuo Matsushita et al., "Competition Policy and Trade" in Mitsuo Matsushita et al. (eds.) *The World Trade Organization: Law, Practice, and Policy* (Oxford University Press 2015), at 739; Mitsuo Matsushita, "Trade and Competition Policy" in Daniel Bethlehem et al. (eds.), *The Oxford Handbook of International Trade Law* (Oxford University Press 2009), at 658.

[87] Telecom Reference Paper, Section 1.

[88] *Ibid.*

materially affect the terms of participation surrounding price and supply in the relevant market for basic telecommunications services as a result of: (a) control over essential facilities; or (b) use of its position in the market.[89]

- Anticompetitive Practices: The Telecom Reference Paper imposes obligations on WTO members to maintain measures for the purpose of preventing suppliers – which alone or together are major suppliers – from engaging in or continuing anticompetitive practices.[90]
- Interconnection Arrangement and Transparency: There is a clear stipulation that interconnection with a major supplier should be provided under nondiscriminatory terms, conditions, and rates, and should be of a quality no less favorable than that provided for its own like services or its subsidiaries.[91]

In brief, the Telecom Reference Paper requires WTO members to ensure that dominant companies do not abuse their market position. As discussed in Chapter 1 of this book, the case of *Mexico – Telecom* represents a concrete application of competition policy within the framework of the Telecom Reference Paper.[92] In this case, the US claimed that the interconnection rates negotiated by Telmex, the incumbent supplier in Mexico, were not cost-oriented. The panel found that Mexico had failed to fulfill its commitments under Section 2.2(b) of the Telecom Reference Paper, in that it did not ensure a major local supplier to provide interconnection at cost-oriented rates to other members' suppliers for the cross-border supply of telecommunications services.[93] The panel also found that Mexico had not met its GATS commitments under Section 1 of the Telecom Reference Paper to maintain "appropriate measures" to prevent anticompetitive practices.[94]

By pointing to the model in the Telecom Reference Paper, this book raises the following questions: To what extent is a set of sector-specific competition disciplines for the data industry possible? Further, what should comprise the "Data Reference Paper?" Turning back to the

[89] *Ibid.*
[90] *Ibid.*
[91] Telecom Reference Paper, Section 2. There is also a requirement that interconnection should be provided in a timely fashion, with terms, conditions, and cost-oriented rates that are transparent and reasonable. A major supplier should make publicly available either its interconnection agreements or an interconnection offer.
[92] Matsushita et al., supra note 86, at 793.
[93] Penal Report, *Mexico – Telecom*, para. 7.216.
[94] *Ibid.*, para. 7.264.

common elements of the regulatory recommendations by the OECD, the EU, and the Australian competition authority, the proposed Data Reference Paper should be a binding set of commitments, perhaps the lowest common denominator, which would serve to guide WTO members to better regulate data, to discipline dominant players, and to thereby help smaller tech companies enter these markets. Much like the regulatory disciplines for the telecommunications market, the concept of "essential facilities" might be applied to big tech companies to prevent the abuse of market dominance by platforms. Similarly, based on the model of the Telecom Reference Paper, a Data Reference Paper would impose obligations on WTO members to maintain measures for the purpose of preventing dominant services suppliers from engaging in or continuing anticompetitive practices. Appropriate mechanisms to prevent collusive practices and review mergers should also be put into place. In addition, a similar focus on pro-competitive effects could include the principles of nondiscrimination and transparency, which would prohibit big platforms from engaging in self-preferential practices that favor their own services.[95]

By imposing cross-border disciplines for competition policy and thus curbing the power of big digital platforms, the proposed Data Reference Paper may well be an effective instrument to address data colonization, which, as discussed in Chapter 3, is an unforeseen phenomenon that interacts with GATS digital trade market access. Moreover, if a set of international competition rules that frame competition concerns in a policy context can be established, there would be less need for *ex-post* enforcement of competition law by competition authorities in developing countries and LDCs, which have relatively limited resources to tackle issues pertaining to digital cartels and data monopolization.[96] To conclude, the increasing inequality in datafication, and in particular the dissymmetric power between those who are the sources of the data and those who accumulate the data, calls for a set of WTO data-specific competition rules to appropriately address market power in the data sector. There is a renewed need for a WTO Reference Paper 2.0, which migrates the competition disciplines from the context of the telecommunications industry to that of the data industry.

[95] See the Google Shopping case, supra note 30.
[96] OECD, supra note 24, at 22.

5.2.3.3 The Inherent Complexity: Sufficient Momentum Needed

Will the need for international competition disciplines for the data sector find an outlet along the path of international economic law, as it did in the telecommunications sector two decades ago? Serious challenges lie ahead. The idea of creating a WTO "Data Reference Paper" may prove difficult in gaining sufficient negotiating momentum to bring it to fruition, primarily because of two structural problems. The first main obstacle is the highly complex, legally technical nature of regulating the digital market. To the extent that the regulatory principles spelled out in the Telecom Reference Paper can inform the development of the data regulatory framework, some adaptations are needed due to the specific characteristics of the data market. As pointed out by the Ofcom, the UK's communications regulator, the regulatory principles of telecommunications services cannot simply be "read-across" and "applied as they exist" to digital services.[97] There are significant similarities between the telecommunications and digital markets. Nevertheless, substantial differences remain.

More specifically, in terms of assessing the "relevant market," far more factors must be taken into consideration when defining the relevant market for digital platforms. All of the "big tech" firms are characterized as multi-sided, which renders the scope of the relevant market even more difficult to define. What constitutes the relevant market of a digital platform inside the big data ecosystem, when various players are involved and have assumed multiple roles? For example, Apple – as a digital platform through the Apple Store and iTunes – also plays an important role in cloud computing services using the iCloud. At the same time, Apple closely interacts with other key social media businesses, including Facebook and LinkedIn. Should each side of the above be defined as a separate market?[98] The multi-sided platform structure poses new difficulties for competition regulations.

Moreover, in terms of assessing abuses of market power, determining "market power" is less straightforward in digital markets. In the case of telecommunications services, dominant market position and significant

[97] See Ofcom, "European Commission Consultation on the Digital Strategy: A Framework of Analysis for an Online Regulatory Regime: Reflections from Ofcom" (September 17, 2020) <www.ofcom.org.uk/__data/assets/pdf_file/0011/203024/european-commission-digital-strategy-170920.pdf>, at 11.

[98] UNCTAD, Digital Economy Report, supra note 38, at 19.

power are closely related to natural monopolies in physical infrastructure, that is, network facilities. Digital services, however, are not necessarily natural monopolies, because their market powers are primarily derived from their access to large datasets created from their users.[99] In practice, market shares in telecommunications markets (*i.e.*, the 25 percent threshold) typically provide useful indications of market importance.[100] In most jurisdictions, a telecom operator is presumed to have significant market power when it holds more than a 25 percent share of a market in a particular geographical area.[101] On the other hand, the possession of data can be used as a barrier to entry, thus becoming the primary source of market power in digital services. The relationship between "market share" and "control over data," however, would prove difficult for competition authorities to investigate.[102] In this regard, the "qualitative criteria" set out by the DMA have been criticized as "arbitrary thresholds"[103] that lack "methodological considerations."[104] It is particularly problematic that the designation of gatekeepers is based on the presumption that the "qualitative criteria"[105] will be met by a firm if it meets the "quantitative criteria."[106] In summary, traditional measuring

[99] Ducci, supra note 12, at 36–43.

[100] Charles H. Kennedy, *An Introduction to U.S. Telecommunications Law* (Artech House 2001), at 231. It should be clarified that market share is not the sole determinative factor in finding significant market power in the telecommunications market.

[101] *Ibid.*

[102] OECD, supra note 24, at 20.

[103] Philip Hanspach and Magdalena Viktoria Kuyterink, "You Can (Try to) Keep the Economists Out of the DMA but You Cannot Keep Out the Economics" (*CPI Competition Policy International,* December 22, 2022).

[104] Christophe Carugati, "The Difficulty of Designating Gatekeepers under the EU Digital Markets Act" (*Bruegel Blog*, February 20, 2023).

[105] DMA Article 3 (Designation of gatekeepers): "1. An undertaking shall be designated as a gatekeeper if: (a) it has a significant impact on the internal market; (b) it provides a core platform service which is an important gateway for business users to reach end users; and (c) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future."

[106] DMA Article 3 (Designation of gatekeepers): "2. An undertaking shall be presumed to satisfy the respective requirements in paragraph 1: (a) as regards paragraph 1, point (a), where it achieves an annual Union turnover equal to or above EUR 7.5 billion in each of the last three financial years, or where its average market capitalization or its equivalent fair market value amounted to at least EUR 75 billion in the last financial year, and it provides the same core platform service in at least three Member States; (b) as regards paragraph 1, point (b), where it provides a core platform service that in the last financial year has at least 45 million monthly active end users established or located in the Union and at least 10,000 yearly active business users established in the Union, identified and calculated in accordance with the methodology and indicators set out in the Annex; (c)

tools, such as market shares, must be adapted in a digital platform context. All of this highly technical complexity will lead to endless technical discussions and will become an obstacle toward the goal of creating a set of international competition principles for digital services.

Another equally or even more important consideration that may impede the creation of such international disciplines is the inherent complexity of the political economy surrounding digital capitalism. Looking back at its history, the telecommunications industry began to rapidly develop in the late 1990s. As a result, the political momentum toward telecommunications liberalization rendered market access and regulatory discipline under WTO negotiations possible. In other words, adoption of the Telecom Reference Paper was seen by "key" delegations – notably, the US, the EU, Canada, Australia, and Japan – as necessary,[107] given the risk that competition in foreign countries' infrastructure markets may be restricted by incumbent operators' abuses of market power. To illustrate, the telecommunications market, especially decades ago, has exhibited specific features that enable incumbents to maintain a certain degree of market power over the competition.[108] Major incumbent suppliers have strong incentives and ample opportunities to delay the provision of interconnection to new entrants, and such delays can significantly inhibit competition.[109] The incumbents could also, for example, impose anticompetitive interconnection conditions on their competitors.[110] National measures might be needed to prevent incumbent operators from using their market power to distort competition. From the perspective of international trade, market access commitments alone cannot guarantee that a market will become truly liberalized. To be able to effectively compete, telecommunications companies of developed countries must be ensured a level playing field in foreign markets.

as regards paragraph 1, point (c), where the thresholds in point (b) of this paragraph were met in each of the last three financial years."

[107] Damien Geradin and Michel Kerf, "Levelling the Playing Field: Is the WTO Adequately Equipped to Prevent Anti-Competitive Practices in Telecommunication?" in Damien Geradin and David Luff (eds), *The WTO and Global Convergence in Telecommunications and Audio-Visual Services* (Cambridge University Press 2004), at 135.

[108] *Ibid.*

[109] *Ibid.*

[110] Shin-yi Peng, "Trade in Telecommunications Services: Doha and Beyond" (2007) 41(2) Journal of World Trade 293, at 318.

However, such political economy momentum, which led to the conclusion of the Telecom Reference Paper, cannot be found in the context of digital services. Unlike the negotiation background of the telecommunications services industry, the economic interests (as well as the regulatory approaches) of the data services industry are quite divergent among key players. Generally speaking, US digital platforms have been persistently dominant in the world, including the European market. At the same time, China – by establishing its own self-sufficient platform economy through Chinese digital giants Baidu, Alibaba, and Tencent[111] – has largely escaped US domination. Nonetheless, three different models for data governance are emerging: The US generally favors an *ex-post* approach, which broadly seeks punitive action for past infractions. Such an innovation-friendly approach is primarily driven by the concept of self-regulation.[112] The EU model, as discussed above, is holding the normative high ground. The *ex-ante* regulations would result in sweeping supervisory actions that impact Silicon Valley's future. China's main concern, however, is to ensure its political stability and security. It is conceivable that China will continue to rely on domestic protectionist regulations to restrict cross-border data flows.[113] When these three models interface in an international organization, it is less likely to result in a compromise given the associated concerns.[114]

5.2.3.4 Digital Trade and Competition Disciplines

How can international economic law contribute to overcoming these impediments? The first direction is the soft law mechanism, which leaves sufficient space for national regulators. Here again, the FTAs provide some inspiration. Although to date none of the Digital Trade/E-Commerce Chapters of the FTAs have incorporated competition rules for the data market, the lesson we have learned from their general

[111] Henry Gao, "Digital or Trade? The Contrasting Approaches of China and U.S. to Digital Trade" (2018) 21(2) Journal of International Economic Law 297, at 308.

[112] *Ibid*., at 316. See generally Julien E. Cohen, *Between Truth and Power: The Legal Constructions of the Informational Capitalism* (Oxford University Press 2019), at 214–217 (pointing out that the positions of the BRICS – Brazil, Russia, India, China, and South Africa – group are also significant in making the conflicts more complex).

[113] Gao, supra note 111, at 319.

[114] Mira Burri, "Towards a New Treaty on Digital Trade," (2021) 55(1) Journal of World Trade 77, at 99.

approaches pertains to the soft legal nature of key provisions.[115] The USMCA parties, for example, merely "recognize the importance" and "endeavor to" comply with certain rules under the Digital Trade Chapter.[116] It might therefore be criticized as a weak instrument. Nevertheless, it can always be argued that without such vague provisions, the Digital Trade Chapter would never have been finalized by the parties. In future trade negotiations on data governance, the "softness" of a treaty requires that substantive rules remain somewhat general. For example, it might be necessary to leave key concepts such as "anticompetitive practices" undefined to allow for policy alternatives. The lack of specificity in the treaty language would allow parties to cater to differences in local needs and maximize the likelihood that the rules will be effectively implemented by regulators. Given the variations that exist in the digital markets of different countries, the strategic use of hard and soft law is of practical significance in introducing a set of data rules into the WTO regime.

The second approach concerns flexible negotiating modality, which helps to reach a critical mass of trade negotiation results. Against this contentious political and economic backdrop, the probability of reaching a consensus under the "single-undertaking" system seems slight.[117] Balancing the interests of 164 WTO members across diverse issues surrounding data governance has made it difficult, if not impossible, to conclude negotiations that "bind all WTO Members equally." In this regard, negotiating on the basis of a critical mass approach, which involves arrangements between a number of parties that do not represent the entire membership but account for a very high proportion of international trade in data services, seems to be a more realistic direction. In this context, despite strong opposition from several members,[118] the

[115] See, for example, USMCA, Article 19.15 (Cybersecurity); Article 19.18 (Open Government Data).

[116] See, for example, USMCA, Article 19.5 (Domestic Electronic Transactions Framework); Article 19.8 (Personal Information Protection); Article 19.9 (Paperless Trading); Article 19.14 (Cooperation).

[117] Alberta Fabbricotti, "Multilateralizing Regionalism and the Future Architecture of International Trade Law as a System of Law: The Paradox of Multilateralizing Regionalism through Flexibility" (2009) 103 Proceedings of the American Society of International Law 119, at 120. The "single undertaking" concept essentially means that all of the instruments which make up the complex body of WTO law are equally binding upon all members, regardless of their stage of economic and social development.

[118] Inside US Trade, India, "South Africa: Plurilaterals Legally Inconsistent with WTO Rules" (February 22, 2021). India and South Africa have maintained that ongoing

ongoing JSI on E-commerce offers a pathway for the WTO to remain responsive and relevant in the digital economy.[119]

5.3 Trade Rules and Algorithmic Transparency

5.3.1 *Algorithms and Platform Competition*

A closely related but distinct aspect is algorithmic transparency, which can serve as a regulatory starting point for global platform governance. In this data-driven world, one important legal tool to promote platform competition is to ensure that algorithms are fair and transparent.[120] As illustrated above, platform capitalism would not ever have existed without big data analytics algorithms. In summary, the market dominance of big tech can be simplified in the following pattern. By taking advantage of their vast user base, big tech companies provide datafication-enabled advertising services to businesses, which in turn bring big tech advertising revenues. Big tech companies then invest more in their data analytics tools to enhance the accuracy of target advertising, which allows big tech to attract more users and collect more data. The more data that is collected, the more the algorithms can learn.[121] Under this pattern, with more and more data amassed, big tech companies are able to attract even more advertisers. The cycle continues.

To put it another way, each time we Google a product and then click on the sponsored ads, Yahoo not only loses a search query to Google, but also loses our behavioral data, which represents an opportunity for its algorithms to learn, as well as potential advertising revenues. This results in a gap between Google and Yahoo in their ability to train their AI, to personalize search results, and to enhance the accuracy of targeted advertising. The more people Google, the wider such gaps grow.[122]

negotiations on the plurilateral e-commerce agreements are "legally inconsistent" with WTO rules and principles. Cf., Inside U.S. Trade, "U.S., EU, Others Defend Plurilaterals after Criticism from India" (March 3, 2021).

[119] Cf., Jane Kelsey, "The Illegitimacy of Joint Statement Initiatives and Their Systemic Implications for the WTO" (2022) 25 Journal of International Economic Law 2.

[120] For the purpose of coherence, this chapter focuses on issues pertaining to the algorithmic transparency of private digital platform companies. Administration of AI in the public sector thus falls outside the scope of this book.

[121] Stucke and Grunes, supra note 40, at 38; Marco Iansiti and Karim R. Lakhani, *Competing in the Age of AI: How Machine Intelligence Changes the Rules of Business* (Harvard Business Review Press 2020), at 96–97.

[122] Stucke and Grunes, *Ibid*., at 202.

In this context, concerns have been raised in relation to the abusive use of algorithms. After all, it may amount to the unfair treatment of competitors if algorithms are programed – wittingly or unwittingly – to prioritize a platform's own services over those of competitors.

Accordingly, increasing consideration is being given to why an algorithm of a search engine makes certain recommendations, as well as how a consumer can achieve different search results or access different ranking systems. In addition, turning back to the social media moderation practices discussed in Chapter 4, AI plays a material role in content moderation, including some context-specific content such as hate speech. When our behavioral data becomes algorithmic input, it is important to empower consumers to understand how a social media algorithm makes content moderation decisions, whether it is appropriate to use that content-moderating algorithm, and how consumers can receive objective algorithmic decisions.

More and more governments and civil societies are addressing commensurate algorithmic practices and calling for algorithmic transparency. They express caution over the unfair outcomes due to the lack of algorithmic transparency and advocate for algorithmic accountability, primarily to require platforms to disclose how their algorithms generate certain outputs.[123] In this regard, disclosing the algorithms or the source code that drives a platform's system may reveal whether the platform values one type of content over another. Alternatively, a lower degree of transparency that informs users of the main parameters that determine ranking, using plain language, may also be useful for the public in understanding how search engines work. Conversely, as discussed in greater detail below, some experts have pointed out that such transparency requirements may prove neither meaningful nor feasible due to the protection of trade secrets and the nature of machine learning.[124] The design of algorithmic systems is the product of substantial investment and may easily be duplicated by competitors if disclosed.

At this moment, regulators all over the world are contemplating various forms of regulation that will improve platform accountability, AI ethics, and algorithmic transparency and explainability for automated

[123] See Heike Felzmann et al., "Towards Transparency by Design for Artificial Intelligence" (2020) 26 Science and Engineering Ethics 3333.

[124] See generally, Dan L. Burk, "Algorithmic Legal Metrics" (2021) 96 Notre Dame Law Review 1147.

decision-making.[125] Algorithms can be governed by various regulatory choices, including who and what will be regulated, to whom information will be disclosed, and how disclosure will occur.[126] In the context of international economic law, the interplay between AI regulation and international trade agreements centers on questions relating to how to ensure that algorithmic accountability is appropriately distributed, as well as how to safeguard public access and oversight over algorithms. More profoundly, how can we balance competing interests in particular trade secrets and prevent AI regulations from being overly trade restrictive?

5.3.2 *Platform Transparency Requirements*

To answer the above questions, five "representative" digital/data regulations – including the DSA, the DMA, the GDPR, the Montréal Declaration for a Responsible Development of Artificial Intelligence (Montréal AI Declaration),[127] and the US bill on the Algorithmic Justice and Online Platform Transparency Act (Algorithmic Justice Act)[128] – are selected for an in-depth investigation. Transparency requirements in the five digital/data regulations, including both hard law and soft law, are reviewed to reveal the variables and their relationships. To clarify, this approach provides examples and is not meant to be comprehensive, as there are plenty of AI-related regulations or draft bills floating around,[129] but it aims to serve as an illustration to better

[125] Stucke and Grunes, supra note 40, at 1.

[126] Shin-yi Peng et al., "Artificial Intelligence and International Economic Law: A Research and Policy Agenda" in Shin-yi Peng et al. (eds), *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration* (Cambridge University Press 2021), at 10.

[127] Université de Montréal, The Montréal Declaration for a Responsible Development of Artificial Intelligence (2018). The Declaration is a set of nonbinding ethical guidelines that provide the basis for future national regulation.

[128] The Algorithmic Justice and Online Platform Transparency Act, S.1896, 117th US Congress (2021–2022) <www.congress.gov/bill/117th-congress/senate-bill/1896>. The Act, introduced by US Senator Edward Markey, aims to bring digital platforms into the regulatory framework, especially when using algorithms to moderate and recommend content. At the time of this writing, there were other key bills in the US House and Senate. Given the growing number of pending proposals, the selection of the Algorithmic Justice Act is not intended to predict that it will come to pass but, rather, to represent potential regulatory trends in the US.

[129] In particular, the EU Artificial Intelligence Act. Proposal for a Regulation of The European Parliament and of the Council Laying Down Harmonized Rules on

understand the key dimensions of platform transparency requirements in a comparative context.

5.3.2.1 Who: The Scope of the Regulatory Targets

As noted in Chapter 4, obligations under the DSA are cumulative depending on the function and size of a services supplier. The larger a services supplier is, and the more extensive the services it provides, the greater the number of obligations that apply. In terms of transparency, the DSA imposes a baseline transparency requirement, which applies to all intermediary services suppliers, and it then adds obligations for hosting services and online platforms, and then once again adds a further set of transparency obligations for VLOPs. In other words, VLOPS must comply with all of the transparency requirements imposed by the DSA, including transparency reporting,[130] transparency of recommender systems, transparency of online advertising,[131] and data sharing with authorities and researchers.[132]

Similarly, as stressed in the DMA's preamble, in most cases, gatekeepers provide online advertising services to business users in a nontransparent manner, which results in higher costs for online advertising services. To address this problem, it is important to ensure that the platform environment, and in particular, the conditions that apply to advertising services and rankings, is generally fair, transparent, and contestable. Therefore, the transparency obligations primarily fall to the gatekeepers.[133]

Unlike the asymmetric regulatory models of the DSA and the DMA, the scope of the regulatory targets of the GDPR, the Algorithmic Justice Act, and the Montréal AI Declaration is broader and more general. This is because concerns surrounding the lack of platform transparency extend to all kinds of platforms, regardless of their size.[134] In this regard, under the GDPR, provisions on platform transparency and accountability apply to all data controllers and processors, as defined in

Artificial Intelligence (Artificial Intelligence Act) and amending Certain Union Legislative Acts, COM/2021/206 final.

[130] This obligation applies to all intermediary services.

[131] These obligations apply to hosting and online services.

[132] This application applies to VLOPs only.

[133] Preamble to the DMA, paras. 45, 52, 58, and 72.

[134] Google's submission, "Digital Services Act package: Open Public Consultation" (2020) <https://blog.google/documents/89/Googles_submission_on_the_Digital_Services_Act_package_1.pdf/>.

Article 4.[135] Likewise, the principles in the Montréal AI Declaration are general and abstract and aim to apply to the digital and artificial intelligence field in a broad sense.[136] As broad as it may sound, however, the nonbinding nature of the declaration means that implementation is on a voluntary basis. Finally, the Algorithmic Justice Act imposes transparency obligations on an "online platform," which is defined as "any public-facing website, online service, online application, or mobile application which is operated for commercial purposes and provides a community forum for user generated content"[137] – a rather broad net.

5.3.2.2 What and to Whom: The Degree of Transparency

The five regulations vary in terms of what type of information should be transparent, ranging from algorithm-based advertising, algorithmic content moderation, algorithmic reporting, factors and parameters shaping algorithmic decisions, auditable records of the algorithmic process, and source code. Indeed, the degree of disclosure is controversial, and the policy options involve trade-offs. Unfettered government access to source code and algorithms may help to ensure that algorithms are fair but may also lead to unnecessary intrusion into privacy and trade secrets.[138] Taken to the extreme, platforms may be required to disclose source code.[139] However, would it be more proportionate to require them to make their algorithms transparent? Or is it more reasonable for platforms to merely publish the general factors and logic involved in algorithmic decisions? These questions must be analyzed in conjunction with the question of who receives transparency. As discussed below, the question of "disclosure to whom" dictates "what to disclose."

▪ **Authorities and Experts** As shown in Figure 5.1, platforms' disclosure obligations to regulatory bodies generally rank high on the scale

[135] GDPR, Article 4(7), 4(8).
[136] Preamble to the Montréal AI Declaration.
[137] Algorithmic Justice Act, Section 3(9).
[138] See generally Neha Mishra, "International Trade Law Meets Data Ethics: A Brave New World" (2020) 53(2) New York University Journal of International Law and Politics 305.
[139] See Section 5.3.3 of this book for further discussions. Note that algorithms and course code are different but related. Source code expresses algorithms. Algorithms are ideas – a process for solving a problem – while source code expresses and executes algorithms. Experts refer to algorithms as "conceptual" and to source code as "the manifestation of the concept in a particular programming language." For the difference between algorithm and code, see "Software Engineering" <https://softwareengineering.stackexchange.com>.

Legal Instruments / Variables	DSA	DMA	GDPR	Montréal AI Declaration	Algorithmic Justice Act
Disclosure Obligations to Authorities and Experts	H	H	H	H	M
Disclosure Obligations to Interested Parties	L	L	M	H	N
Disclosure Obligations to the Public	M	L	L	M	M
Explanation Obligations	H	H	H	L	L

Figure 5.1 Transparency requirements in context
Notes:
–Degree of Disclosure Obligations (Rows 1–3)
H: high (all data including algorithms and source code)
M: medium (algorithm parameters, algorithm auditing)
L: low (transparency reports, standard contracts)
N: none (no explicit rules)
–Degree of Explainability (Row 4)
H: high (inspections and interviews)
M: medium (machine-readable formats)
L: low (meaningful and comprehensible descriptions)
N: none (no explicit rules)

when measuring transparency. To illustrate, transparency can be restricted to governmental authorities. The rationale is that authorities need to use these records to verify compliance with regulatory requirements. On this matter, the GDPR focuses on supervisory authorities' investigative powers to obtain access to any premises of the data controller and the processor, including "any data processing equipment and means."[140] The Montréal AI Declaration, although nonbinding in nature, stresses the need for the code for algorithms to be accessible to relevant public authorities for verification and control purposes.[141] The Algorithmic Justice Act also calls for platforms to maintain records of algorithmic processes, and to make available to the supervisory agency

[140] GDPR, Article 58.
[141] Montréal AI Declaration, Principle 5(3).

complete records upon request.[142] After all, the algorithm itself may only be part of the story. Algorithmic decision-making cannot be accurately audited by reviewing the algorithms alone. It is important to ensure that the data on which an algorithm is trained is equally accessible.

In practice, however, the disclosed information, whether algorithms or source code, may not be understood by regulators, let alone the general public. Government agencies in most circumstances do not have the technical expertise to keep pace with and thus oversee the industry's sophisticated algorithms, which represents an impediment that would negate many benefits of disclosure.[143] Disclosure requirements may therefore need to involve specialized experts in carrying out necessary analyses.[144] In other words, authorities most likely rely on experts who are in a position to make assessments of the disclosed technical details. In this regard, the DSA explicitly stipulates that auditors and experts appointed by the EC during administrative inspections may require VLOPs to provide necessary information, including their information technology systems and algorithms.[145] Similarly, the DMA states that the Commission may require access to any data and algorithms of undertakings and information in order to carry out its duties.[146] Persons working under the supervision of the authorities, including auditors and experts appointed pursuant to the DMA, shall not disclose information acquired during inspections.[147] Limiting transparency to regulators and researchers, but not to the general public, appears to be an important mechanism by which to protect potentially sensitive information and data that would not be considered releasable to the public.

▪ **Interested Parties** Variations can be found in platforms' disclosure obligations to interested parties. In Figure 5.1, the degree of the obligations ranks low in the DSA and the DMA, medium in the GDPR, high in the Montréal AI Declaration, and is nonexistent in the Algorithmic Justice Act. To illustrate, both the DSA and the DMA have transparency provisions that would be available to interested parties, but the obligations are limited to relatively general information, without associated

[142] Algorithmic Justice Act, Section 4.
[143] Ezrachi and Stucke, supra note 36, at 231.
[144] Burk, supra note 124, at 1187.
[145] DSA, Article 69(5).
[146] DMA, Articles 21 and 36.
[147] *Ibid.*

technical details. For example, regarding content moderation, a platform should inform the recipient at the time of the removal of the decision through "a clear and specific statement of reasons" when it removes specific content.[148] Likewise, regarding advertising and ranking, a gatekeeper shall provide each advertiser to which it supplies advertising services with information regarding prices, fees, and remunerations. The gatekeeper shall also provide advertisers and publishers with access to "the performance measuring tools of the gatekeeper and the data necessary for advertisers and publishers to carry out their own independent verification of the advertisements inventory, including aggregated and non-aggregated data."[149]

On the contrary, the Montréal AI Declaration empowers "stakeholders and those affected by the situation" the same opportunity to access "the code for algorithms" for verification and control purposes.[150] The GDPR, in this regard, requires the data controller to provide individuals with the information necessary to ensure fair and transparent data processing. Where automated decision-making is involved, the disclosure obligations include the provision of "meaningful information about the logic involved" and "the envisaged consequences of such processing" to individuals.[151] A great deal of literature has explored what constitutes "meaningful information."[152] In any event, it can be presumed by reading in context that the information required under Articles 13 and 14 of the GDPR, although it need not be source code or complex algorithms, must be more than a general overview of the decision-making system – sufficiently concrete for the data subject to understand the reasons for a specific decision.[153] It therefore ranks medium in terms of the degree of transparency.

▪ **The Public** Finally, in connection with disclosure obligations to the public, among the five selected regulations, three of them rank medium, while two rank low. As revealed in Figure 5.1, the transparency requirements toward the public under the DSA, the Montréal AI Declaration, and the Algorithmic Justice Act extend to the level of algorithms'

[148] DSA, Article 17.
[149] DMA, Articles 5 and 6(8).
[150] Montréal AI Declaration, Principle 5(3), 5(4).
[151] GDPR, Article 14(2)(g).
[152] See, for example, Andrew D Selbst and Julia Powles, "Meaningful Information and the Right to Explanation" (2017) 7(4) International Data Privacy Law 233.
[153] *Ibid.*, at 236.

parameters and auditing, whereas those in the DMA and the GDPR remain at the level of general transparency reporting and standard contracts. More specifically, under the DSA, VLOPs are required to publish transparency reports at least every two months, and to release, in their terms and conditions, "the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters."[154] The "main parameters" include but are not limited to "the criteria which are most significant in determining the information suggested to the recipient of the service" and "the reasons for the relative importance of those parameters."[155] In a similar manner, the Montréal AI Declaration calls for public transparency of "the social parameters of the artificial intelligence systems,"[156] while the Algorithmic Justice Act advocates that the online platform should disclose, among other matters, "the method by which the type of algorithmic process prioritizes, assigns weight to, or ranks different categories of personal information to withhold, amplify, recommend, or promote content to a user."[157]

In terms of a textual comparison, public transparency obligations under the DMA and the GDPR are less specific and are therefore weaker. Under the DMA, gatekeepers are required to publish and update non-confidential summary of transparency reports, as well as make publicly available and update an overview of the audited descriptions.[158] The obligation is even less clear in the GDPR, under which the EC has the power to "lay down standard contractual clauses" for data processing. In addition, associations representing platforms may prepare codes of conduct addressing "fair and transparent processing."[159] On the whole, the degree of transparency to the broad public is relatively low in these two instruments.

5.3.2.3 How: The Degree of Explainability

Some skeptics emphasize that algorithmic transparency requirements may lend themselves to legal problems, because the algorithms themselves cannot explain "how they have arrived at a particular output."[160]

[154] DSA, Article 27(1).
[155] DSA, Article 27(2).
[156] Montréal AI Declaration, Principle 5(6), 5(8).
[157] Algorithmic Justice Act, Section 4(a)(1).
[158] DMA, Articles 11, 15.
[159] GDPR, Articles 28(7), 40(2).
[160] Selbst and Powles, supra note 152, at 234.

For example, releasing algorithms does not necessarily explain how they work and may not provide much meaningful information about, for example, the content moderation or ranking systems. Any degree of meaningful algorithmic transparency must therefore be accompanied by the requirement of explainability, that is, providing insights into the functioning of the algorithms "in a format that makes sense to the reader."[161]

The question is how. First of all, accurately explaining the functioning of algorithmic systems – particularly those developed using AI – is not always technically feasible. Algorithmic decision-making may involve complex and dynamic processes, as well as multiple profiling elements and data sources.[162] It may be commercially impossible to carry out an effective review.[163] Moreover, disclosure of incomprehensible technical details, even when available in machine-readable format, does not necessarily empower either the regulators or the interested parties to understand how they actually work.[164] Accordingly, as a subset of transparency requirements, the degree of explainability strongly correlates with to "whom to explain." As for the regulators, the power to acquire insights into how and why the algorithms work in certain ways by conducting inspections and carrying out input and output auditing is useful for supervisory purposes. Conversely, as for the general public, digital platforms' descriptions of algorithms' objectives, processes, and functioning, in plain language that is intelligible to lay people, represent meaningful information responsive to the right to know.[165]

Both the DSA and the DMA require different levels of explainability depending on "whom to explain to" and "why explain." The two instruments impose upon platforms the obligation to publish annual transparency reports "in clear, easily comprehensible language" and "in a machine-readable format."[166] Moreover, the EC has the power to conduct all necessary inspections at the premises of the VLOPs/gatekeepers, including requiring the services suppliers to provide access to and explanations of their "organization, functioning, IT system, algorithms,

[161] DOT Europe Position Paper, "Algorithmic Decision Making Transparency As Explainability" (2022) <https://doteurope.eu/wp-content/uploads/2022/01/DOT-Europe-PP-on-Algorithmic-Transparency.pdf>.
[162] *Ibid.*, at 1.
[163] Burk, supra note 144, at 1182.
[164] *Ibid.*, at 1187.
[165] *Ibid.*, at 1188.
[166] See, for example, DSA, Article 15.

data-handling and business practices," and allowing regulators to "address questions to their key personnel," and "record or document the explanations given."[167] The EC can also require access to any data and algorithms and request explanations of them.[168] Furthermore, the EC is mandated to carry out interviews and take statements during the investigation and is entitled to "record such interviews by any technical means."[169] As shown in Figure 5.1, the VLOPs/gatekeepers' cumulative obligations for explanations rank high in the given context. In contrast, requirements that algorithmic decision-making is explainable are relatively light in the Montréal AI Declaration and the Algorithmic Justice Act, which basically obligate services suppliers to provide a description of how the algorithmic process operates,[170] or to justify AI-based decisions in plain language that is understood by individuals whose quality of life and reputation are affected by the consequences of the algorithmic process.[171]

In this regard, it is worth noting that the text of the GDPR has provoked debate over whether it imposes upon data controllers an obligation of explainability when algorithmic decision-making is involved. Article 22 states that individuals "have the right not to be subject to a decision based solely on automated processing, including profiling" if such a decision has "legal effects or similarly significant effects" on concerned individuals. The same article requires a services supplier to "implement suitable measures" to safeguard individuals' "rights and freedoms and legitimate interests."[172] This requirement has been a source of controversy over whether algorithmics should be explainable. Note that suitable safeguards, according to Article 22, must include "at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision." The term "at least" indicates that this is not an exhaustive list of rights. Namely, it is an open list of suitable safeguards, and a services supplier is expected to do more than the basic requirements. Additionally, Recital 71 has added that the suitable safeguards are to include a right to an explanation of an automated decision. This textual interpretation thus creates a *sui generis* due process for algorithmic

[167] DSA, Article 69(5); DMA, Article 23(2)(d).
[168] DSA, Article 72(1); DMA, Article 21.
[169] See, for example, DMA, Article 22.
[170] Algorithmic Justice Act, Section 4(a)(2)(A)(iii).
[171] Montréal AI Declaration, Principle 5(2).
[172] GDPR, Article 22.

practices – a right to be heard, to be given an explanation, and to challenge an automated decision.[173]

In any event, just as the DSA and the DMA empower authorities to demand a high level of explainability for supervisory purposes, Article 58 of the GDPR states that authorities' investigative powers include access to any premise of the services supplier, any data processing equipment and means, as well as the ability to order the services supplier to "provide any information it requires for the performance of its tasks" – an outright obligation of explainability.[174] For this reason, the GDPR ranks high in terms of explainability, as shown in Figure 5.1, which denotes the cumulative degree of a given regulation.[175]

5.3.2.4 Variables and Comparison

To summarize, the five regulations selected implement various transparency measures, depending on the regulatory objectives and their context. Generally speaking, of the four dimensions assessed in Figure 5.1, the transparency obligation to authorities and experts appears in all five regulations and is the most significant requirement in terms of what must be disclosed. It is worth noting that the most evident variations are seen in transparency obligations to the interested parties and to the public. Moreover, the degree of technical detail required for explanation also varies greatly, from detailed auditable trails of algorithmic processing to general, plain-text descriptions. However, consistency has been found in the DSA, the DMA, and the GDPR, as they contain identical provisions requiring a high degree of explanation. To conclude, this case study demonstrates that the emerging regulations bring about greater transparency and oversight of the algorithms. The legal-technical details, however, differ in important ways. Although all of the five instruments place pressure on digital platforms to be more transparent, what kind of information should be provided and how it should be provided are dependent upon context, as well as to whom the disclosure is made.

Figure 5.1 measures the key elements of platform transparency and explainability reflected in the selected regulations, which form the basis of

[173] See generally European Parliament, "The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence" (2020) <www.europarl.europa.eu/stoa/en/document/EPRS_STU(2020)641530 > .

[174] GDPR, Article 58(1)(a), (1)(e), (1)(f).

[175] See generally Laura Edelson, "Platform Transparency Legislation: The Whos, Whats and Hows" (Lawfare, April 29, 2022).

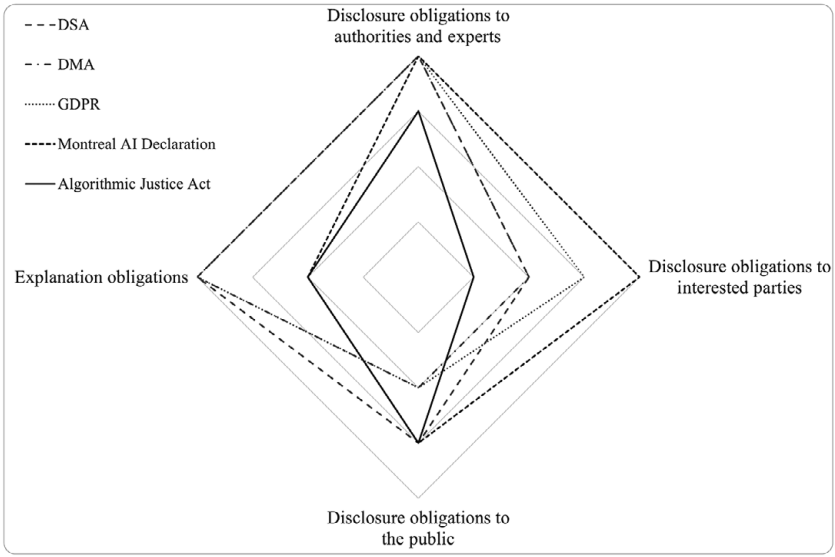

Figure 5.2 Regulatory fragmentation of transparency requirements
Notes:
–Central axis: none
–Second central axis: low
–Inner axis: medium
–Outer axis: high

the mapping exercise in Figure 5.2. Before this mapping exercise, one caveat is in order. Issues arise when comparing values across these axes, because each has a unique measuring scale. Note especially that the variables on the explanation obligations (row 4) represent different measuring scales. In other words, variables on the axis of explanation obligations are independent. With all of this in mind, Figure 5.2 shows the four variables mapped onto axes. The central axis is defined as "none," the second central axis as "low," the inner axis as "medium," and the outer axis as "high." As such, the areas of the polygons represent the overall degree of transparency and explainability requirements. Evidently, the five polygons overlap in some areas but are completely independent in other areas. Additionally, the shapes of individual polygons vary greatly. This case study thus concludes that the fragmentation of platform governance within and across jurisdictions is growing. Section 5.4 will continue to address how international trade agreements can help curb such fragmentation. However, let us first dive into the relevant provisions on

nondisclosure of source code and algorithms in the FTAs. What are the relevant provisions in international trade agreements, and how, if at all, do they affect a state's ability to regulate platform?

5.3.3 *Trade Rules on Source Code Disclosure*

5.3.3.1 Source Code Nondisclosure Provisions under the FTAs

A growing number of FTAs contain provisions to restrict access to source code. Article 14.17 of the CPTPP, for example, prohibits "the transfer of, or access to, source code" as a condition of the "import, distribution, sale or use" of software.[176] Essentially, source code nondisclosure provisions aim to prevent states from requiring technology transfer in exchange for international trade. In the context of digital platforms, services suppliers generally have invested resources in the development of source code. If they are required to disclose the source code as a condition of market access, they risk exposing their technologies to competitors and losing their competitive advantage. Source code nondisclosure provisions therefore safeguard software owners' rights over their intellectual property against mandatory disclosure.[177]

Traditionally, trade secret law has been the most widely used legal mechanism to protect software source code. Nonetheless, the specific expression of innovative software ideas can also be protected through other intellectual property rights, such as copyrights and patents. In this regard, the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) has for some time been the most relevant legal tool in terms of source code protection under the realm of international economic law.[178] Source code nondisclosure protections under the FTAs, however, go beyond the TRIPS by directly barring governments from demanding the disclosure of source code as a prerequisite for market

[176] See, for example, CPTPP, Article 14.17; USMCA, Article 19.16; Australia-Singapore Digital Economy Agreement, Article 28; The US–Japan Digital Trade Agreement, Article 17; The EU–Japan Economic Partnership Agreement, Article 8.73; The EU–UK Trade and Cooperation Agreement, Article 207.

[177] See generally Magdalena Słok-Wódkowska and Joanna Mazur, "Secrecy by Default: How Regional Trade Agreements Reshape Protection of Source Code" (2022) 25(1) Journal of International Economic Law 91. See also the UK Parliament, "Digital Trade and Data" First Report (June 23, 2021) <https://committees.parliament.uk/publications/6451/documents/70389/default/>, paras. 73–76.

[178] TRIPS, Articles 27 and 39.

access, subject to exceptions. Arguably, the trend to include the ban on the mandatory disclosure of source code provisions in the FTAs stems from the emerging need for greater source code protections, and in particular, in response to some state actions, such as China's policy of forcing foreign firms to disclose their source code and/or "other parts of their intellectual property" as a condition for doing business in China.[179]

In addition to source code, several FTAs extend the general prohibition on disclosure requirements to algorithms. For example, Article 19.16 (Source Code) of the USMCA bans mandatory transfers and access to both the source code and the algorithm expressed in it, stating the following:

> 1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, *or to an algorithm expressed in that source code*, as a condition for the *import, distribution, sale or use* of that software, or of products containing that software, in its territory (emphasis added).
> 2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to *the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding*, subject to safeguards against unauthorized disclosure[180] (emphasis added).

Here, an algorithm is broadly defined in these agreements as "a defined sequence of steps, taken to solve a problem or obtain a result."[181] At the time of this writing, similar text could be found in Section C.3 (1) – Source Code of the WTO JSI on E-commerce.[182] The inclusion of algorithms substantially broadens the scope of the source code nondisclosure provisions. By preventing the mandatory disclosure of

[179] See Cosmina Dorobantu et al., "Source Code Disclosure: A Primer for Trade Negotiators" in Ingo Borchert and Alan Winters (eds), *Addressing Impediments to Digital Trade* (CEPR Press 2021), at 105–140.

[180] USMCA, Article 19.16.

[181] USMCA, Article 19.1. See also supra note 139 for the distinction between source code and algorithms.

[182] WTO Electronic Commerce Negotiations – Consolidated Negotiating Text, INF/ECOM/62/Rev.1 (December 2020).

algorithms in addition to that of source code as a condition for market access, the USMCA-type of source code nondisclosure provision makes it clear that it also prohibits requirements to disclose algorithms. Unless justified by exceptions, a USMCA party seeking access to the algorithms used by digital platforms as a condition for digital trade market access would be inconsistent with Article 19.16 of the USMCA.

The expanded scope of the prohibition on disclosure requirements thus raises concerns about its impact on the ability of governments to regulate the use of algorithms at the domestic level. Civil societies such as the Australian Council of Trade Unions stressed that preventing relevant authorities from accessing source code and algorithms altogether would unduly restrict governments from supervising platforms' compliance with domestic regulations and ensuring algorithmic accountability.[183] They believed that keeping source code and algorithms secret also makes it difficult for the public to understand how the algorithms make decisions, and whether there is bias or discrimination within the process.[184] Indeed, compared to FTA provisions that only preclude the accessibility of source code, FTA provisions that additionally preclude the mandatory accessibility of algorithms place further restrictions on the power of authorities to protect consumers.[185] It is notable that the key source codes and algorithms that drive datafication are primarily owned by the digital platforms, and in particular the big tech companies. Some critics have therefore asserted that the consequences of restrictions to algorithm access would jeopardize the ability of governments to "develop regulatory measures that could ensure transparency of algorithmic governance tools."[186] In their view, the expanded scope of source code nondisclosure provisions in international economic law conceivably protects private capital – the source code and algorithms owned by the digital platforms – at the expense of governments' full regulatory autonomy to supervise legal compliance.[187]

[183] Australian Council of Trade Unions, "Australia-Singapore Digital Economy Agreement: Submission by the Australian Council of Trade Unions to the Joint Standing Committee on Treaties" ACTU D. No 49/2020 (25 September 2020), at 11.

[184] *Ibid.*

[185] Dorobant et al., supra note 179, at 114.

[186] Słok-Wódkowska and Mazur, supra note 177, at 93.

[187] *Ibid.* See also Jane Kelsey, "Digital Trade Rules and Big Tech: Surrendering Public Good to Private Power" (2020) Public Services International, at 16. See also the UK Parliament, supra note 177, para. 78.

5.3.3.2 The Supervision of Algorithms

To the contrary, some believe that the USMCA-type source code nondisclosure provisions, given their broad scope to cover "vital digital assets," can better help to enhance business trust and protect foreign firms from unauthorized disclosure.[188] In the view of Mitchell and Mishra, a diligent balance has been achieved in USMCA Article 19.16 by restricting governments from forcing the disclosure of both source code and algorithms on the one end, and ensuring that governments can place demands on foreign firms to disclose their source code and algorithms for accountability and regulatory purposes, on the other end.[189] Specifically, attention should be given to the second paragraph of USMCA Article 19.16, which explicitly states that the provision does not preclude a regulatory body or judicial authority from requiring access to source codes or algorithms "for a specific investigation, inspection, examination, enforcement action, or judicial proceeding."

In fact, such a similarly worded regulatory/judicial preclusion can be found in the source code nondisclosure provisions of several international trade agreements, such as the US–Japan Digital Trade Agreement, the Australia-Singapore Digital Economy Agreement (DEA), and the Korea-Singapore Digital Partnership Agreement (KSDPA).[190] Moreover, as a subset of regulatory/judicial preclusion, the EU-Japan Economic Partnership Agreement and EU-New Zealand FTA, for example, also allow a court, an administrative tribunal, or a competition authority to require access to source code owned by foreign firms to remedy a violation of competition law.[191] Altogether, source code nondisclosure provisions do not seem to compromise the regulatory autonomy on digital platforms, because governments still retain the power to investigate and audit automated content-moderating systems, biased and discriminatory algorithms, and algorithmic recommendation and ranking processes.

It should also be emphasized that the source code nondisclosure provisions in the FTAs target the market access of software businesses,

[188] Andrew D. Mitchell & Neha Mishra, "Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute" (2019) 22(3) Journal of International Economic Law 389, 413.

[189] *Ibid*., at 414.

[190] See, for example, Australia-Singapore Digital Economy Agreement, Article 28. See also Korea-Singapore Digital Partnership Agreement, Article 14.19.

[191] The EU–Japan Economic Partnership Agreement, Article 8.73. See also the EU–New Zealand FTA, Article 12.11.

namely, "import, distribution, sale or use of software," for supplying international trade. Essentially, these provisions are centered on "market access" and are not designed to constrain governments from requiring information to investigate compliance. It can be argued that a country's right to regulate digital platforms would not be adversely affected by these provisions as long as the regulatory actions do not block the market access of foreign services. Turning back to the first row of Figure 5.1, platforms' disclosure obligations to the regulatory body generally rank high on the scale when measuring transparency. For instance, Article 69 of the DSA mandates that regulators conduct inspections, including requiring access to the algorithms of the very large online search engines. In a similar vein, Articles 21 and 23 of the DMA empower regulators to require access to all necessary information for the inspection, including any data and algorithms. One could contend that such inspection power under the DSA and the DMA does not necessarily constitute a condition for market access and therefore is consistent with the FTAs' source code nondisclosure provisions.

Nonetheless, as discussed in Section 3.5, there are situations in which the boundary between market access prerequisites and non-market access regulations is blurred. To some extent, any transparency requirement, no matter how "pure" its design for regulatory purposes, would potentially affect the "distribution, sale, or use" of software in the given market. Therefore, it is disputable how far the FTAs' nondisclosure provisions can go in this regard. In any event, assuming that any regulatory action had been broadly construed as a market access prerequisite, the government would have to rely on the carve-out and exceptions to justify the mandatory disclosure of the source code and algorithms.

First turning to the carve-outs for critical infrastructure services: Some source code nondisclosure provisions allow for the forced disclosure of information relating to critical infrastructure.[192] The term "critical infrastructure," however, was left undefined in the Digital Trade/E-Commerce Chapter. Accordingly, what the concept of "critical infrastructure" might cover would be interpreted pursuant to the previous discussion in Chapter 2.

[192] Article 14.17(2) of the CPTPP states: "For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure."

Second, the general exceptions and the security exceptions are available in all of these provisions.[193] In my view, even if measures that are necessary to enhance platform accountability and maintain digital legal order were found to fall within the scope of market access-related restrictions, they could be justifiable under exceptions, and in particular, the public morals general exceptions. As previously discussed in Chapters 1 and 2, the country implementing the disputed transparency requirements would have to prove that the measure at issue satisfies the necessity test and the Chapeau test under the public morals exceptions. It is worth reiterating that according to WTO jurisprudence, a country has the regulatory autonomy to choose its level of protection in relation to the objective being pursued, which is, in this context, fair and transparent algorithmic decision-making in a datafied business environment. Any less trade-restrictive alternatives proposed by the governments of foreign platforms must qualify as reasonably available alternatives under the necessity test.

At the end of the day, the ambit within which source codes and algorithms can be kept secret under international economic law relies on the exceptions, entailing a delicate balance between the competing interests involving platforms' trade secrets, digital innovation, algorithmic accountability, and other legitimate public objectives. With that in mind, this book argues that international regulatory coherence and cooperation surrounding platform regulations should be an important direction for global governance in a platform economy. Good regulatory practices (GRP) with *ex-ante* regulatory impact assessment (RIA), when appropriately implemented, can help identify and address unnecessary trade restrictions, forestall potential trade disputes at earlier stages, and reduce the likelihood of lengthy and costly dispute settlement procedures. Section 5.4 will continue to discuss the opportunities and challenges of such an approach to global platform governance.

5.4 Good Regulatory Practices for Platform Governance

5.4.1 Potential Fragmentation and Overreaching

Drawing from the analysis above, the fragmentation of platform regulation – whether it relates to content moderation, competition policy, or

[193] See, for example, CPTPP, Article 14.2; Australia-Singapore Digital Economy Agreement, Article 28 and FN 17.

algorithmic transparency – is growing. The proliferation of platform regulations and algorithmic disciplines means that services suppliers are confronting more and more difficulties when attempting to comply with diverse national "behind-the-border measures." The lack of regulatory coherence among states may create costly and burdensome tasks for services suppliers, because when operating at international scale, they must meet different degrees of obligation and satisfy divergent legal standards. Such regulatory fragmentation may direct resources away from more effective business management. This is particularly true for non-big tech, small and medium-size enterprises (SMEs) that lack the resources to manage unique legal requirements in different locations. Taking transparency obligations as an example, as shown in Figure 5.2, complexity surrounding various legal approaches may become a barrier to digital trade, especially for SMEs when those rules apply to them. Truly, as Trachtman pointed out, platform regulations of different states have varying concerns and varying exceptions, and thus may prove contradictory in a complex fashion.[194] The emerging fragmentation and possible contradiction of data governance call for cross-border regulatory coherence and cooperation mechanisms to harmonize the divergent regulatory approaches stemming from disparate public policy objectives and digital trade interests.

At the same time, and relatedly, there are more and more examples of potential regulatory overreaching governmental intervention, which render global platform governance even more difficult. Going beyond the selected five regulations in Figure 5.2, several national and local regulations on algorithmic transparency have raised concerns about policymakers' emerging overreaching practices in this innovation sector. Taking China's "Qinglang – 2022 Algorithm Comprehensive Governance Special Action" as an example, which aims to keep digital platforms on tight leashes, under this special action, Chinese tech giants – including Alibaba, Tencent and TikTok (ByteDance) – have submitted algorithms used in their services to China's Internet watchdog.[195] Indeed, digital platform regulations reflect different priorities in different countries, which further complicates the question of how to manage fragmentation in global platform governance.

[194] Joel P. Trachtman, "Platforms and Global Governance: Globalization on Steroids" (2023) 26(1) Journal of International Economic Law 78, at 83.

[195] "China Regulator Says Alibaba, Tencent Have Submitted App Algorithm Details" (*Reuters*, August 15 2002).

At the crux of the matter is the desire to promote the development of a more harmonized regime that encourages innovation while protecting other public objectives. Conceptually, as denoted by the Manila Principles, platform regulations should comply with the tests of necessity and proportionality to ensure that platform obligations are linked to a specific public objective, the degree of obligations are proportionate to that objective, and regulators' powers extend only to the necessary information.[196] This raises the question of whether international economic law can serve as an effective tool to promote regulatory coherence and prevent regulatory overreach. As the global economy goes digital, how can we apply GRP to the domestic regulation given the complex issues involved in a datafied world? Can the regulatory disciplines in the GATS or the FTAs help reduce the likelihood of disguised or unnecessarily restrictive impediments to the platform economy and ease potential regulatory fragmentation and overreaching?

5.4.2 *Good Governance Obligations*

There has been substantial progress in the development of regulatory discipline through international trade instruments at both the multilateral and regional levels. The ambition of the international GRP agenda is aimed at fostering regulatory coherence by offering a systemic response to the inherent potential problems of regulation that may impose costs but add little overall benefits.[197] At the multilateral level, the WTO JSI on Domestic Regulation of Services (the "DR JSI," or "DR Reference Paper") was concluded in December 2021.[198] The participating members, which

[196] Developed by NGOs, the Manila Principles are a set of standards for takedown that aim to guide governments to protect free expression. "Manila Principles on Intermediary Liability" <https://manilaprinciples.org/index.html>.

[197] Martin Lodge and Kai Wegrich, *Managing Regulation: Regulatory Analysis Politics and Policy* (Palgrave Macmillan 2012), at 211. In the WTO context, Article VI:1 of the GATS, which contains procedural requirements to ensure that all measures of general application affecting trade in services are to be administered in a "reasonable, objective and impartial manner," can be seen as an obligation that imposes a fundamental standard for due process. In the FTA context, the regulatory chapters set forth specific obligations with respect to GRP, including procedural transparency and engagement with interested persons. See for example, USMCA, Article 28.4 (Internal Coordination); Article. 28.6 (Early Planning); Article 28.8 (Use of Plain Language); Article 28.13 (Retrospective Review). See also CPTPP, Article 25.8 (Engagement with Interested Persons).

[198] WTO, "Declaration on the Conclusion of Negotiations on Services Domestic Regulation" WT/L/1129 (December 2, 2021).

represent more than 90 percent of the services trade, have agreed on a set of GRP, which will be implemented by incorporating the DR Reference Paper into their GATS Schedules of Commitments. While the DR JSI was negotiated plurilaterally, the outcome will be implemented on a most-favored-nation basis. In other words, the benefits will apply to all WTO members, not just the participants.[199] The DR JSI contains three core principles:[200]

- Regulatory transparency: measures aimed at promoting prompt publication and availability of information and stakeholder engagement in regulatory processes;
- Regulatory predictability: measures aimed at ensuring a reasonable time frame and procedural due process;
- Regulatory quality: measures aimed at disseminating GRP to facilitate the services trade, including ensuring that regulators develop technical standards through open processes and reach their decisions in a manner independent of services suppliers.

In the context of digital platform regulation, these regulatory disciplines establish legally binding guidelines, within which participating countries have the flexibility to regulate the platforms and pursue their policy objectives. Participating countries retain the right to impose digital/data regulations including algorithmic transparency, which arguably is a "technical standard" within the meaning of Article VI:4 of the GATS, on services suppliers.[201] However, it must be done in accordance with the regulatory disciplines laid out in the DR Reference Paper – that is, to improve the good governance landscape through regulatory transparency, predictability, and nondiscrimination.[202]

At the regional level, the development of GRP under the FTAs can be seen as a response to the issues of regulatory fragmentation and overreaching. Within the last decade or so, good governance obligations have

[199] WTO, "Joint Initiative on Services Domestic Regulation Reference Paper on Services Domestic Regulation" INF/SDR/2 (November 26, 2021).

[200] *Ibid.*

[201] Informal Note by the Chairman, "Disciplines on Domestic Regulation Pursuant to GATS Article VI:4" Room Document (April 18, 2006), para. II:5. "Technical standards" are "measures that lay down the characteristics of a service or the manner in which it is supplied." Technical standards also include the procedures relating to the enforcement of such standards.

[202] Panagiotis Delimatsis, "Concluding the WTO Services Negotiations on Domestic Regulation – Hopes and Fears" (2010) 9(4) World Trade Review 643, at 659.

been progressively negotiated, and in some cases, incorporated into bilateral and regional trade agreements.[203] The reality that market access alone cannot sufficiently safeguard services suppliers to operate effectively in foreign markets has led international trade negotiations to address the issue of GRP.[204] Notable developments in this regard can be found in the more recent FTAs that include a comprehensive set of good governance obligations in a separate chapter. Parties to these FTAs agreed to adopt "GATS plus" regulatory obligations, which are largely equivalent to the DR Reference Paper or even extend beyond it with more advanced disciplines. More recent examples include Chapter 22 (Good Regulatory Practices and Regulatory Cooperation) of the EU–New Zealand FTA, concluded in 2022, and Chapter 26 (Good Regulatory Practice) of the UK–Australia FTA, concluded in 2021. These new regulatory disciplines are set to stipulate minimum standards that must be observed by the FTA parties when adopting and applying domestic regulations, which, if implemented effectively, might in turn offer promising venues for overcoming regulatory fragmentation and potential overreaching. The assumption is that domestic administrative practices in different jurisdictions would become more compatible and reasonable if countries observe, throughout the regulatory cycle, a set of "minimum common quality standards."[205]

Taking CPTPP and USMCA as representative instruments, the Regulatory Coherence Chapter under the CPTPP and the Good Regulatory Practices Chapter under the USMCA set forth specific obligations with respect to GRP, such as promoting information quality, procedural transparency, clear and plain regulatory language, early planning and retrospective review of regulations, central and internal coordination, and engagement with interested persons.[206] In particular, parties have committed to "minimize unnecessary regulatory differences and to

[203] Rodrigo Polanco, "The Trans-Pacific Partnership Agreement and Regulatory Coherence" in Tania Voon (ed), *Trade Liberalization and International Cooperation: A Legal Analysis of the Trans-Pacific Partnership Agreement* (Edward Elgar 2013) 231, at 232–238.

[204] Laura Baiker et al., "Services Domestic Regulation: Locking in Good Regulatory Practices" WTO Working Paper ERSD-2021–14 (September 17, 2021) <www.wto.org/english/res_e/reser_e/ersd202114_e.pdf>, at 7.

[205] Gabriel Gari, "Recent Preferential Trade Agreements' Disciplines for Tackling Regulatory Divergence in Services: How Far beyond GATS?" (2020) 19(1) World Trade Review 1, at 12.

[206] See supra note 197.

facilitate trade or investment,"[207] without compromising each state's regulatory autonomy to pursue its public policy objectives. Possible mechanisms for promoting regulatory coherence include exchanging technical information and data and exploring common approaches to tackling the risks posed by the use of emerging technologies.[208] In addition, under both the CPTPP and the USMCA, the core of GRP is the need to conduct an impact assessment when developing regulations. More specifically, the second paragraph of Article 28.11 of the USMCA delineates the procedures and considerations under which an RIA should be conducted, which highlights the procedures of the regulatory assessment as follows:

> (a) the need for a proposed regulation, including a description of the nature and significance of the problem the regulation is intended to address;
> (b) feasible and appropriate regulatory and non-regulatory alternatives that would address the need identified in subparagraph (a), including the alternative of not regulating;
> (c) benefits and costs of the selected and other feasible alternatives, including the relevant impacts . . . as well as risks and distributional effects over time, recognizing that some costs and benefits are difficult to quantify or monetize; and
> (d) the grounds for concluding that the selected alternative is preferable.[209]

Amid the Biden administration's agenda to increase economic cooperation through the IPEF, it is not surprising to see that GRP is one of the key initiatives under the framework. The USTR has declared that it will seek to "advance the benefits of good regulatory practices in supporting good governance"[210] and "build on the outcome reached in the WTO Joint Initiative on Services Domestic Regulation, as appropriate."[211] In fact, when the USTR of the Obama administration led the TPP negotiations, the USTR repeatedly stressed the importance of the inclusion of a chapter on regulatory coherence in the TPP, as it reflects the growing

[207] USMCA, Article 28.17.
[208] *Ibid.*
[209] USMCA, Article 28.11 (Regulatory Impact Assessment), paragraph 2.
[210] USTR, "Ministerial Text for Trade Pillar of the Indo-Pacific Economic Framework for Prosperity" (September 23, 2022).
[211] *Ibid.*

relevance of regulatory issues to international trade and investment.[212] In light of the fact that the legal and regulatory environment in TPP parties is diverse, the USTR had advocated for the incorporation of regulatory coherence into the TPP to eliminate the problem of "overlapping and inconsistent regulatory requirements or regulations being developed unfairly and without a sound basis."[213] Now, six years after the US withdrew from the CPTPP, the IPEF seems to have the potential to reassert US economic engagement to counter China's growing influence and promote US regulatory approaches and standards in the region.

The crux of the matter, however, is to what extent good governance obligations in international trade agreements can tackle regulatory fragmentation and combat unreasonable administrative practices. Will these regulatory principles and methodological tools bring about greater policy coherence in the governance of the digital economy? When domestic regulators are faced with questions of how to regulate digital platforms, in what way can these GRP converge the fragmented legal approaches to issues such as content moderation, cultural diversity, platform competition, and algorithmic transparency? For the reasons explained below, this book contends that far more political will is needed to ensure that the GRPs/RIAs do the trick.

5.4.3 Marching toward Policy Coherence in Platform Governance?

5.4.3.1 The Breadth and Strength of GRP/RIA

First of all, although relatively ambitious GRP provisions can be found in some FTAs,[214] other FTAs contain only symbolic GRP provisions. For example, the chapter on the "General Provisions and Exceptions" of the RCEP establishes obligations on minimum standards of regulatory transparency and due process in the administrative proceedings. However, the RCEP is silent on many higher standards of GRPs to prevent undue delay in authorization or arbitrary administration. In particular, the absence of RIA in the RCEP implies fewer safeguards to ensure regulatory quality

[212] USTR, "Summary of the Trans-Pacific Partnership Agreement" (October 4, 2015) <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership>.

[213] *Ibid.*

[214] Outstanding examples include the EU-Canada Comprehensive Economic and Trade Agreement (CETA), CPTPP, USMCA, Australia–UK FTA, EU-New Zealand Free Trade Agreement, etc.

than if such provisions were included, leaving the RCEP behind in the developments of GRPs compared to other recently negotiated FTAs.[215] Arguably, divergences in the regulatory frameworks of Asian countries, especially China, have made it challenging to conclude "harder GRP obligations."

Second, even for those countries that are parties to FTAs with more ambitious GRPs, one fundamental question surrounding the possible contributions of the GRPs to the quality of platform regulation is the breadth of their application. Normatively speaking, the applicable coverage of the GRPs is rather uncertain. Here, a typical example is Article 25.1 of the CPTPP, which stipulates that the "covered regulatory measure" under its Regulatory Coherence Chapter refers to "the regulatory measure determined by each Party."[216] According to Article 25.3, each party shall determine and make publicly available the scope of its covered regulatory measures. Article 25.3 further requires that "in determining the scope of covered regulatory measures, each Party should aim to achieve significant coverage."[217] In other words, although the definition of "regulatory measure" is rather broad, referring to "any measure of general application . . . adopted by regulatory agencies with which compliance is mandatory,"[218] the exact scope of the "covered regulatory measures" is flexible. Each party has the discretion to decide to what extent its domestic regulation should be subject to GRPs. Empirically speaking, some notifications from the CPTPP parties in this regard are encouraging. In particular, developed countries such as Japan and Australia have adopted "covered regulatory measures" that are general and extensive.[219] However, considering that the application of the GRPs generally requires administrative resources to complete, it is likely that some governments may tend to establish a minimum threshold in terms of the obligation to perform GRPs.[220] After all, GRPs not only require

[215] APEC, "Study on APEC's Non-binding Principles for Domestic Regulation of the Services Sector" (2021) <www.apec.org/Publications/2020/01/Study-on-APECs-Non-binding-Principles-for-Domestic-Regulation-of-the-Services-Sector>, at 23.

[216] CPTPP, Article 25.1.

[217] CPTPP, Article 25.3.

[218] CPTPP, Article 25.1.

[219] Ministry of Foreign Affairs of Japan, "Related Information on CPTPP Chapter 25 (Regulatory Coherence)" <www.mofa.go.jp/ecm/ep/page24e_000257.html>; Australian Government, "Chapter Summary: Regulatory Coherence" <www.dfat.gov.au/sites/default/files/regulatory-coherence.pdf>.

[220] This discussion draws upon materials in Shin-yi Peng, "Lessons from the TPP Regulatory Coherence Chapter: The Laws Governing Unsolicited Commercial

changes in the institutional setting, but also demand adjustments in the behavior and mindset of civil servants.[221] Therefore, platform regulations are not necessarily subject to GRPs/RIAs.

Third, even assuming that a country has made legally binding commitments to GRPs in FTAs, the real impact may not be significant due to the narrow range of domestic regulatory instruments that are subject to GRPs. For example, Article 28.1 of the USMCA explicitly limits the scope of "regulation" under the Good Regulatory Practices Chapter to the "measure of general application adopted, issued, or maintained by a regulatory authority with which compliance is mandatory."[222] The definition of "regulatory authority" under the chapter, however, is limited to "an administrative authority or agency at the Party's central level of government that develops, proposes or adopts a regulation."[223] The definition explicitly excludes "legislatures or courts."[224] In other words, the GRPs/RIAs only apply to "few" but not "all" regulatory instruments that impact platform activities. In terms of platform regulation, the fact that the GRPs only apply to the executive branch of governments but not to legislatures or parliaments means that the RIAs, in some countries, are at most carried out by agency-made digital rules.

Finally, assuming *arguendo* that a platform regulation falls within the range of regulatory instruments subject to GRPs, the strength of the application of RIAs might be weakened by divergent methodologies. As previously indicated, RIA has been defined as a systemic approach to critically identifying and assessing the regulatory effects – including the existing regulations and proposed nonregulatory alternatives.[225] In the context of digital platform regulations, policymakers should identify problems arising from platform monopolies and data capitalism, determine the need for intervention, propose alternative regulatory options ranging from competition law to algorithmic transparency, and then assess and decide upon the preferred policy option. Throughout the process, the assessment – whether it is qualitative or quantitative – can be

Electronic Messages as a Case Study" in Shin-yi Peng et al. (eds), *Governing Science and Technology under the International Economic Order: Regulatory Divergence and Convergence in the Age of Mega-regionals* (Edward Elgar 2018) 64, at 70–80.

[221] *Ibid.*, at 71.

[222] USMCA, Article 28.1 (Definitions).

[223] *Ibid.*

[224] OECD, "Regulatory Impact Assessment, OECD Best Practice Principles for Regulatory Policy" (2020), at 19–20.

[225] OECD, "Regulatory Impact Analysis: A Tool for Policy Coherence" (2009), at 185.

accomplished by employing various techniques. According to the OECD, the adoption of RIA is now becoming widespread, but it operates differently within and across countries.[226] Methodologically speaking, various RIA procedures can be designed and used. As a result, policymakers' understanding of the procedure of RIA varies greatly. In practice, RIA has been uniquely practiced by different countries or even different governmental bodies.[227]

This raises the question of how the good governance obligations under the FTAs help ensure that policymakers "choose the best regulatory option" when designing and implementing platform regulations, and how the GRPs/RIAs help converge the fragmented legal approaches to the platform economy. At their heart, GRPs under the FTAs were intentionally framed in flexible terms to reserve room for an individual FTA party to decide how extensively it will commit. It is clear that the RIA provisions under the FTAs do not provide much guidance as to how to operate the process. To place these questions into a more concrete setting, both the DSA and the DMA "passed" the RIA test conducted by the EC before implementation. The European Commission's Impact Assessment Report of the DSA (the RIA Report) is over 200 pages long, containing a detailed analysis of what the problem drivers are, why the EU should act, what the policy options are, what the impacts of these options are, how the options compare, and which option is preferred.[228] The RIA Report concludes that the DSA is in full compliance with the EU's international obligations in the WTO and FTAs.[229] The RIA Report underscores that the DSA is in line with the nondiscrimination provisions of the GATS, as it establishes objective criteria, including the definition of VLOPs, regardless of the origin of the services supplier.[230] Moreover, the RIA Report states that the asymmetric regulation, which imposes additional transparency requirements on the VLOPs, does not jeopardize the protection of trade secrets of digital platforms because the DSA entails

[226] *Ibid.*, at 8.
[227] *Ibid.*, at 19–20.
[228] European Commission, "Impact Assessment Accompanying the document Proposal For a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC" SWD(2020) 348 final (December 15, 2020).
[229] *Ibid.*, para. 8.
[230] *Ibid.*, para. 213.

a secrecy obligation on the authorities and experts with regard to trade secrets.[231]

Would the same conclusion of the RIA Report be drawn if a different RIA methodology is introduced? Probably not. As explained by Alemanno, a cost–benefit analysis in many cases can be "extra-territorially blind."[232] Both the costs of regulatory fragmentation and the benefits of regulatory coherence might be underestimated. Measurements in the RIA procedure can also be problematic when quantification is not possible, and in that case, the RIA might become a "rubber stamp" to endorse administrative decisions without carefully scrutinizing them,[233] effectively serving as a mere justification for policymakers' choices. At the end of the day, the cost–benefit analysis is more about local value preferences. When local preferences and policy priorities are involved, the process has a more subjective character.[234] As Gari observes, this world might be increasingly globalized and interconnected, but deep differences among countries remain in terms of regulatory needs.[235]

5.4.3.2 Political Support Needed for Future Governance

All in all, in light of the above, the trend of developing GRP obligations under the international trade agreements has the potential to serve as an important tool to address regulatory fragmentation, but much will depend on the political will of the governments involved. Given that the "obligations" of regulatory coherence are predominately phrased in a soft and loose way, the effectiveness of the GRPs, especially the successful incorporation of RIAs into regulatory policy, is dependent upon strong administrative determination. To put it another way, regulatory

[231] *Ibid.*, para. 259.

[232] Alberto Alemanno, "Is There a Role for Cost–Benefit Analysis Beyond the Nation-State? Lessons from International Regulatory Co-operation" in Michael A. Livermore & Richard L. Revesz (eds), *The Globalization of Cost–Benefit Analysis in Environmental Policy* (Oxford University Press 2013), at 104.

[233] OECD, "Policy Brief: Improving the Quality of Regulations" (2009), at 3; Stuart Shapiro, "The Triumph of Regulatory Politics: Benefit–Cost Analysis and Political Salience" (2012) 6 Regulation & Governance 189.

[234] Shin-yi Peng, "Levelling the Playing Field between Sharing Platforms and Industry Incumbents: Good Regulatory Practices?" in Anupam Chander and Haochen Sun (eds), *Data Sovereignty: From the Digital Silk Road to the Return of the State* (Oxford University Press 2023), chapter 7.

[235] Gari, supra note 205, at 29.

divergence can also be seen as an outcome of democratic legitimacy.[236] The potential impact of the good governance obligations under the WTO or FTAs in tackling regulatory fragmentation is therefore constrained.[237] Pushing the goals of GRPs/RIAs too far may generate concerns related to an undue degree of intrusion upon a country's right to regulate.[238] For this reason, the breadth and strength of the GRPs/RIAs fundamentally rest on political support for good-faith implementation. However, despite the above considerations, there are reasons for being optimistic about better governance through international trade agreements.

First, in terms of the applicable coverage of the GRPs, there seems to be a growing political willingness to endorse the relevant initiatives. At the WTO, additional members have joined the DR JSI to "make their regulatory environment more conducive to business," and to "lower trade costs for services suppliers seeking to access foreign markets."[239] At the regional level, more and more new-generation FTAs contain the GRP obligations. Although they are primarily drafted in flexible language, they nevertheless provide a baseline for parties to undertake regulatory reform. Over time, such soft obligations may help the parties to align with trends leaning toward more transparent and predictable regulatory frameworks – which are vital to services trade across borders.[240] Platform suppliers, especially SMEs, will eventually benefit from improved regulatory quality and facilitation.

Second, in terms of a greater political willingness to implement GRPs, one promising direction is to establish a central oversight body to perform checks of draft RIA reports.[241] Historically, it has not been unusual for regulators to conduct an "incomplete" assessment of the economic costs and benefits of regulatory alternatives.[242] Policymakers may fail to generate a comprehensive evaluation of the possible impacts of regulation, resulting in "stove-piped" internal decisions that lead to conflicting regulatory approaches in the administrative system.[243]

[236] Anne Meuwese, "Constitutional Aspects of Regulatory Coherence in TTIP: An EU Perspective" (2015) 78 Law & Contemporary Problems 153.
[237] Gari, supra note 205, at 28.
[238] *Ibid.*, at 29.
[239] WTO, "Georgia, Timor-Leste and United Arab Emirates Join Initiative on Services Domestic Regulation" (June 13, 2022).
[240] Baiker et al., supra note 204, at 33, 40.
[241] OECD, supra note 224, at 17–20.
[242] *Ibid.*, at 17.
[243] *Ibid.*, at 19.

However, according to OECD studies, more and more jurisdictions, including both OECD and non-OECD countries, have dedicated a single governmental body to be responsible for reviewing regulatory quality in the national administration from a "whole-of-government" perspective.[244] Alternatively, an increasing number of countries are establishing a specific parliamentary committee with responsibilities for monitoring the quality of the RIA system as a whole.[245] As previously discussed, in the context of platform regulation, the primary institutional challenge in the introduction of RIAs is to coordinate diverse considerations – for example, competition policy, consumer protection, freedom of speech, trade secrets, industrial innovation, and other public objectives – in an integrated manner. The fact that many countries are now creating a centralized coordinating body within their jurisdictions as a quality assurance mechanism is a sign of governments' willingness to embed GRPs and RIA scrutiny in their policymaking systems.

Finally, in terms of the methodology of RIAs, some innovative approaches have been introduced into the realm of platform regulation, which represent a significant step in promoting coherence in digital policy. For example, the "Digital Checklists" contained in the EU's "Better Regulation toolbox" are specifically designed to identify the digital issues and impacts surrounding new policies. Any proposed regulation with digital dimensions should go through the Toolbox when defining the problem, assessing impacts, developing policy options, and choosing digital policy solutions.[246] Similar approaches have been adopted in the UK's RIA guidance, which effectively integrates competition policy with RIAs by requiring the assessment to "incorporate an explicit consideration of the competition impacts of regulatory proposals."[247] More importantly, there is a general tendency to not only embrace domestic market dynamics, but to also address international aspects such as market openness.[248] The increasing degree of attention accorded data-driven factors in the RIA context indicates a

[244] *Ibid.*
[245] *Ibid.*, at 33.
[246] European Commission, "Better Regulation: Guidelines and Toolbox" (November 3, 2021) <https://ec.europa.eu/info/law/law-making-process/planning-and-proposing-law/better-regulation-why-and-how/better-regulation-guidelines-and-toolbox_en>.
[247] UK's Department for Business, Energy & Industrial Strategy, "Better Regulation Framework" (2020) <www.gov.uk/government/publications/better-regulation-framework>, at 14.
[248] OECD, supra note 224, at 20.

promising venue to advance the more coherent governance of platform activities.[249]

5.5 Conclusion

We have investigated the driving forces of platformization. When data becomes capital and the algorithmic input of the digital platforms, the interplay between national regulation and international economic law is complex and multilayered. The specific aspects considered in Chapters 3–5 help formulate views and outlooks regarding the role of international economic law in the politics of datafication. The discussions in Part II also lead us to reflect on what international trade agreements have done and can do in global platform governance. Let us now shift gears to the broad digital ecosystem and continue to explore the phenomenon of datafication from a cross-layer perspective: data flows. Chapter 6 will bring a sharper focus to privacy and cybersecurity.

[249] *Ibid*., at 31.