9

International Economic Law's Regulation of Data as a Resource for the Artificial Intelligence Economy

Thomas Streinz

I DATA AS A RESOURCE FOR THE ARTIFICIAL INTELLIGENCE ECONOMY

Business capacity to collect and process digitalized information (data) at unprecedented scale and speed is transforming economies around the globe. One aspect of this transformation is the relevance of data as a 'resource' for relatively recent advancements in artificial intelligence (AI) technology in various forms of machine learning, most notably 'deep learning'. The theoretical foundations for this kind of AI go back to the 1950s, but only the availability of novel and larger datasets led to the end of a long 'AI winter' and the dawn of an 'AI spring'.[1]

The growing but unevenly distributed ability to capture information about the world in digital form is a complex phenomenon. The public discourse surrounding data seems somewhat detached from the sophisticated ways in which scholars have theorized the relationship between data, information, knowledge, and wisdom.[2] The lack of adequate terminology to capture the phenomena caused by the gradual digitalization of economies and societies is evidenced by the vain search for metaphorical equivalents.[3] The effort to assess the effects of digitalization on the economy is severely hindered by a paradoxical lack of data about data, since the commercial value of data is reflected neither in balance sheets nor in the conventional metrics used to assess the state of the economy or trade.[4] Yet, it seems misguided to attribute this lamentable state of affairs solely to the notorious intransparency of global digital corporations or the inertia of accountants, statisticians,

[1] TJ Sejnowski, *The Deep Learning Revolution* (Boston, MA, MIT Press, 2018). On the relevance of AI technology for international economic law, see also Chapter 1 in this volume.

[2] R Kitchin, 'Conceptualising Data', in *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* (Los Angeles, CA, SAGE Publishing, 2014).

[3] 'The World's Most Valuable Resource Is No Longer Oil, but Data' (*The Economist*, 6 May 2017), https://perma.cc/YBN2-XW6D.

[4] J Haskel and S Westlake, *Capitalism Without Capital: The Rise of the Intangible Economy* (Princeton, NJ, Princeton University Press, 2017); M Mazzucato, *The Value of Everything: Making and Taking in the Global Economy* (London, Penguin Books, 2017); D Ciuriak, 'Unpacking the Valuation of Data in the Data-Driven Economy' (27 April 2019), https://ssrn.com/abstract=3379133.

https://doi.org/10.1017/9781108954006.010 Published online by Cambridge University Press

and policy-makers in responding to digitalization on unprecedented scales. Data's variegated characteristics pose distinct challenges for data's economic evaluation and legal conceptualization.[5] This chapter cannot resolve these questions. It treats data as an essential rent-generating productive asset in the AI economy – and therefore also a contested economic resource.[6]

The chapter builds on and expands earlier work on data-related provisions in recent instruments of international economic law (IEL) and sketches some questions for ongoing and future research about how IEL might need to be recalibrated to adapt to a global digital economy.[7] This earlier work focused on the new template of rules for a global digital economy that the United States championed in the negotiations for the Trans-Pacific Partnership (TPP), now in force as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),[8] followed by the US-Mexico-Canada Agreement (USMCA),[9] and the Japan-US Digital Trade Agreement (JUSDTA).[10] Negotiations on new rules for 'electronic commerce' in the World Trade Organization (WTO) seem unlikely to yield tangible outcomes in the near term,[11] but certain CPTPP members have moved ahead with TPP-plus templates for digital economy agreements, ostensibly designed for adoption by others.[12] While the tension between data governance in trade agreements and domestic data protection and privacy policies is increasingly

[5] This is one theme of the Global Data Law project launched by Guarini Global Law & Tech at NYU Law. More information and videos from the first two conferences are available at www.guariniglobal.org/global-data-law.

[6] D Ciuriak and M Ptashkina, 'The State Also Rises: The Role of the State in the Age of Data' (June 2020), https://ssrn.com/abstract=3663387; D Ciuriak, 'Data as a Contested Economic Resource: Framing the Issues' (23 November 2019), https://ssrn.com/abstract=3496281.

[7] See also T Streinz, 'Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy', in Benedict Kingsbury et al. (eds), *Megaregulation Contested: Global Economic Ordering After TPP* (Oxford, Oxford University Press, 2019) ch. 9.

[8] CPTPP entered into force for Australia, Canada, Japan, Mexico, New Zealand, and Singapore in December 2018, and for Vietnam in January 2019. Brunei, Chile, Malaysia, and Peru have signed the agreement but did not ratify it. A consolidated version of CPTPP is available at www.iilj.org/megareg/materials.

[9] Initially signed on 30 November 2018. Revised version signed on 10 December 2019. Text available at https://perma.cc/GS3J-WSTR. The agreement entered into force on 1 July 2020.

[10] Signed on 7 October 2019. Text available at https://perma.cc/UUA9-7NUD. The agreement entered into force on 1 January 2020.

[11] As of January 2020, 83 WTO members participated in plurilateral negotiations, albeit only five African countries, only three least developed countries, and no WTO members from the Caribbean or developing Pacific Island countries. See Y Ismail, 'E-commerce in the World Trade Organization: History and latest developments in the negotiations under the Joint Statement' (IISD Report, January 2020). In December 2020, a consolidated negotiating text (WTO Doc. INF/ECOM/62) was leaked, indicating both progress and continued disagreement. See also Henry Gao's Chapter 15 in this volume.

[12] The Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand, and Singapore – signed electronically during the COVID-19 pandemic in June 2020 – follows a modular logic to facilitate flexible adoption. DEPA's text is available at https://perma.cc/U23E-URUS. The agreement has been in force between Singapore and New Zealand since December 2020. The Australia-Singapore Digital Economy Agreement (ASDEA) was signed in August 2020. It

better understood (despite the persistent silos and splendid isolation in which the trade and privacy communities have long operated),[13] there is surprisingly little discussion about the ways in which existing and emerging IEL constrain and shape states' policy choices for data-driven economic development.

This chapter is an attempt to contribute to this much-needed debate by exploring the extent to which IEL regulates data as a resource for the AI economy. Section II identifies regulatory interventions – open data initiatives, cross-border data transfer restrictions, and mandatory data sharing – that nation states are already enacting or at least contemplating to ensure access to data for their domestic AI economy. Section III shows how some of these regulatory interventions are in tension with existing and emerging commitments under international trade and investment law along the dimensions of data control (mainly through international intellectual property law and international investment law) and data mobility (mainly through commitments in favor of free data flows and against data localization). Section IV concludes by imagining ways through which IEL could provide more flexibility for experimental digital economy policies to confront asymmetric control over data as countries transition, asynchronously and unevenly, toward an AI economy.

II EMERGING DIGITAL ECONOMY POLICIES: REGULATING DATA AS A RESOURCE

By January 2020, twelve of the G20 countries had announced official AI strategies, with others bound to follow.[14] Virtually all of these strategies discuss the relevance of data for a future AI economy, commonly under the somewhat vague concept of 'data governance'. The emphasis is often on data protection and privacy-related concerns, which is a function of the dominant legal discourse in the digital domain and the gradual emergence and subsequent entrenchment of certain regulatory models for data protection.[15] Countries' AI strategies increasingly also recognize and address concerns about discrimination caused by algorithmic bias. In contrast, the regulatory interventions that states are considering to challenge the domination of the digital domain by US and Chinese companies, especially in AI, are relatively timid, with the notable exceptions of the European Union's (EU's) antitrust enforcement

contains novel provisions on submarine data cables and digital standard-setting; its text is available at www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf.

[13] See, for example, S Yakovleva and K Irion, 'Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade' (2020) *International Data Privacy Law* 1; see also Alan Hervé's Chapter 10 in this volume.

[14] See the very helpful overview by T Struett, 'G20 AI Strategies on Data Governance', https://datagovhub.org/g20-ai-strategies (https://perma.cc/FLM3-UBCW).

[15] See T Streinz, 'The Evolution of European Data Law', in P Craig and G de Burca (eds), *The Evolution of EU Law* (3rd ed., Oxford: Oxford University Press 2021) ch. 29, preprint available at https://ssrn.com/abstract=3762971.

https://doi.org/10.1017/9781108954006.010 Published online by Cambridge University Press

against US companies[16] and India's emerging e-commerce policy that espouses an openly protectionist agenda to grow a domestic AI economy fueled by 'Indian data'.[17]

Countries that recognize the salience of data for the AI economy often endorse efforts to make governmental data available as 'open data'. While several countries have some form of data transfer restrictions to retain jurisdictional control over data, India stands out in its advocacy for restricting the outward transfer of data to safeguard data as a national resource, thereby challenging the anti-protectionism consensus in IEL. Some jurisdictions recognize a need for regulatory intervention to transfer data from those who have it to those who want or need it. Exploring each of these three interventions – open data, data transfer restrictions, and mandatory data sharing – as efforts to regulate data as a resource for the AI economy reveals their limited purchase in confronting pervasive data concentration – and makes apparent that alternative measures might be needed.[18]

A *Open Data Initiatives*

The open data movement has been quite successful in convincing governments that making *governmental* data publicly accessible under open data licenses is in their best interest to stimulate the domestic (or even local) AI economy. Examples include the EU's Open Data Directive[19] and Singapore's 'Smart Nation' initiative,[20] but the open data bandwagon also carries several developing countries.[21] There are many reasons for and drivers behind the push for open data, one of which is the purported value for innovation and economic growth.[22] AI development is often referenced as a use case for open data: the remarkable improvements in algorithmic image recognition technology, now widely deployed for facial recognition purposes, have been linked to the ImageNet dataset providing free and publicly available access to image data.[23]

[16] See, for example, I Graef, 'When Data Evolves into Market Power: Data Concentration and Data Abuse under Competition Law', in M Moore and D Tambini (eds), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford, Oxford University Press, 2018), at 71.

[17] 'Draft National e-Commerce Policy: India's Data for India's Development' (23 February 2019), https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.

[18] See A Fisher and T Streinz, *Confronting Data Inequality*, World Bank Development Report 2021 background paper (1 April 2021), https://ssrn.com/abstract=3825724.

[19] Directive (EU) 2019/1024 on open data and the re-use of public sector information, OJ 2019 No. L 172, 26 June 2019, at 56.

[20] See Singapore's open data resources: https://perma.cc/JAX3-55U8.

[21] SG Verhulst and A Young, 'Open Data in Developing Economies' (GovLab, November 2017), https://perma.cc/W9VN-452K.

[22] See J Gray, 'Towards a Genealogy of Open Data' (2014), https://ssrn.com/abstract=2605828.

[23] See 'ImageNet', www.image-net.org. See also Kayu Yang et al, 'Towards fairer datasets: Filtering and balancing the distribution of the people subtree in the ImageNet hierarchy' FAT* '20 (January 2020), https://doi.org/10.1145/3351095.3375709 (detailing problems in the ImageNet dataset).

It is, however, much less clear who actually benefits from 'public' data becoming available as 'open' data. Open data might be beneficial for a wide range of reasons,[24] but it is not an effective way to counterbalance the pervasive data control asymmetries in the global digital economy. To the contrary, one might suspect that those with the capacity to collect open data and to correlate it with the 'closed data' under their (often infrastructural) control stand to gain more than those who lack such capabilities and have to rely on open data entirely. This also has geopolitical implications as those operating out of relatively closed digital economies – such as China – are able to capture open data elsewhere in addition to the data they collect domestically without much external competition.[25]

In certain cases, the local relevance of a certain dataset (for example, traffic data in Taipei) might indicate heightened relevance for a local community, which might incentivize local initiatives to use such local data for local development. But the frequency and salience of such a dynamic, while plausible, needs to be empirically established. It is equally possible that non-local actors will use local data to train algorithms for deployment locally, or indeed elsewhere. Opening up governmental data may benefit AI development, but the local or domestic development of an AI economy is highly contingent on other factors, such as research capacity, data processing ability, and so forth.

Against this backdrop, it is worth noting that the question of whether more privately held data should be made available to governments, businesses, or citizens seems comparatively underexplored.[26] Private entities are willing to share certain datasets for research purposes, but the legal technology used for such data transfers is usually contracting, not open data licenses.[27] Data contracting allows for more legal control over the conditions under which data is being shared, used, and distributed.[28] If governments wanted to make private data available, they could facilitate private–public data sharing by providing more legal certainty (for example, through model contracts, especially with a view toward mitigating liability risks) or by requiring the openness of data generated with public support (analogous to open access publishing requirements),[29] if not requiring mandatory data sharing outright, as explored further below.[30]

[24] See BS Noveck, 'Rights-Based and Tech-Driven: Open Data, Freedom of Information, and the Future of Government Transparency' (2017) 19 *Yale Human Rights & Development Law Journal* 1 (claiming benefits for innovation and state–citizen collaboration more broadly).

[25] I owe this insight, and many others, to Benedict Kingsbury.

[26] But see A Alemanno, 'Data for Good: Unlocking Privately-Held Data to the Benefit of the Many' (2018) 9 *European Journal of Risk Regulation* 2.

[27] There are exceptions; for example, Google's open image dataset of more than 9 million labeled images has been made available under a CC-BY 4.0 license: https://perma.cc/2ERW-JC4L.

[28] See 'Data Sharing Agreement', www.contractstandards.com/public/contracts/data-sharing-agreement.

[29] The EU requires open access publishing under Article 29.2 of the Model Grant Agreement of its Horizon 2020 research agenda: https://perma.cc/2VUD-KSUM.

[30] See Section II.C.

https://doi.org/10.1017/9781108954006.010 Published online by Cambridge University Press

B *Data Transfer Restrictions*

Several jurisdictions impose data transfer restrictions to secure jurisdictional control over certain categories of data.[31] The EU's General Data Protection Regulation (GDPR)[32] is routinely accused by US actors as a 'protectionist' instrument, designed to favor the European digital economy, albeit with questionable results.[33] This critique often alleges that the GDPR's intended purpose of protecting European data subjects' personal data and privacy and its underlying fundamental rights justification are false pretenses for protectionist digital industrial policy.[34] Drawing a contrast between data protection and data protectionism tacitly assumes that the economic theories in support of trade in goods and services also apply to data, despite its different and arguably unique characteristics.[35] The relationship between data protection and privacy on the one hand and data-driven innovation and economic growth on the other is more complicated than the protection/protectionism binary suggests.[36] The GDPR's predecessor – the European Data Protection Directive (DPD) – was in part motivated by concerns that disparate data protection regimes across the European single market would stymie the nascent European Internet economy.[37] Much less attention was paid, however, to the question of how European data protection law would affect the conditions under which the European digital economy operates in comparison to the rest of the world. The DPD's restriction on transfers of personal data from the EU to third countries was not designed as an instrument of economic policy but was meant to ensure that personal data would remain protected even if transferred outside the EU's territory.[38] These features contributed to the 'Brussels Effect' and the global diffusion of EU-style

[31] T Streinz, 'Data Localization as an Instrument of Jurisdictional Control' (draft paper, on file with author).

[32] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ 2016 No. L 119, 4 May 2016, at 1.

[33] The Washington, DC-based Information Technology and Innovation Foundation (ITIF) is among the most outspoken critics of the European approach to regulating the digital economy. See, for example, E Chivot and D Castro, 'What the Evidence Shows About the Impact of the GDPR After One Year' (ITIF, 17 June 2019), https://perma.cc/TW8V-GGLW.

[34] See for a careful analysis of the competing narratives S Yakovleva, 'Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy' (2020) 74 *University of Miami Law Review* 416.

[35] But see SA Aaronson, 'What Are We Talking About When We Talk About Digital Protectionism?' (2019) 18 *World Trade Review* 541.

[36] Y Lev-Aretz and KJ Strandburg, 'Privacy Regulation and Innovation Policy' (2020) 22 *Yale Journal of Law and Tech* 256; M Gal and O Aviv, 'The Competitive Effects of the GDPR' (2020) *Journal of Competition Law and Economics* 349.

[37] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 No. L 281, 23 November 1995, at 31.

[38] Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, ECLI:EU:C:2020:559 (16 July 2020); on the genesis of the restriction see K Hon, *Data Localization Law and Policy* (Cheltenham, Edward Elgar Publishing, 2017), at chs 2 and 3; Paul M. Schwartz, 'European Data Protection Law and Restrictions on International Data Flows' (1995) 80 *Iowa Law Review* 471.

data protection through law.[39] The EU's new data strategy, announced with great fanfare in February 2020, conceives of data as an economic resource and seeks to reframe the GDPR as sound economic policy domestically (ensuring consumer trust in the digital economy) and globally (supposedly giving the European digital economy a competitive edge because of the EU's role as global data regulator), without mentioning the restriction on extra-EU transfers of personal data explicitly.[40]

In contrast, India has come forward with a draft 'e-commerce policy' that openly advocates for data transfer restrictions for reasons of economic policy rather than data protection concerns, whether genuine or not. The policy document – which, of course, still needs to be converted into operational law – laments the absence of a legal framework that would allow the Indian government to impose restrictions on the export of valuable data:

> Without having access to the huge trove of data that would be generated within India, the possibility of Indian business entities creating high value digital products would be almost nil. . . . Further, by not imposing restrictions on cross-border data flow, India would itself be shutting the doors for creation of high-value digital products in the country.[41]

This is a remarkable departure from a key tenet of the Silicon Valley Consensus according to which the uninhibited "free flow" of data is the best way to develop a digital economy. Whatever one's initial view of this policy proposal, it deserves careful legal and economic analysis, because it asks important and underexplored questions: if data is the key resource of the digital economy, especially for AI development, how to facilitate optimal allocation of this resource? Who captures its value? And how can those who do not immediately benefit from the digital transformation be supported, and by whom?

The Indian proposal assumes a strong role for the government in mediating the transition of India toward a digital economy, but this is by no means the only institutional solution imaginable. Moreover, in light of India's proposal to limit the transfer of data *from* India to ensure access to data for the domestic AI economy, one may wonder whether it might be more beneficial to incentivize the transfer of relevant data *to* India. Such ideas challenge the Silicon Valley Consensus, which holds that optimal data allocation is to be achieved through market mechanisms only – despite the digital economy's pervasive data control asymmetries and resulting market failures.[42]

[39] A Bradford, *The Brussels Effect* (New York, Oxford University Press, 2020) ; P Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 *NYU Law Review* 771.

[40] European Commission, A European Strategy for Data, COM(2020) 66 final (hereinafter European Strategy for Data).

[41] Draft National e-Commerce Policy, note 19 above, at 15.

[42] D Ciuriak, 'Rethinking Industrial Policy for the Data-Driven Economy' (2018) CIGI Papers No. 192, at 6 (calling this the 'original sin' of the data-driven economy). Even those in favor of radical market solutions lament that the 'data titans' do not pay for the data on which they rely: see EA Posner and

C *Mandatory Data Sharing*

Digitalization changes the conditions under which capitalism operates.[43] Companies with superior data collection capacities benefit as they exploit the resulting information asymmetries.[44] E-commerce platforms may be able to leverage their intermediary position to gather information about commercial transactions on either side of the two-sided market they facilitate. Relying on predictive algorithms, they may be able to engineer demand through targeted advertising. The price to be paid may no longer be uniform – determined by aggregate supply and demand – but is 'personalized' (i.e., discriminatory).[45] Legally mandated data sharing has been proposed as a policy intervention to counterbalance the digital economy's tendency to create winner-takes-all dynamics and to ensure a competitive environment conducive to innovation.[46] But alternative justifications for mandatory data sharing are plausible, including data redistribution.

The EU and Australia are among the jurisdictions that have experimented with certain forms of mandatory data sharing. The EU's GDPR contains a right to data portability that requires data controllers to transmit personal data in a structured, commonly used, and machine-readable format to another data controller, at the request of the data subject.[47] The provision is supposed to enhance data protection by creating a more competitive environment (on the assumption that consumers will gravitate toward firms with higher data protection standards), but its impact has been muted.[48] In contrast, Australia's Consumer Data Right (CDR) bill was not primarily designed as a data protection law. It provides for the sharing of consumption data with consumers and accredited third parties, subject to data privacy safeguards, in certain sectors.[49]

EG Weyl, *Radical Markets: Uprooting Capitalism and Democracy for a Just Society* (Princeton, NJ, Princeton University Press, 2018), at 231.

43 Some even call into question whether Friedrich Hayek's conceptualization of the market as a superior information aggregation mechanism still holds and imagine alternative arrangements; see E Morozov, 'Digital Socialism? The Calculation Debate in the Age of Big Data' (2019) 116/117 *New Left Review* 33; P Pałka, 'Algorithmic Central Planning: Between Efficiency and Freedom' (2020) 83 *Law and Contemporary Problems* 125.

44 J Stiglitz, 'The Revolution of Information Economics: The Past and the Future' (2017) NBER Working Paper No. 23780.

45 EG Weyl, 'A Price Theory of Multi-Sided Platforms' (2010) 100 *American Economic Review* 1642.

46 V Mayer-Schönberger and T Ramge, *Reinventing Capitalism in the Age of Big Data* (New York, Basic Books, 2018); J Prüfer, 'Competition Policy and Mandatory Data Sharing on Data-Driven Markets' (2020) TILEC Policy Paper.

47 GDPR, Article 20; see also Frederike Zufall and Raphael Zingg's Chapter 11 in this volume.

48 G Nicholas and M Weinberg, 'Data Portability and Platform Competition: Is User Data Exported from Facebook Actually Useful to Competitors?' (2019), www.law.nyu.edu/centers/engelberg/pubs/2019-11-06-Data-Portability-And-Platform-Competition.

49 Treasury Laws Amendment (Consumer Data Right) Bill 2019; see J Meese et al., 'Citizen or Consumer? Contrasting Australia and Europe's Data Protection Policies' (2019) 8 *Internet Policy Review* 1.

The discussion around mandatory data sharing is most advanced in the banking sector. The EU's second payment services directive requires banks to share consumers' payment account data with third-party providers (under the condition that the consumers explicitly consented to such transfers).[50] The goal is to advance competition between traditional banks and newly emerging financial services providers, some of which rely heavily on algorithmic analysis of financial data. Banks seem to have acquiesced to these new regulatory demands by creating dedicated data transfer infrastructures in the form of web-based application programming interfaces (APIs).[51] Automotive vehicle data is another data category that is increasingly subject to mandatory data-sharing requirements. In some jurisdictions, car manufacturers must make vehicle data available to independent repair shops.[52] The EU's European data strategy contemplates further interventions in a variety of sectors, including agricultural, industrial, and health data, where other arrangements prove insufficient to facilitate data sharing.[53] The salience of data for AI development seems likely to spur further such initiatives elsewhere. As the next section explores, data holders will seek to mobilize existing and emerging commitments under IEL to oppose mandatory data sharing and data mobility restrictions.

III REGULATION OF DATA MOBILITY AND CONTROL UNDER INTERNATIONAL ECONOMIC LAW

IEL regulates data along at least two dimensions that are somewhat in tension with each other: data mobility (where does data reside and where can it move?) and data control (who has data and who decides how it can be used?). While new rules on free flows and data localization regulate data in favor of transnational data mobility, existing IEL, especially international IP and investment law, entrenches private control over data by limiting states' ability to mandate data disclosure and sharing. This chapter's focus on substantive disciplines regarding data mobility and data control is not to downplay the extent to which contemporary IEL leads to deep transformations of the regulatory state by introducing a wide range of horizontal and sectoral *procedural* requirements, which may be especially salient if new regulation is being considered in a not yet or under-regulated

[50] Directive (EU) 2015/2366 on payment services in the internal market, OJ (2015) L No. 337, 23 December 2015, at 35. Australia is contemplating a comparable 'consumer data right' for banking; see Australian Competition and Consumer Commission, Competition and Consumer (Consumer Data Right) Rules 2019, accc.gov.au.

[51] O Borgogno and G Colangelo, 'Data Sharing and Interoperability: Fostering Innovation and Competition through APIs' (2019) 35 *Computer Law & Security Review* 1.

[52] See 'Mandatory Scheme for the Sharing of Motor Vehicle Service and Repair Information' (29 October 2019), https://treasury.gov.au/publication/p2019-30661. Vehicle data sharing with the government is under consideration: see National Transport Commission, 'Government Access to Vehicle-Generated Data Discussion Paper' (May 2020), ntc.gov.au.

[53] European Strategy for Data, note 40 above.

https://doi.org/10.1017/9781108954006.010 Published online by Cambridge University Press

domain.[54] Indeed, it is precisely through these procedural mechanisms that those who control data will seek to mobilize IEL to their advantage transnationally.[55] IEL is routinely invoked by lawyers representing firms, trade associations, regulatory agencies, and other actors in opposition to or support of their clients' preferred policy outcome. In this way, domestic law is to a significant extent continuously being shaped and reshaped by IEL.[56]

A *Regulation of Data Mobility*

Several disciplines in international trade law regulate data mobility in favor of cross-border transfers of data, at the expense of nation states' ability to restrict such transfers or to require the location of computing facilities (such as routers, servers, or data centers) within their territory. While established disciplines under the rules for trade in goods and trade in services in general, and telecommunication services in particular, only apply to certain categories of data, the new disciplines in "e-commerce" and "digital trade" chapters of agreements like CPTPP or USMCA apply to 'information', including personal information, generally.[57] Under the 'digital trade' framing, certain cross-border transfers of data can be conceptualized as trade in digital goods or as trade in digital services. To accommodate nonphysical goods, dedicated provisions address 'digital products'[58] that enjoy protections from discriminatory treatment.[59] However, data that is not produced for commercial sale or distribution but that is generated or assembled for machine learning purposes apparently escapes the digital product category. Similarly, if data is used to train algorithms that provide services (for example, financial services based on algorithms trained with financial market data), only the services, but not the data used to

[54] See Streinz, note 9 above. The Agreement on Technical Barriers to Trade (TBT), in particular, has emerged as a frame of reference for digital policies generally and World Trade Organization (WTO) members now routinely use the TBT committee to raise their concerns regarding new regulatory policies in the digital domain. For example, China's keystone data regulation, the Cybersecurity Law of 2017, has given rise to specific trade concerns in eleven meetings of the TBT Committee since June 2017 as members took issue with the requirement for domestic storage of personal information and the restriction on cross-border data flows, among other matters. See the WTO's dedicated TBT database at http://tbtims.wto.org and also Aik Hoe Lim's Chapter 5 in this volume.

[55] See P Mertenskötter and RB Stewart, 'Remote Control: Treaty Requirements for Regulatory Procedures' (2019) 104 *Cornell Law Review* 165.

[56] The impact of international economic law on domestic law-making outside of litigation is difficult to ascertain and requires a sophisticated social science methodology not generally used by legal scholars. But see T Dorlach and P Mertenskötter, 'Interpreters of International Economic Law: Corporations and Bureaucrats in Contest Over Chile's Nutrition Label' (2020) 54 *Law & Society Review* 571.

[57] TPP, Article 14.11; USMCA, Article 19.11; USJDTA, Article 11.

[58] Article 1 (g) of the USJDTA defines 'digital product' as a computer program, text, video, image, sound recording, or other product that is digitally encoded, produced for commercial sale or distribution, and that can be transmitted electronically. Footnote 1 clarifies that a digital product does not include a digitized representation of a financial instrument, including money, thereby excluding cryptocurrencies.

[59] USJDTA, Article 8. Note the qualified carve-out for taxation measures in Article 6.

provide the services, enjoy the protections under the General Agreement on Trade in Services (GATS) and the equivalent provisions in free trade agreements. GATS commitments apply if data is an end (data as a service) and not just a means to an end, and only if the WTO member in question has made specific commitments toward services liberalization in its schedule. Relevant categories in this regard encompass data processing services, software programming services, and various kinds of telecommunication services.[60]

Under the contested principle of technology neutrality, established commitments for services – formerly provided in analog form but now increasingly provided digitally – automatically acquire the same liberalization status as their analog counterparts.[61] In this way, the gradual digitalization of services can lead to a gradual liberalization of services economies that registered relatively liberal commitments for analog services. Conversely, some digital services escape the WTO's classification of services altogether, thereby creating new gaps within the system. It was, for example, unclear under which category Google's core business – providing search services – could be subsumed before the revised classification included a dedicated category for 'web search portal content'.[62]

If a WTO member has made specific commitments to allow for cross-border market access of digital foreign service providers, full-scale data transfer limitations that amount to a 'total prohibition' of the relevant service are principally illegal under Article XVI:2 (c) GATS (zero quotas).[63] Data transfer limitations that fall short of a 'total prohibition', as is the case under both the EU and the proposed Indian model, are not affected by this prohibition. They would need to comply, however, with the general obligation to national (that is, nondiscriminatory) treatment contained in Article XVII GATS and the requirement to administer any such limitation in a reasonable, objective, and impartial manner under Article VI GATS. The former would not apply to a situation in which both domestic and foreign service suppliers would need to comply with the data transfer limitations in question. The latter may give rise to a violation if the GATS member can show that the EU, for instance, conducted its adequacy assessment in an unreasonable, subjective, or partial manner. In this way, the GATS metaregulates the regime for personal data

[60] The full list of specific commitments can be found in WTO members' GATS schedules registered as GATS/SC/135 according to the WTO's Services Sectoral Classification List (W/120).

[61] See J Kelsey, 'How a TPP-Style E-commerce Outcome in the WTO Would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO)' (2018) 21 *Journal of International Economic Law* 273; see also R Baldwin, *The Globotics Upheaval: Globalisation, Robotics and the Future of Work* (Oxford, Oxford University Press, 2019).

[62] Compare H Gao, 'Google's China Problem: A Case Study on Trade, Technology, and Human Rights under the GATS' (2011) 6 *Asian Journal of WTO and International Health Law and Policy* 349 (discussing several possibilities for classification under the original services classification in force when most WTO members entered their commitments); I Willemyns, 'GATS Classification of Digital Services – Does "The Cloud" Have a Silver Lining?' (2019) 53 *Journal of World Trade* 59 (arguing for comprehensive GATS application to digital services based on functionalist analysis).

[63] Reasoning by analogy to WTO Appellate Body, *US – Gambling*, WT/DS285/AB/R (20 April 2005).

https://doi.org/10.1017/9781108954006.010 Published online by Cambridge University Press

transfers under the EU's GDPR. While the EU is principally allowed to adopt and enforce measures to protect the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts, it must not do so in a manner that would constitute an arbitrary or unjustifiable discrimination between comparable countries or a disguised restriction on trade in services.[64] In contrast, no such general exception exists for the Indian proposal to limit the transfer of Indian data for overtly protectionist purposes. This is likely inconsequential, because India made only minimal commitments toward services liberalization, but nevertheless paradigmatic for international trade law's aversion against 'protectionism' that is being carried forward in the digital domain.

Contrast the multilateral rules for trade in services under GATS – which are contingent on services classification, dependent on specific commitments by states, and not tailored toward questions of data mobility – with the newly created rules in agreements such as CPTPP, USMCA, and USJDTA that are specifically designed to protect data mobility against transnational data transfer restrictions.

These rules contain commitments to refrain from prohibiting or restricting the cross-border transfer of information, unless such measures are necessary to achieve a public policy objective and are not arbitrary, unjustifiably discriminatory, a trade restriction in disguise, or more restrictive than necessary.[65] The last clause, the trade law version of a necessity test, in particular, is reason enough for the EU to oppose these kinds of provisions in plurilateral (as in the case of the failed Trade in Services Agreement (TISA)) and bilateral negotiations (as in the case of the cratered EU-US Transatlantic Trade and Investment Partnership (TTIP)). While data and privacy protection are universally recognized as legitimate public policy objectives, at least in principle, views about what is necessary to achieve these objectives differ considerably. Accordingly, the EU carves out its data protection regime, including the data transfer restrictions, from external scrutiny in its trade agreements.[66]

The model inaugurated in TPP and subsequently used in USMCA and USJDTA also created a dedicated rule on a certain form of data localization that requires foreign businesses to use or locate computing facilities within a treaty party's territory as a condition for conducting business in that territory.[67] In contrast to the TPP, which allowed for the possibility to justify such measures in principle under the same conditions as applicable to cross-border data transfer restrictions, the USMCA and USJDTA do not preserve this option.[68] They also 'fix' the 'gap' that the TPP had

[64] GATS, Article XIV.
[65] USJDTA, Article 11.
[66] Horizontal provisions for cross-border data flows and for personal data protection in EU trade and investment agreements: https://perma.cc/GJ8J-AUJE. In the EU-UK Trade and Cooperation Agreement (TCA), the EU deviated from this template and conceded that it would provide for data transfer arrangements under 'conditions of general application'. See TCA, Article 202.2.
[67] TPP, Article 14.13.
[68] USMCA, Article 19.12; USJDTA, Article 12.

created for financial data at the insistence of US financial regulators and to the disappointment of US financial services providers. While still treating financial services data differently from other information, the USA, Mexico, Canada, and Japan, respectively, agreed to refrain from mandating the use of domestic computing facilities requirements for financial services, as long as their respective financial regulatory authorities have immediate, direct, complete, and ongoing access to information processed or stored on financial services computing facilities outside their territory.[69] In this way, the USMCA and USJDTA preserve both the right of financial service providers to locate data territorially where they see fit and the right of regulators to access the data transnationally.

In sum, established rules in the multilateral trading system only protect certain kinds of data from certain kinds of restrictions. In this sense, factual data mobility – that is, the ability of data holders to decide where data resides and where it moves – exceeds the legal protection of data mobility under WTO law. For this reason, the USA and like-minded countries have been advocating for more stringent rules to preserve transnational data mobility as other countries have sought to impose data transfer restrictions.[70] The design of these provisions, in particular their reliance on categories borrowed from international investment law conducive to regulatory arbitrage by way of strategic incorporation, means that countries that sign on to the US model effectively opt for an open digital economy favoring transnational data mobility vis-à-vis everyone. The EU, and other jurisdictions interested in a more differentiated regime, are hence prudent in refraining from such commitments.[71]

B *Regulation of Data Control*

IEL regulates control over data mainly through commitments under international IP law and international investment law. International IP law – which shifted into the trade regime with the WTO's agreement on 'trade-related aspects of intellectual property rights' (TRIPS) and has since become a staple of 'free trade' agreements – regulates control over data by requiring IP protection for certain categories of data. Recent US agreements have gone further by creating new rights to data exclusivity in their IP chapters and novel protections for algorithms in 'digital trade' chapters. Yet, the entrenchment of data control under international investment law might be even more far-reaching as it lends itself to protecting data as an asset (investment), which entitles data holders (investors) to certain guarantees enforceable against nation

[69] USMCA, Article 17.18; USJDTA, Article 13.

[70] The USA considered targeted data localization measures against the Chinese-owned company TikTok before ordering its parent company, ByteDance, to divest itself from its US operations. The national security exception included in all US trade agreements – including USDTA, Article 4 – provides some cover for such measures, but they are nevertheless in tension with longstanding US policy favoring global "free flow" of data.

[71] T Streinz, 'Data Governance in International Economic Law: Non-Territoriality of Data and Multi-Nationality of Corporations' (draft paper, available at https://ssrn.com/abstract=3831743).

https://doi.org/10.1017/9781108954006.010 Published online by Cambridge University Press

states by way of investor–state dispute settlement (ISDS). While ostensibly in favor of data mobility, IEL tends to entrench data control by protecting those who have data rather than those who need it or want it. The only exception are new commitments in recent agreements that encourage governments to make 'their' data available as 'open data'.[72] This encourages a shift from governmental control over data toward 'public' access, which is, in reality, often mediated by private actors such as data brokers or cloud providers.[73] No international agreement contemplates data sharing by private data holders, despite the regulatory trend toward compulsory data-sharing mechanisms in certain jurisdictions.

IEL's regulation of data control is especially salient as the question of legal ownership over data remains unsettled in domestic law.[74] The integration of international IP law into IEL has led to the gradual transformation of IP as a coordinative system of incentive governance into a commodity that can be 'traded' transnationally and an asset that enjoys investment protection.[75] While the reconceptualization of established IP rights as investments might upset the balance found under TRIPS,[76] the dynamic might be different for data where such a balance is yet to be found. Both common and civil law systems grapple with questions of whether and to what extent property rights in data should be recognized, newly established, or – where they exist – abolished. IEL may have a significant and potentially long-lasting influence on these debates. In this context, it is important to differentiate between legal rights of data ownership (property rights in data) and factual control over data. Data holders may exercise infrastructural control over data without commensurate property rights that a domestic court would recognize or enforce. Conversely, data transfer, storage, and processing infrastructures can be designed in ways that separate forms of legal or technological control over data. One example is cloud computing models in which the owner and operator of the physical and digital data infrastructure has no access to its consumer's data.[77] Another is 'safe sharing sites', which provide for differentiated access to data, while distinguishing between raw data and insights derived from them.[78] Neither of these contractual arrangements hinges on the recognition of property rights in data.

However, legal ownership claims over data can be critical when de facto control over data is being challenged. When governmental regulators require the disclosure of information or when data-sharing requirements between businesses are being

[72] USMCA, Article 19.18; USJDTA, Article 20; DEPA, Article 9.4; ASDEA, Article 27.

[73] See, for example, L Palk and K Muralidhar, 'A Free Ride: Data Brokers' Rent-Seeking Behavior and the Future of Data Inequality' (2018) 20 *Vanderbilt Journal of Entertainment & Technology Law* 779.

[74] T Scassa, 'Data Ownership' (2018) CIGI Papers No. 187 (surveying legal bases for data ownership).

[75] RC Dreyfuss and S Frankel, 'From Incentive to Commodity to Asset: How International Law Is Reconceptualizing Intellectual Property' (2015) 36 *Michigan Journal of International Law* 557.

[76] RC Dreyfuss and S Frankel, 'Reconceptualizing ISDS: When Is IP an Investment and How Much Can States Regulate It?' (2019) 21 *Vanderbilt Journal of Entertainment & Technology Law* 377.

[77] This is the data stewardship model as explained by P Schwartz, 'Legal Access to the Global Cloud' (2018) 118 *Columbia Law Review* 1681.

[78] LM Austin and D Lie, 'Safe Sharing Sites' (2018) 94 *New York University Law Review* 581.

instituted, data controllers will claim 'data ownership' to guard their economic interests in data exploitation. Such claims under domestic law can be shaped and entrenched by commitments under IEL.

The TRIPS agreement sets a baseline for IP protection for certain categories of data, but such protection is not comprehensive and remains contested. Copyright, for example, only covers expressions (such as images, texts, videos) as data.[79] Compilations of data can be protected if they constitute intellectual creations, but such protection does not extend to the data contained therein.[80] Trade secrets might be able to fill some of these gaps. Technological shifts toward cloud computing and ML make it easier to satisfy the three-pronged test that Article 39.1 TRIPS stipulates. First, the secrecy of data can be achieved, for example, by keeping the data internal and by only allowing differentiated access. Second, the commercial value derived from secrecy may flow from competitive advantages in machine learning applications attributable to superior datasets. And third, secrecy can be maintained by way of technological safeguards such as encryption.[81] While the extent to which trade secrecy under TRIPS protects against data disclosure requirements transnationally has not yet been tested in dispute settlement proceedings,[82] companies rely routinely on trade secrecy to fight transparency domestically.[83] In light of uncertainty about the level of protection of undisclosed test data provided by Article 39.3 TRIPS, the USA has been aggressively pushing for 'data exclusivity' provisions in recent agreements.[84] While so far confined to regulatory approval for agricultural chemical and pharmaceutical products – where data exclusivity creates de facto exclusivity for the relevant product – these demands might be a precursor for future contests around data exclusivity in other contexts. Novel provisions protecting against source code disclosure that go beyond the traditional copyright protection for software are another pointer in the same direction.[85]

Meanwhile, international investment law's bearing on data control has been largely overlooked, but this might just be the calm before the storm.[86] The broad

79 TRIPS, Article 9(2).

80 TRIPS, Article 10(2).

81 See JC Fromer, 'Machines as the New Oompa-Loompas: Trade Secrecy, the Cloud, Machine Learning, and Automation' (2019) 94 *New York University Law Review* 706 (discussing the equivalent criteria under US law).

82 But see request for consultation by the EU against China regarding certain measures on the transfer of technology, WT/DS549/1 (1 June 2018) (alleging that China does not ensure effective protection of undisclosed information contrary to Article 39.1 and 39.2 TRIPS).

83 DS Levine, 'The Impact of Trade Secrecy on Public Transparency', in RC Dreyfuss and KJ Strandburg (eds), *The Law and Theory of Trade Secrecy* (Cheltenham, Edward Elgar Publishing, 2010).

84 See, for example, TPP, Article 18.47 and Article 18.50, the latter of which was suspended under CPTPP.

85 See, for example, JUSDTA, Article 17.

86 See JE Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (New York, Oxford University Press, 2019), at 259–260 (predicting that ISDS disputes about states' interfering with cross-border flows of personal data will materialize).

'investment' definitions found in many agreements and the variety of approaches deployed by tribunals make it plausible that 'data' will soon be recognized as a protected asset under international investment law by at least some tribunals,[87] thereby granting property-type protection under international law where such protection under domestic law remains uncertain.[88] While the broad and relatively open-ended guarantee of fair and equitable treatment contained in many investment agreements can be leveraged against many forms of data regulation, the guarantees against indirect or even direct expropriation appear to be particularly apt to challenge the growing trend toward mandatory data sharing. To be sure, in the absence of ISDS jurisprudence, many open questions remain: does the recognition of data as an asset presuppose the recognition of IP-type rights in data (fostering convergence between international IP and investment law)?[89] Is the collection of data making a contribution to the host state economy, as required under the *Salini* test?[90] What kind of territorial nexus, if any, is required between a company's data-related activities and the host state to enjoy investment protection?[91] Answers to these question will only emerge over time. The development of ISDS jurisprudence on data control questions is likely to depend on what kind of cases are being brought against whom and on what basis. The failed attempt to challenge Australia's tobacco regulation may cause investors to tread more carefully when challenging the regulatory ambitions of developed countries (e.g., the EU's data strategy).[92] Developing countries with industrial data policies that challenge the Silicon Valley Consensus are likely targets for ISDS-backed counter pressure.

[87] The threshold question of what constitutes an 'investment' is far from settled; see, for example, JD Mortenson, 'The Meaning of "Investment": ICSID's Travaux and the Domain of International Investment Law' (2010) 51 *Harvard International Law Journal* 257 (urging tribunals to recognize any activity or asset that is plausibly economic in nature); S Pahis, 'Investment Misconceived: The Investment-Commerce Distinction in International Investment Law' (2020) 45 *Yale Journal of International Law* 69 (suggesting that ordinary commercial transactions can be subject to investment protection).

[88] In this regard, the dynamic is the inverse of the one identified by J Arato, 'The Private Law Critique of International Investment Law' (2019) 113 *American Journal of International Law* 1, at 10–12. Rather than displacing domestic private law, international investment law may grant property-like protections where it is not (yet) clear whether comparable protections are available under domestic law.

[89] See E Horváth and S Klinkmüller, 'The Concept of "Investment" in the Digital Economy: The Case of Social Media Companies' (2019) 20 *Journal of World Investment & Trade* 577, at 608 (asserting that de facto control over data is insufficient for 'investment' status).

[90] See, for example, D Tamada, 'Must Investments Contribute to the Development of the Host State? The *Salini* Test Scrutinised', in P Szwedo et al. (eds), *Law and Development: Balancing Principles and Values* (Singapore, Springer, 2018).

[91] See, for example, *Abaclat and others (formerly Giovanna a Beccara and others) v. Argentine Republic*, ICSID Case No. ARB/07/5, Decision on Jurisdiction and Admissibility (4 August 2011) (holding that for investments of a purely financial nature, the relevant criteria should be where and/or for the benefit of whom the funds are ultimately used).

[92] *Philip Morris Asia Limited v. Commonwealth of Australia* (PCA Case No. 2012–12).

IV ADAPTING INTERNATIONAL ECONOMIC LAW FOR THE ARTIFICIAL INTELLIGENCE ECONOMY

The picture that emerges is one in which new commitments toward data mobility under IEL enable those who have data to decide where they want to store, process, and transfer data, while international IP and investment law guard against governmentally mandated transparency about and/or re-distribution of control over data. Protections of mobility and control of capital are, of course, familiar ways in which IEL has facilitated global capitalism. Yet, data differs from other means of production and might necessitate changes to the global regulatory environment to generate societally beneficial outcomes. Developing countries appear to be in a particularly precarious position. Embracing the shift toward a data-driven economy is widely seen as the best path toward development.[93] Yet, charting this path while respecting local conditions and values such as human agency and self-determination is challenging because of the concentration of power over the relevant digital infrastructures and data that lends itself to new dependencies and carries the risk of data extractivism without adequate compensation.[94] For these reasons, contemporary IEL's tendency to apply policy prescriptions of the twentieth century to the emerging AI economy in the twenty-first century needs critical evaluation and, where necessary, reconfiguration. Future work will consider the following questions and tentative propositions.

First, how can governmental interests in local access to and/or regulatory control over data be reconciled with transnational business interests in cross-border data flows? While territorial data localization requirements are by no means the only or best way to ensure local access to data, it seems premature for governments to tie their hands when viable alternatives are not yet in place. In particular, countries that are interested in maintaining a differentiated approach to transnational data flows (or at least the possibility to institute such a regime eventually) may want to avoid the sweeping provisions that the CPTPP, USMCA, and JUSDTA have pioneered. Instead, imposing conditionalities under IEL directly on multi-national digital corporations – trading protections of free flow of data against commitments toward regulatory commands – might be a superior regulatory approach.[95]

Second, what are the implications of the fundamental differences between financial capital and data-as-capital for international investment law? As international investment law is undergoing critical re-evaluation and at least partial reform in both substance and procedure, its implications for an AI economy in

[93] UNCTAD, 'Value Creation and Capture: Implications for Developing Countries' (2019), https://perma.cc/2XDY-PVZ3; World Bank, Development Report (2020), https://perma.cc/88SN-8WJK.

[94] See H Farrell and AL Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion' (2019) 44 *International Security* 42; N Couldry and UlA Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford, CA, Stanford University Press, 2019).

[95] Streinz, note 71 above.

https://doi.org/10.1017/9781108954006.010 Published online by Cambridge University Press

which data is treated as a resource ought to be part of the agenda. Vague references to the 'right to regulate' may be insufficient to enable creative experimentation with digital economy policies without risk of 'regulatory chill'. As an ISDS moratorium for COVID-19-related measures is being considered, a comparable moratorium for certain digital economy policies should be on the table as well.

Third, is there a need to recalibrate the temporal mismatch between long-lasting obligations under IEL and the rapid pace of technological development? IEL's traditional commitment to providing 'certainty' for transnational business activity seems at odds with the rapid pace of innovation in the digital economy. The principle of technology neutrality may need to be cabined when new technologies transform the economy fundamentally.

And finally, how can IEL help to confront (rather than exacerbate) the pervasive data control asymmetries in the digital economy? A first step in this direction might lie in addressing the uncertainty about the value of data and data flows in a globalized digital economy. Existing proxies for the value of data flows (e.g., bandwidth expansion) and of data control (e.g., market capitalization) seem insufficient to inform policy-makers and treaty drafters. While the Organisation for Economic Co-operation and Development (OECD) and the WTO have gradually begun to address this challenge, their efforts so far have failed to consider proactive measures through which the data amassed by global platform companies could be leveraged to (re)assess the state of the global digital economy. As it turns out, data is a resource not just for the AI economy but also for the future development and reconfiguration of IEL.