INTERNATIONAL TRADE LAW MEETS DATA ETHICS: A BRAVE NEW WORLD

NEHA MISHRA*

* Lecturer, ANU College of Law, Australian National University. University of Singapore. Email: mishra.neha@gmail.com. I thank Neeraj RS and Svetlana Yakovleva for very helpful comments on an earlier draft of this article, and Shin-yi Peng, Thomas Streinz, and other participants of AIELN 2019 for their comments on a presentation on the use of public moral exceptions in GATS for Data Ethics-Related Measures. I also thank the editorial team at the *NYU Journal of International Law and Politics* for their helpful comments and diligent editing.

The unprecedented integration of digital technologies in the economic and social spheres has led to strong concerns regarding the ethical use of data collected by such technologies. In response to these concerns, several intergovernmental and multistakeholder bodies as well as individual governments have started devising data ethics compliance frameworks. These frameworks integrate certain core principles such as human rights protection, ethical design, algorithmic accountability, and data privacy and security. Governments are also imposing measures to achieve greater compliance with these core principles of data ethics, including banning certain, especially foreign, data-driven applications and services; restricting cross-border transfers and processing of data; and imposing varied corporate compliance requirements for offering data-driven technologies. However, some measures aimed at protecting and promoting data ethics (Data Ethics Measures) can have the consequence of restricting cross-border trade, especially in digital and data-driven services and technologies.

Against this background, this article assesses whether Data Ethics Measures are consistent with international trade law, looking at the treaties of the World Trade Organization (WTO) and several Preferential Trade Agreements (PTAs). It argues that certain Data Ethics Measures may be inconsistent with obligations contained in international trade agreements, including obligations on non-discrimination, market access, domestic regulation, and intellectual property protection. However, international trade law does not per se inhibit Data Ethics Measures. For instance, exceptions contained in international trade agreements can be interpreted to allow measures that support a human rights-centric approach to data governance. Further, rules on trade secret protection may be meaningfully interpreted and applied to balance commercial and critical public interests such as facilitating algorithmic accountability and ethical design in data-driven technologies. Finally, provisions on domestic regulation can potentially ensure that Data Ethics Measures are implemented in a fair and objective manner, and that technical standards and licensing requirements for data-driven digital services are transparent, objective, and not unnecessarily burdensome. However, given the legal, technological, and political uncertainties at hand, governments are unlikely to consider trade rules a foolproof mechanism to preserve their policy discretion to regulate data-driven technologies for ethical reasons.

Accordingly, this article explores new avenues in international trade law to accommodate data ethics norms. It argues that international trade institutions can better co-opt data ethics frameworks by facilitating enhanced high-level cooperation among countries on cross-border data transfer mechanisms as well as digital development and inclusion. For example, trade bodies, including the WTO, can proactively engage with other international, regional, and transnational or multistakeholder bodies involved in norm development in data ethics, especially on privacy protection, digital inclusion, and the ethical use of data in designing and applying digital technologies. Further, where appropriate and necessary,

international trade rules must acknowledge the prevailing global best practices in data-driven sectors, especially the role of multistakeholder and private technical standards and protocols in promoting ethical and robust data-driven technologies. One possible means of doing so is to adopt new rules at the WTO and through PTAs—especially for trade in services and electronic commerce—that recognize relevant technical standards, protocols and best practices developed by multistakeholder internet institutions and representative private sector bodies.

I. INTRODUCTION

Data-driven technologies bring both opportunities and challenges. The widespread adoption of Big Data Analytics and Artificial Intelligence (AI)/Machine Learning (ML) has transformed the global economy by creating new economic, social, and technological opportunities, increasing market efficiencies, and reducing trade costs.[1] Experts predict that these technologies can foster meaningful innovation and enable human advancement in different fields of life,[2] such as health-

1. WORLD TRADE ORG., WORLD TRADE REPORT 2018 4, 8, 16 (2018), https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf [https://perma.cc/W394-ZU6L].

2. *See Data-Driven Innovation for Growth and Well-Being*, OECD, https://www.oecd.org/sti/ieconomy/data-driven-innovation.htm [https://perma.cc/HN5K-BXZS] (last visited Nov. 10, 2020) (noting the impact of "data-driven innovation" on the economy, energy sector, health outcomes, and governance); FILIPPO A. RASO ET AL., ARTIFICIAL INTELLIGENCE & HUMAN RIGHTS 3 (Berkman Klein Ctr. for Internet & Soc'y, Research Publication No. 2018-6, 2018) (assessing AI's human rights impacts on criminal justice, finance, healthcare, content moderation, human resources, and education). Several initiatives are underway for assessing the social benefits of data-driven technologies, especially AI, by organizations such as the UN, *Global Partnership for Sustainable Development Data*, SUSTAINABLE DEV. GOALS, https://sustainabledevelopment.un.org/partnership/?p=9691 [https://perma.cc/BS6R-NRGB] (last visited Nov. 10, 2020), *Big Data and Artificial Intelligence*, GLOBAL PULSE, https://www.unglobalpulse.org/ [https://perma.cc/6WE7-Z77L] (last visited Nov. 10, 2020); the World Economic Forum, *Shaping the Future of Technology Governance: Artificial Intelligence and Machine Learning*, WORLD ECON. F., https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-artificial-intelligence-and-machine-learning [https://perma.cc/NY6U-7MMT] (last visited Nov. 10, 2020); and Data-Pop Alliance and International Telecommunications Union. *About Us*, AI FOR GLOBAL GOOD, https://aiforgood.itu.int/about-us/ [https://perma.cc/75W3-ZYUW] (last visited Nov. 10, 2020).

care,[3] disaster management,[4] and delivery of public services.[5] However, data-driven technologies are also increasingly misused to propagate disinformation campaigns,[6] prejudice online privacy and security,[7] and further algorithmic discrimination.[8] A recent illustration of this dichotomy is the contact tracing applications used by governments to monitor and control the Covid-19 pandemic.[9] In response to the various con-

---

3. Adam Steventon, *Better Health Through Analytics and Data-Driven Technology*, HEALTH FOUND. (Oct. 29, 2019), https://www.health.org.uk/news-and-comment/blogs/better-health-through-analytics-and-data-driven-tech nology [https://perma.cc/9KGM-29D8]; Mikael Hagstroem, *Big Data Analytics for Inclusive Growth: How Technology Can Help Elevate the Human Condition*, *in* WORLD ECON. F., THE GLOBAL INFORMATION TECHNOLOGY REPORT 2015 79, 82 (2015), http://www3.weforum.org/docs/WEF_GITR_Chapter1.8_2015.pdf [https://perma.cc/W6WA-AVYX]; Hannah Kuchler, *Google AI System Beats Doctors in Detection Tests for Breast Cancer*, FIN. TIMES (Jan. 1, 2020), https://www.ft.com/content/3b64fa26-28e9-11ea-9a4f-963f0ec7e134 [https://perma.cc/7BJ6-LP9P].

4. Kylie Wiggers, *Google's AI Predicts Local Precipitation Patterns 'Instantaneously'*, VENTURE BEATS (Jan. 13, 2020), https://venturebeat.com/2020/01/13/googles-ai-predicts-local-precipitation-patterns-instantaneously/ [https://perma.cc/7YXU-ANWK].

5. Lok Siying, *The Impetus of Big Data for Public Service Delivery*, J. INT'L & PUB. AFF. (Apr. 30, 2018), https://www.jipasg.org/posts/2019/4/30/the-impetus-of-big-data-for-public-service-delivery [https://perma.cc/V322-NPY2].

6. Samuel Woolley, *We're Fighting Fake News AI Bots by Using More AI. That's a Mistake*, MIT TECH. REV. (Jan. 8, 2020), https://www.technologyreview.com/2020/01/08/130983/were-fighting-fake-news-ai-bots-by-using-more-ai-thats-a-mistake/ [https://perma.cc/75EG-HZKB].

7. DAVID LESLIE, ALAN TURING INST., UNDERSTANDING ARTIFICIAL INTELLIGENCE ETHICS AND SAFETY 5 (2019), https://www.turing.ac.uk/sites/default/files/2019-06/understanding_artificial_intelligence_ethics_and_safety.pdf [https://perma.cc/96KG-VB77].

8. *See, e.g.*, Joi Ito , *Supposedly 'Fair' Algorithms Can Perpetuate Discrimination*, WIRED (May 2, 2019), https://www.wired.com/story/ideas-joi-ito-insurance-algorithms/ [https://perma.cc/98GJ-7ZFN] (demonstrating the potential for discrimination in the insurance sector due to the use of AI); Karen Hao, *Facebook's Ad-Serving Algorithm Discriminates by Gender and Race*, MIT TECH. REV. (Apr. 5, 2019), https://www.technologyreview.com/2019/04/05/1175/facebook-algorithm-discriminates-ai-bias/ [https://perma.cc/F98Z-6DC5] (arguing that advertising algorithms are inherently discriminatory).

9. Urs Gasser et al., Digital Tools Against Covid-19: Framing the Ethical Challenges and How to Address Them (Apr. 21, 2020) (unpublished manuscript) (on file with arXiv.org), https://arxiv.org/ftp/arxiv/papers/2004/2004.10236.pdf [https://perma.cc/34QU-ATLT] (highlighting the ethical concerns around digital tracing technologies).

cerns about data-driven technologies and services, governments are developing new laws and policies, including checks on the design of data-driven technologies and restrictions on the collection, processing, and cross-border transfer and sharing of data.[10]

Promoting data-driven innovation and economic growth while safeguarding governments' ability to regulate the digital sector is expectedly challenging. This article delves into a specific dimension of this challenge, focusing on the restrictions imposed by governments based on ethical or moral concerns pertaining to the designing of data-driven services and the gathering, processing, use, and sharing of digital data. Broadly, the article refers to all moral or ethical concerns regarding data as "data ethics."[11] This formulation of data ethics aligns with the definition put forth by Floridi, who describes data ethics as a "moral compass" to determine "good" digital regulation and governance:

> [Data ethics is a] branch of ethics that studies and evaluates moral problems relating to data and information (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including AI, artificial agents, machine learning and robots) and corresponding practices and infrastructures (including responsible innovation, programming, hacking, professional codes and standards), in order to formulate and support morally good solutions (e.g. good conduct or good values).[12]

With the rapid development of data-driven technologies, governments and other concerned stakeholders (including international organizations, private companies, academics, and civil society organizations) are devising multiple frameworks on data ethics. In fact, certain experts believe that numerous efforts to devise data ethics frameworks will eventually lead to

---

10. *See* discussion *infra* Section II.

11. *See generally Data Ethics Canvas*, OPEN DATA INST. (2019), https://theodi.org/article/data-ethics-canvas/ [https://perma.cc/V2LU-8JN6] (providing guides to ethical uses of data).

12. Luciano Floridi, *Soft Ethics and Governance of the Digital*, 31 PHILOS. & TECH. 1, 3–4 (2018).

"ethics shopping"[13] or "ethics washing."[14] While this article does not exhaustively discuss or debate these frameworks,[15] it does highlight the core principles of data ethics and how the laws, regulations, policies, and standards developed by governments enhance compliance with these core Data Ethics Measures.

Data Ethics Measures can potentially restrict cross-border trade in digital and data-driven services and technologies and, thus, have an adverse economic impact. Some examples of measures discussed in this article are bans on foreign data-driven services and applications; restrictions on the transfer and processing of data; requirements on companies to disclose their algorithms[16] and source code[17] to regulators for verification or approval in order to sell their digital technologies in the domestic market; restrictions on the use of foreign or international technical standards; and imposition of domestic technical standards or licensing requirements for data-driven services.

To date, scholars and policy experts have paid little attention to the interface of international trade and data ethics, despite the significant role of data-driven technologies in trade.

---

13. Luciano Floridi, *Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical*, 32 PHILOS. & TECH. 185, 186–87 (2019).

14. Karen Hao, *In 2020, Let's Stop AI Ethics-Washing and Actually Do Something*, MIT TECH. REV. (Dec. 27, 2019), https://www.technologyreview.com/2019/12/27/57/ai-ethics-washing-time-to-act/ [https://perma.cc/XEG4-S6G9].

15. For an interdisciplinary analysis of AI ethics, see JESSICA FJELD ET AL., PRINCIPLED ARTIFICIAL INTELLIGENCE: MAPPING CONSENSUS IN ETHICAL AND RIGHTS-BASED APPROACHES TO PRINCIPLES FOR AI (2020), https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf?sequence=1&isAllowed=Y[https://perma.cc/J6JW-FWQG]. *See also* Anna Jobin et al., *The Global Landscape of AI Ethics Guidelines* 1 NATURE MACH. INTEL. 389 (2019) (analyzing AI ethics frameworks from across the world, including converging principles).

16. In computer science, an algorithm means the mathematical formula or series of logical steps used to solve a problem. Philip A. Olamigoke, *Definition — Computer Science, Algorithm, Programming and Computation*, MEDIUM (Nov. 28, 2019), https://medium.com/@olamigokayphils/definition-computer-science-algorithm-programming-and-computation-731db5b127cf [https://perma.cc/6CSH-25PG].

17. Source code means instructions written in any computer programming language for the computer to execute. *Source Code*, TECHOPEDIA (Jan. 4, 2017), https://www.techopedia.com/definition/547/source-code.

For instance, the 2018 World Trade Report, which focused on AI technologies, mentioned the word "ethics" only once.[18] However, as ethical practices pertaining to data-driven technologies become important policy considerations for governments, questions are likely to arise if adopted Data Ethics Measures conflict with countries' obligations in international trade agreements.[19] Therefore, whether international trade agreements restrict the ability of governments to protect or promote data ethics policy objectives is a relevant issue, one this article addresses with reference to the law contained in WTO treaties and relevant provisions in certain recent PTAs.[20] As the article largely focuses on data-driven services, it covers trade in services by looking at the General Agreement on Trade in Services (GATS)[21] and electronic commerce chapters in PTAs. This article also references relevant provisions in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement).[22]

Section II highlights the fundamental principles of data ethics and how governments are influenced by these principles in devising Data Ethics Measures. Section III explains that while Data Ethics Measures are important in building digital trust, they may sometimes have a trade-restrictive impact, leading to economic inefficiencies in data-driven technologies. Section IV examines how Data Ethics Measures can implicate rules in international trade law, focusing on obligations on non-discrimination and market access. The section also explores domestic regulation and technical standard-setting for digital services, the role of exceptions in preserving policy space for individual countries to regulate data-driven services and technologies for ethical reasons, and rules on trade secret

18. WORLD TRADE ORG., *supra* note 1, at 32. R

19. *See* discussion *infra* Section IV.

20. PTA is an omnibus term referring to bilateral, regional and megaregional trade agreements, excluding WTO treaties. WORLD TRADE ORG., WORLD TRADE REPORT 2011 44 (2011), https://www.wto.org/english/res_e/booksp_e/anrep_e/wtr11-2a_e.pdf [https://perma.cc/J366-9LHP].

21. General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183 (1994) [hereinafter GATS].

22. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 (1994) [hereinafter TRIPS Agreement].

under the TRIPS Agreement and other PTAs in the context of algorithmic accountability. Section V outlines the policy challenges arising due to the growing interface of international trade law and data ethics. This section then addresses various means of establishing a synergistic and meaningful role for international trade agreements in promoting higher standards of data ethics in the digital sector.

The ethical dimension of data regulation is at least as important as economic or commercial dimensions. International trade law can play an important role in curbing protectionist behavior, such as prohibiting Data Ethics Measures used as a disguise for illegally protecting domestic companies. Rules on trade secrets and source code can also be applied meaningfully to balance commercial intellectual property (IP) protection interests with public interests on the ethical use of data. Finally, certain fundamental aspects of data ethics, such as compliance with human rights, privacy protection, ethical design, and algorithmic accountability, can be read into the exceptions in international trade agreements. However, rapid technological changes and the differences among countries' data-driven technology regulations lead to uncertainties in applying international trade law to Data Ethics Measures. Therefore, this article argues that the WTO and regional trade institutions, must better adapt and respond to the policy developments and norm evolution in data governance and play a greater role in facilitating international regulatory cooperation on transborder data flows and related issues. To do so, this article proposes new trade rules that acknowledge relevant multistakeholder and private standards and best practices in data-driven sectors, including AI/ML.

II. Implementing Principles of Data Ethics

Several government initiatives and international institutions have deliberated on the high-level principles of data ethics to set rules and standards promoting the ethical use of data-driven technologies, especially AI/ML.[23] This section pro-

23. *See, e.g.*, Select Committee on Communications, Regulating in a Digital World, 2017-19, HL 299, ¶ 98 (UK) (setting out various principles for modern digital regulation, including ethical technology); A Comprehensive European Industrial Policy on Artificial Intelligence and Robotics, Eur. Parl. Doc. P8_TA(2019)0081 (2019) (recommending that the European

vides an overview of the core elements of data ethics, including respect for human rights, enforcing ethical design, promoting algorithmic accountability, and protecting data privacy and security. These principles apply to the entire life cycle of data-driven technologies and datasets, from design to collection of data, sharing it with third parties, and reusing it to generate new services and products.[24] This section also discusses examples of various Data Ethics Measures intended to achieve these principles in practice.

Data ethics principles are usually not directly binding, but they can complement international legal frameworks.[25] For example, data ethics principles aimed at eliminating gender and racial discrimination further basic human rights principles enshrined in international treaties. Some experts classify these emerging data principles as soft law norms.[26] Finally, data ethics principles inform some binding domestic laws and regula-

---

Union consider new rules on AI technologies that comply with fundamental European values); *Ethics Guidelines for Trustworthy AI* (Apr. 8, 2019), https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai [https://perma.cc/KRB6-XDDL] (setting guidelines for trustworthy AI in the European Union such as respecting laws and regulations, respecting ethical values, and technical robustness); Org. for Econ. Coop. & Dev. [OECD], *Recommendation of the Council on Artificial Intelligence* (May 22, 2019), https://www.fsmb.org/siteassets/artificial-intelligence/pdfs/oecd-recommendation-on-ai-en.pdf [https://perma.cc/7GKF-FRPC] (recommending value-based principles for AI technologies); Nat'l Inst. Standards & Tech., U.S. Dep't of Com., US Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools (2019), https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf [https://perma.cc/6CBR-A3SH] (focusing on technical standards in AI to promote innovation, public trust, and public confidence in systems that use AI technologies).

24. *See* OECD, Scoping the OECD AI Principles 13 (2019) (focusing on the specific context of AI-driven services). *See generally* World Econ. F., Responsible Use of Technology (2019), http://www3.weforum.org/docs/WEF_Responsible_Use_of_Technology.pdf [https://perma.cc/QM6V-28AW] (setting out a framework for the responsible and ethical use of digital technologies through multistakeholder collaborations between governments and technology businesses from creation and marketing till end use).

25. A useful approach is viewing data and AI governance as a layered system consisting of the socio-legal layer containing laws and regulations, the ethical layer containing principles, and the technical layer consisting of the algorithms and the data. Urs Gasser & Virgilio A.F. Almeida, *A Layered Model for AI Governance*, 21 IEEE Internet Computing 58, 60–61 (2017).

26. Jobin et al, *supra* note 15, at 389.

tions. As data-driven technologies become closely integrated with human lives, these principles are arguably inching closer towards international recognition as emerging transnational principles.[27] However, as data ethics principles are embedded in specific socio-technological contexts, they are likely to continue evolving in "open-ended spaces of negotiation."[28]

A. *Protection of Human Rights*

The most fundamental principle in data ethics is the protection of human rights.[29] There is a growing consensus that the use, processing, and sharing of data in different digital technologies must comply with the basic principles of human rights.[30] The key essence of a human rights-centric approach is protecting the dignity and rights of individuals, thus requiring governments to respect, protect, and fulfill human rights.[31] In

27. *See, e.g.*, FJELD ET AL., *supra* note 15, at 5 (arguing that the commonality of AI principles across different instruments suggests that they represent a "normative core" in data governance). R

28. Gry Hasselbach, *Making Sense of Data Ethics: The Powers Behind the Data Ethics Debate in European Policymaking*, 8 INTERNET POL'Y REV., June 13, 2019, at 1.

29. *See* Corriane Cath & Luciano Floridi, *The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights*, 23 SCI. & ENG'G ETHICS 449, 451–55 (2016) (explaining the trend of embedding human rights in Internet governance principles); IEEE, ETHICALLY ALIGNED DESIGN 10 (1st ed. 2019), https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf [https://perma.cc/8F2D-RRKA] (indicating human rights is one of the three pillars of the Ethically Aligned Design conceptual framework); WORLD ECON. F., *supra* note 24, at 8 ("Human rights reinforce ethics, and ethics reinforce human rights—indeed, human-rights-based approaches draw upon many traditions of ethical thinking and represent universal principles that have been broadly endorsed across borders and cultures."). R R

30. Hum. Rts. Council, Progress Rep. of the U.N. High Comm'r for Hum. Rts. on Legal Options and Practical Measures to Improve Access to Remedy for Victims of Business-Related Human Rights Abuses, U.N. Doc. A/HRC/29/39, at 3 (May 7, 2015). *See also* INVEN_T, MONTREAL DECLARATION FOR RESPONSIBLE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE 7 (2018), https://www.montrealdeclaration-responsibleai.com/the-declaration [https://perma.cc/M7K3-TQ93].

31. *See generally* Comm. on Econ., Soc. and Cultural Rts., General Comment No. 24 (2017) on State Obligations Under the International Covenant on Economic, Social and Cultural Rights in the Context of Business Activities, U.N. Doc E/C.12/GC/24 (August 10, 2017) (requiring all businesses to respect human rights).

adopting a human rights-centric approach to data regulation, governments must address whether data-driven applications such as AI/ML are compatible with human rights. This entails various responsibilities, such as protecting individuals from and redressing harm arising from data-driven technologies.[32] A human rights-centric approach also entails protecting the privacy of individuals.[33]

Data-driven technologies can breach human rights in various ways, especially when employing automated algorithms. For instance, datasets used to train algorithms for automated processing based on prior data (also called training data) can result in biased outcomes in decision-making. For example, due to historical exclusion of women or minorities for jobs or loans, training data may program algorithms to continue to exclude such groups.[34] This discriminatory decision-making may be unconstitutional in several jurisdictions and is also inconsistent with the principles of international human rights law.[35] Even if programmers try to improve datasets by gathering more robust data, certain inherently sensitive proxy variables such as education or zip code cannot be completely avoided.[36] Thus, some experts have emphasized that the manner in which data scientists build datasets is an extremely important aspect of human rights accountability in data governance.[37]

Additionally, unintended technological or systemic errors might arise as companies use the same generic algorithms in

32. Hasselbach, *supra* note 28, at 11. **R**

33. *E.g.*, U.N. High-Level Comm. on Mgmt., Personal Data Protection and Privacy Principles (Oct. 11, 2018) https://unsceb.org/sites/default/files/imported_files/UN-Principles-on-Personal-Data-Protection-Privacy-2018_0.pdf [https://perma.cc/VSD5-4MU8]. *See infra* Section II(D).

34. FJELD ET AL., *supra* note 15, at 49; Joshua A. Kroll et al., *Accountable Algorithms*, 165 U. PA. L. REV. 633, 681 (2017); Karen Hao, *The Problems AI Has Today Go Back Centuries*, MIT TECH. REV. (Jul. 31, 2020), https://www.technologyreview.com/2020/07/31/1005824/decolonial-ai-for-everyone/ [https://perma.cc/Q2M3-DX3Y].

35. U.N., *Equality and Non-Discrimination*, https://www.un.org/ruleoflaw/thematic-areas/human-rights/equality-and-non-discrimination/ [https://perma.cc/QUP4-KS2F] (last visited Nov. 10, 2020).

36. Kroll et al., *supra* note 34, at 685. **R**

37. David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 663–64 (2017).

contexts as varied as processing a credit card application to providing choices for entertainment.[38] Further, internet platforms increasingly employ algorithms for filtering or screening content, thus potentially affecting individuals' right to freedom of expression and access to information. Such errors or biases may be reduced by increasing human intervention to ensure compliance with human rights.[39]

The international community has recognized the importance of aligning data regulations with international human rights. Several governments, such as Australia and Singapore, have recognized the centrality of human rights-centric approach in promoting an ethical data governance framework.[40] Moreover, the United Nations has explicitly acknowledged the importance of international human rights law as a fundamental guideline in the framing of data ethics principles, proposing guidelines for greater digital inclusion and participation, transparency, privacy, and accountability.[41] The Organization for Economic Cooperation and Development (OECD) has recommended that data be used, processed, and shared to promote human rights-centric growth, thus promoting economic and social opportunities for individuals and reducing discrimination against minorities.[42] The Internet Universality ROAM Principles developed by the United Nations Educational, Scientific and Cultural Organization (UNESCO), focuses on the importance of promoting AI technologies that align with

38. Brent Daniel Mittelstadt et al., *The Ethics of Algorithms: Mapping the Debate*, BIG DATA & SOC'Y, July-Dec. 2016, at 1, 7–8 (2016).

39. The extent of human intervention in the functioning of specific algorithms can vary. For a useful classification, *see* Michael Latzer & Naomi Festic, *A Guideline for Understanding and Measuring Algorithmic Governance in Everyday Life*, INTERNET POL'Y REV., June 30, 2019, at 1, 4–5.

40. *AI Ethics Principles*, AUSTL. GOV'T DEP'T INDUS., SCI., ENERGY & RES., https://www.industry.gov.au/data-and-publications/building-australias-artificial-intelligence-capability/ai-ethics-framework/ai-ethics-principles [https://perma.cc/N2GT-2PPE] (last visited Nov. 10, 2020); PERSONAL DATA PROTECTION COMMISSION SINGAPORE, MODEL ARTIFICIAL INTELLIGENCE GOVERNANCE FRAMEWORK 64–66 (2d ed. 2020).

41. *See* U.N. DEV. GROUP, DATA PRIVACY, ETHICS AND PROTECTION: GUIDANCE NOTE ON BIG DATA FOR ACHIEVEMENT OF THE 2030 AGENDA (2017) (providing guidance on "data privacy, data protection and data ethics" and serving as a "risk management tool taking into account fundamental human rights.")

42. OECD, *supra* note 23. R

human rights and improve digital access for individuals, thus reinforcing the right to development and digital inclusion.[43]

The internet policy community and the civil society have also raised concerns regarding the potential misuse of data-driven technologies, particularly in the context of AI. For example, in 2019, the Internet Society, a non-profit organization working on various policy issues surrounding internet and data governance,[44] issued a policy brief highlighting the importance of respect for individual internet users.[45] The brief called for responsible data handling by governments, strengthening domestic laws to protect internet users, and increasing digital education, especially of minority communities.[46] Some civil society groups, such as Access Now, have recommended mandatory human rights impact assessment for AI/ML technologies.[47]

One of the fundamental problems with the implementation of a human rights-centric approach in data governance is the variations in formulation and implementation of broad human rights principles across countries, especially in the online context. Regulatory diversity often means that governments do not uniformly implement Data Ethics Measures and may even have different benchmarks for assessing human rights breaches. Thus, in certain countries, governments themselves might use algorithms to discriminate against minorities or persecute dissidents, violating international human rights standards.[48] However, several countries have recently collabo-

---

43. U.N. Educ., Sci. & Cultural Org. [UNESCO], Steering AI and Advanced ICTs for Knowledge Societies (2019), https://en.unesco.org/system/files/unesco-steering_ai_for_knowledge_societies.pdf [https://perma.cc/GPX5-TEPY].

44. ISOC, *About Internet Society*, https://www.internetsociety.org/about-internet-society/ [https://perma.cc/NE38-6WHY?type=image] (last visited Aug. 31, 2020).

45. ISOC, POLICY BRIEF: PRINCIPLES FOR RESPONSIBLE DATA HANDLING 9 (2019), https://www.internetsociety.org/wp-content/uploads/2019/06/Responsible-Data-Handling-Policy-Brief-EN.pdf [https://perma.cc/NR8Z-3M4U].

46. *Id.*

47. *See* FJELD ET AL., *supra* note 15, at 30 (discussing the Access Now report).

48. *See, e.g.*, Darren Byler, *China's Hi-Tech War on its Muslim Minority*, GUARDIAN (Apr. 11, 2019), https://www.theguardian.com/news/2019/apr/11/china-hi-tech-war-on-muslim-minority-xinjiang-uighurs-surveillance-face-

rated with the OECD to establish a global, multistakeholder partnership to "support the responsible and human-centric development and use of AI in a manner consistent with human rights, fundamental freedoms, and . . . shared democratic values."[49] Therefore, despite regulatory differences, various governments are making efforts to achieve greater normative consensus in data ethics at an international level, especially for AI/ML technologies.

Another critical issue in enforcing a human-rights centric approach is holding private actors accountable for their algorithms or software that discriminates against individuals. As per the Ruggie Principles, although states are primarily responsible for safeguarding human rights, companies must also take a more active role in ensuring that their own operations do not undermine human rights.[50] Applying these principles to the digital context, technology companies have a responsibility to ensure that their designs and algorithms do not undermine individual human rights. While some technology companies have publicly acknowledged the importance of core human values in AI/ML,[51] the extent of their compliance with human rights remains debatable.[52]

---

recognition [https://perma.cc/GF78-QWLD] (discussing the use of data-driven technologies to discriminate against Uighur Muslims in China).

49. The countries involved include those of the European Union, Canada, the United States, the United Kingdom, India, Mexico, Japan, Australia, Singapore, New Zealand, and South Korea. *Joint Statement from Founding Members of the Global Partnership on Artificial Intelligence*, GOV.UK (June 15, 2020) https://www.gov.uk/government/publications/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence [https://perma.cc/SQD4-K9NZ].

50. *See generally* John Ruggie (Special Representative of the Secretary General), *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011) (setting out the framework for corporate responsibility to respect human rights, including not infringing on the rights of individuals and mitigating or remedying adverse human rights impacts of business activities).

51. Sundar Pichai, *Why Google Thinks We Need to Regulate AI*, FIN. TIMES (Jan. 20, 2020), https://www.ft.com/content/3467659a-386d-11ea-ac3c-f68c10993b04 [https://perma.cc/4WQ3-WJMU]; *Microsoft AI Principles*, MICROSOFT, https://www.microsoft.com/en-us/ai/responsible-ai?activetab=pivot1%3aprimaryr6 [https://perma.cc/J2VC-LM78] (last visited Nov. 10, 2020).

52. *See, e.g.*, U.N. Secretary-General, *Report of the Special Rapporteur on Extreme Poverty and Human Rights*, ¶ 72, U.N. Doc A/74/493 (Oct. 11, 2019)

B. *Ethical Design*

The principle of ethical design directly flows from a human rights-centric approach to data governance. It essentially means that technical designs and standards underlying data-driven technologies must comply with basic human rights. Regulators may implement ethical design by enforcing rules requiring digital service suppliers to adopt and incorporate technologies and corporate policies that ensure individuals' privacy and protect their data from unauthorized intrusions. This approach is premised on the understanding that technological solutions to privacy or security issues are sustainable and more pragmatic to implement.[53] The principle of ethical design promotes a "responsibility-by-design approach"[54] or "technological due process,"[55] meaning designers are required to verify that data-driven technologies function as expected.[56] Ethical design can also facilitate more meaningful human control over certain aspects of data-driven technologies,[57] making it easier for engineers to explain technical designs.[58]

As evidenced by the increasing influence of ethics in engineering choices and technical standards, ethical design is emerging as an industry best practice.[59] Engineers in various standard-setting institutions have attempted to develop standards compliant with human rights. One such example is the Institute of Electronics and Electrical Engineers (IEEE), which has developed technical standards for AI compliant with ethi-

---

(arguing that digital technology companies operate in "an almost human rights-free zone," which has dangerous repercussions for a digital welfare state).

53. See INFO. COMM'N OFF., BIG DATA, ARTIFICIAL INTELLIGENCE, MACHINE LEARNING AND DATA PROTECTION 72–73 (2017) (UK) (describing the benefits of privacy by design measures).

54. Cath & Floridi, *supra* note 29, at 451. R

55. Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law* 31 HARV. J.L. & TECH. 1, 8 (2017) (citing Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008)).

56. Kroll et al., *supra* note 34, at 637. R

57. *Cf.* FJELD ET AL., *supra* note 15, at 53 (explaining the globally recognized need for human control and how it promotes human values).

58. *Cf.* SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE, AI IN THE UK: READY, WILLING & ABLE?, 2017–19, HL 100, at 27 (Apr. 16, 2018) (discussing the importance of public understanding of AI and its implications).

59. FJELD ET AL., *supra* note 15, at 25.

cal design.[60] The Internet Engineering Task Force (IETF)[61] also plays an instrumental role in incorporating ethical principles into designs for the technical protocols of the internet, particularly protecting users' privacy rights.[62]

Expectedly, implementing ethical design entails challenges. One such challenge is deciding who should determine whether a technical design complies with the principles of data ethics and against which benchmark.[63] For example, although the General Data Protection Regulation (GDPR) of the European Union contains provisions requiring privacy-by-design, there is no definitive guidance on determining design compliance.[64] Similarly, the E.U. Cybersecurity Act promotes security-by-design and privacy-by-design.[65] In the absence of any clear domestic or universal international standards, determining compliance with such requirements is likely to involve

60. IEEE, *supra* note 29. R

61. The IETF consists of a "large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet." *About the IETF*, IETF, https://www.ietf.org/about/ [https://perma.cc/Q4MC-S2XG] (last visited Nov. 10, 2020).

62. Stephen Farrell & Hannes Tschofenig, *Pervasive Monitoring is an Attack*, IETF (May 2014) https://tools.ietf.org/html/rfc7258. For a more critical approach on whether IETF incorporates human rights, see Cath & Floridi, *supra* note 29, 449–68 (recommending a responsibility-by-design approach to address the deficiencies in the system). R

63. *See generally* Cedric Ryngaert and Mistale Taylor, *The GDPR as Global Data Protection Regulation*, 114 AJIL UNBOUND 5, 5–9 (2020) (discussing the issues of jurisdiction and extraterritoriality under GDPR).

64. Commission Regulation 2016/679 of Apr. 27, 2016, Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 25, 2016 O.J. (L 119) 48 [hereinafter GDPR]. While Article 25 of the GDPR sets out examples of design measures such as pseudonymization and data minimization, it does not further delineate the "necessary safeguards" or how companies can implement them in an "effective manner." *Id.*

65. Regulation (EU) 2019/881 of Apr. 17, 2019, Regulation on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), ¶ 41, O.J. (L 151) 21 [hereinafter Cybersecurity Act].

some degree of guesswork, thereby impacting technological and legal certainty.[66]

Adapting engineering solutions to comply with legal or policy requirements can present further challenges. For example, various practical difficulties exist in implementing a mathematical model of differential privacy (a popular mathematical model allowing companies to share aggregated data without compromising personally identifiable information).[67] For instance, engineers are often unsure about what exactly constitutes personally identifiable information.[68] Indeed, the concept of personally identifiable information is defined differently and ambiguously across jurisdictions, often left to subjective interpretation. This is directly opposite to the traditional precise computer science specifications upon which designers rely to design robust and ethically compliant technologies.[69] In order to address this gap between engineering and technology law and policy, it will be critical to develop a two-way dialogue where designers and regulators can discuss specific legal ambiguities and their underlying policy rationales.

C. *Algorithmic Accountability*

The basis of algorithmic accountability is that data-driven technologies, their services, or technology suppliers should be able to explain how their algorithms and technical designs use and process data to generate certain results, and how they can be modified to comply with laws and regulations.[70] This kind of transparency and technical clarity can help check instances of unfair or discriminatory outcomes, thus providing redress to the affected individuals[71] and allowing for modification of

66. Christopher Kuner et al., *The Language of Data Privacy Law (and How it Differs from Reality)*, 6 INT'L DATA PRIV. L. 259, 259 (2016).

67. Kobbi Nissim et al., *Bridging the Gap Between Computer Science and Legal Approaches to Privacy*, 31 HARV. J.L. & TECH. 687, 692 (2018).

68. *Id.*

69. Kroll et al., *supra* note 34, at 695. **R**

70. Letter from Daniel Castro, Director, Ctr. for Data Innovation, to Ellen Connelly, Off. Pol'y Plan., Fed. Trade Comm'n 26–27, 30 (Feb. 15, 2019), (on file with the Ctr. for Data Innovation), http://www2.datainnovation.org/2019-ftc-competition-consumer-protection.pdf [https://perma.cc/89EY-GDBT].

71. What constitutes adequate redress in such cases is a related question.

malfunctioning software and other digital services.[72] As the use of AI becomes increasingly common, the principle of algorithmic accountability plays a significant role in addressing "blackbox malfunctioning," which occurs when the lack of transparency regarding the functioning of AI algorithms leads to unfair or discriminatory outcomes without the user knowing anything about the underlying data-based discrimination.[73] Thus, the principle of algorithmic accountability can also be viewed as preserving human rights.[74]

Several governments, such as Singapore, Australia, and the United Kingdom, have advocated for transparency and explainability to improve algorithmic accountability and ensure greater trust in data-driven technologies.[75] The general thrust of such policies is that computer programs must have human controls to allow verification of the processes used in reaching decisions (for example, data processing and automated decision-making in AI technologies). However, certain governments, such as the United Kingdom, pragmatically recognize that different methods are necessary to achieve algorithmic accountability:

> We believe that the development of intelligible AI systems is a fundamental necessity if AI is to become an

---

72. Letter from Daniel Castro, *supra* note 70, at 3. R

73. *See generally* FRANK PASQUALE, THE BLACK BOX SOCIETY (2015) (discussing the various policy dangers of hidden, non-transparent algorithms in Big Data-driven technologies).

74. Lorna McGregor et al., *International Human Rights Law as a Framework for International Human Rights Accountability*, 68 INT'L & COMP. L.Q. 309, 313 (2019) ("A human rights-based approach to algorithmic accountability offers an organizing framework for the design, development and deployment of algorithms, and identifies the factors that States and businesses should take into consideration in order to avoid undermining, or violating, human rights. This is a framework which is capable of accommodating other approaches to algorithmic accountability—including technical solutions—and which can grow and be built on as international human rights law itself develops, particularly in the field of business and human rights.").

75. PERSONAL DATA PROTECTION COMMISSION SINGAPORE, *supra* note 40, at 12; *AI Ethics Principles*, *supra* note 40; SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE, *supra* note 58, at 40. The European Commission has also noted the importance of transparency and explainability. High-Level Expert Group on Artificial Intelligence, European Commission, *Policy and Investment Recommendations for Trustworthy AI* 10 (June 26, 2019), https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence [https://perma.cc/VZX3-RA8K]. R R R

> integral and trusted tool in our society. *Whether this takes the form of technical transparency, explainability, or indeed both, will depend on the context and the stakes involved, but in most cases we believe explainability will be a more useful approach for the citizen and the consumer.* This approach is also reflected in new EU and UK legislation. We believe it is not acceptable to deploy any artificial intelligence system which could have a substantial impact on an individual's life, unless it can generate a full and satisfactory explanation for the decisions it will take. *In cases such as deep neural networks, where it is not yet possible to generate thorough explanations for the decisions that are made, this may mean delaying their deployment for particular uses until alternative solutions are found.*[76]

Similarly, the Singaporean government also emphasized the importance of explainability and transparency in algorithms, while acknowledging that this is not always fully achievable.[77]

Modalities of achieving algorithmic accountability are controversial. Several experts argue that unfettered government access to source code and algorithms is essential to ensure that algorithms are fair, transparent, predictable, and non-discriminatory.[78] However, others argue that this approach is often less effective in practice, as algorithm decision-making cannot be accurately predicted by looking at the algorithms or codes alone, especially in cases involving complex AI/ML technologies.[79] Another controversial question is

---

76. SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE, *supra* note 58 , at 128 (emphases added). R

77. PERSONAL DATA PROTECTION COMMISSION SINGAPORE, *supra* note 40, at 12. The Australian government also treats these principles as aspirational. *AI Ethics Principles*, *supra* note 40. R R

78. *See* Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 25–30 (2014) (explaining the importance of transparency in automated scoring systems for insurance, credit finance and real estate); Nuria Oliver, *Governance in the Era of Data-Driven Decision-Making Algorithms*, *in* WOMEN SHAPING GLOBAL ECONOMIC GOVERNANCE 171, 175 (Arancha González & Marion Jansen eds., 2019) (arguing that transparency and accountability of algorithms used in data-driven technologies generates trust).

79. The development of explainable AI (XAI) could help resolve this technological gap. *See* Explainable AI, Google, https://cloud.google.com/

whether disclosing source code and algorithms to governments may lead to illegitimate, exploitative, or unauthorized uses of such technologies by governments themselves. For instance, governments could use technical information to install backdoors in digital devices or services to target dissidents or minorities. Such actions would directly impact the privacy of individuals and the security of their data as well as the digital technologies themselves.[80]

Some experts distinguish between algorithms being transparent and being explainable.[81] They argue that transparency of source code and algorithms cannot explain how programs work, and therefore excessive focus on transparency can lead to unintelligible outcomes.[82] Several experts even call this approach "naive" because it creates false trust that transparency of source code and algorithms ensures "procedural regularity."[83] Given that algorithms are influenced by training data and the environment in which they operate, the algorithms themselves reveal only "the machine learning method used and not the data-driven decision rule" and cannot accurately predict how the programs will function in all sets of circumstances.[84] For example, examining algorithmic enforcement in copyright infringement cases reveals very little about whether an algorithm effectively applied the factors of the fair use test,[85] which involve human judgment and discretion on a case-by-case basis.

Experts have proposed alternatives to regulatory access to source code and algorithms for achieving algorithmic accountability. Some alternatives include technological means to en-

---

explainable-ai/ [https://perma.cc/S4CE-M5VF] (last visited Aug. 31, 2020) (describing the benefits and features of XAI).

80. Mittelstadt et al., *supra* note 38, at 6. **R**

81. Maayan Perel & Niva Elkin-Koren, *Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement*, 69 FLA. L. REV. 181, 188–89 (2017). *See also* Kroll et al., *supra* note 34, at 649–50 (pointing out that transparency of source code only allows for static analysis while computer designs work in a dynamic environment). **R**

82. Perel & Elkin-Koren, *supra* note 81, at 184–85, 188. **R**

83. Kroll et al., *supra* note 34, at 657. **R**

84. *Id.* at 638, 648, 659–60; *see also* Perel & Elkin-Koren, *supra* note 81, at 189 (explaining that "transparent information about the structure of the underlying code may sometimes be relevant only to the precise moment when the information was originally released."). **R**

85. Perel and Elkin-Koren, *supra* note 81, at 197. **R**

sure that algorithms can be verified as fair, non-discriminatory, and lawful, and potentially holding designers and technology companies accountable for achieving these outcomes.[86] To do so, however, governments must understand the values and motivations that influence programmers.[87] Further, governments must clearly define public harm in the context of data-driven technologies so designs may be tailored to avoid such harm. Where public harm is unavoidable, governments may avoid the use of automated data-driven technologies completely.

Elements of algorithmic transparency and explainability are reflected in various domestic laws and regulations. For example, Article 22 of the GDPR provides an individual the right not to be subjected to a decision based solely on automated decision-making or profiling if that decision has "legal effects" or "significantly affects" the concerned individuals.[88] However, significant debate exists as to whether this provision incorporates a right to understand how the algorithms used in AI/ML technologies work.[89] In France, the Digital Republic Act sets a more explicit requirement that algorithms be explainable, but this law is applicable only to government decision-making.[90]

---

86. *See* FJELD ET AL., *supra* note 15, at 5 (discussing the incorporation of a set of AI principles into laws and regulations).

87. Perel and Elkin-Koren, *supra* note 81, at 189. R

88. GDPR, *supra* note 64, art. 22. The GDPR defines profiling very broadly to include "any form of automated processing" that considers personal information to analyze an individual. *Id.* art. 4(4). R

89. *Compare* Sandra Wachter et al., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIV. L. 7 (2017) (arguing that the GDPR incorporates a limited right for individuals to be informed about the logic of algorithmic decision-making and has no meaningful safeguards against automated decision-making), *with* Andrew D. Selbst and Julia Powles, *Meaningful Information and the Right to Explanation*, 7 INT'L DATA PRIV. L. 233 (2017) (arguing that the GDPR provisions arts 13–15 and 22 provide a meaningful right to explanation). *See also* Lilian Edwards and Michael Veale, *Slave to the Algorithm? Why a 'Right to Explanation' is Probably Not the Remedy You're Looking For*, 16 DUKE L. & TECH. REV. 18 (2017) (arguing that the GDPR does not provide a strong or clear right to an explanation of algorithms, but acknowledging that other GDPR provisions, such as the right to be forgotten, can improve explainability of algorithms).

90. For a discussion of the Digital Republic Act, see Lilian Edwards & Michael Veale, *Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?*, AI ETHICS, May-June 2018, at 46, 48. Similarly, the Algorithm Charter For Aotearoa New Zealand contains a commitment of the

U.S. Senators Cory Booker and Ron Wyden have also proposed an Algorithmic Accountability Act, which would impose obligations on digital technology providers to scrutinize their algorithms for potential privacy and security risks and discriminatory biases, thereby enabling greater algorithmic accountability.[91] This legislation would vest the U.S. Federal Trade Commission with the authority to implement regulations requiring companies to conduct risk assessment of automated technologies,[92] thereby identifying security issues and potential biases in algorithms, including the training data.[93] This legislation also allows companies to consult external technical experts in conducting such assessments.[94] However, the legislation fails to consider that explaining the functioning of automated algorithms is not always technically feasible. It also lacks clear guidance on what constitutes detrimental impact on accuracy, fairness, bias, discrimination, privacy, and security.

D. *Privacy and Security*

Online privacy and security have long been recognized in international policy as being of the utmost importance. This position is reflected not only in various internet multistakeholder declarations,[95] but also in several domestic laws and regulations.[96] Privacy and security issues are relevant both

---

government to ensure transparency of algorithms used in public decision-making. *See generally* GOV'T N.Z., ALGORITHM CHARTER FOR AOTEARAOA NEW ZEALAND (July 2020) https://data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020_Final-English-1.pdf [https://perma.cc/SY2V-F8N7] (committing to algorithmic transparency in public decisions, including explaining the decision-making logic of algorithms).

91. *See, e.g.*, Algorithmic Accountability Act, S.1108, 116th Cong. (2019).

92. *Id.*, § 2(2).

93. *Id.*, §§ 3(b)(1)(A)–(B).

94. *Id.*, § 3(b)(1)(C).

95. *See* Neha Mishra, *Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows*, 52 VAND. J. TRANSNAT'L L. 463, 484–93 (2019) (discussing various examples of multistakeholder declarations on internet privacy and cybersecurity).

96. According to the UNCTAD, 66% of countries have adopted data privacy laws. While there is no direct account of the number of countries with cybersecurity laws, UNCTAD has found that 79% of countries have adopted laws on cybercrime. *Summary of Adoption of E-Commerce Legislation Worldwide*, UNCTAD, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx [https://perma.cc/N56X-S5W8] (last visited Nov. 10, 2020).

in the development of data-driven services and in how individuals are affected while using such technologies: for instance, when subjected to automated algorithm decision-making.[97] Increasingly, scholars also argue that protecting privacy includes "group privacy," as Big Data analytics[98] permits discrimination against a specific group of people without regard to the personal data of individual members of that group.[99]

Privacy-related laws and regulations can address data management at all stages of data processing. Article 12 of the GDPR imposes an obligation on data controllers to provide concise, transparent, easily understandable, and accessible information regarding how they use personal data, including the extent to which they may be using or relying upon personal data for automated decision-making.[100] Articles 44 and 45 of the GDPR restrict data transfers outside the European Union to a limited number of circumstances in order to protect the privacy of E.U. residents.[101] A strong focus in domestic laws and regulations is on the anonymization of data,[102] especially given the growing use of personal data in several data-driven applications.[103]

Security in this context means protecting data-driven systems both internally from technical failures, data risks, and algorithmic security risks[104] and externally against cyber-at-

97. FJELD ET AL., *supra* note 15, at 4.

98. Big Data can be defined as "extensive datasets—primarily in the characteristics of volume, variety, velocity, and/or variability—that require a scalable architecture for efficient storage, manipulation, and analysis." *Information technology — Big Data Reference Architecture*, INT'L ORG. FOR STANDARDIZATION (Feb. 15, 2018) https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:20547:-5:ed-1:v1:en.

99. Luciano Floridi & Mariarosaria Taddeo, *What is Data Ethics?*, PHIL. TRANS. R. SOC., 2016, at 3.

100. GDPR, *supra* note 64, art. 12. R

101. GDPR, *supra* note 64, arts. 44, 55. R

102. *See* NITI AAYOG, NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE #AIforAll 62 (2018) (listing "advanced anonymisation protocols for data security and privacy" among AI challenges common to other countries).

103. Directorate General of Human Rights and Rule of Law (Council of Europe), *Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, T-PD(2018)09Rev, at 3 (Jan. 25, 2019), https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6 [https://perma.cc/VV4C-KGN4].

104. *See* Elsa Kania et al., *Translation: Key Chinese Think Tank's "AI Security White Paper" (Excerpts)*, DIGICHINA, (Feb. 21, 2019), https://

tacks.[105] While data security does not prima facie appear to be a data ethics issue, data security has implications for the ethical use of data-driven technologies. For example, unsecured technologies are more prone to privacy breaches, including illegal government surveillance. The security implications of data-driven technologies, such as AI, are especially complicated and widespread given that these technologies are general purpose technologies, widely used and thus potentially more insecure. Further, security vulnerabilities in data-driven technologies could lead to massive mistakes in training data known as "data poisoning," which can cause computer algorithms to function in an unexpected or undesirable manner, producing inaccurate outcomes that harm public interests.[106] With respect to AI technologies, governments concerned about public security risks[107] sometimes treat cybersecurity threats as national security risks.[108] Consequently, they may impose domestic security standards for data and algorithmic security[109] that may also prejudice individual rights.

Although present in many domestic regulatory frameworks, the concept of privacy and security varies significantly across countries. Certain countries, and most prominently the European Union, conceive of privacy and security in a highly human rights-centric manner, focusing on protecting individual rights and sheltering individuals from harm.[110] Other countries, such as the United States, rely on market forces to produce optimal outcomes in online privacy and security.[111] Still other countries, such as China, take a more cen-

---

www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-key-chinese-think-tanks-ai-security-white-paper-excerpts/ [https://perma.cc/E5KW-UL8M] (translating a paper on AI security risk by a Chinese think tank, which includes a discussion on the various types of related risks).

105. FJELD ET AL., *supra* note 15, at 39.

106. MILES BRUNDAGE ET AL., THE MALICIOUS USE OF ARTIFICIAL INTELLIGENCE: FORECASTING, PREVENTION, AND MITIGATION 17 (2018).

107. Kania et al., *supra* note 104 **R**

108. J. Benton Heath, *The New National Security Challenge to the Economic Order,* 129 YALE L. J. 1020, 1023–24 (2020).

109. Kania et al., *supra* note 104. **R**

110. The GDPR is a prime example of this phenomenon. GDPR, *supra* note 64. **R**

111. *See, e.g.*, NAT'L INST. STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [https://

tralized approach to privacy and security, relegating privacy and data security as secondary to issues of national security and government access to data.[112] In the latter scenario especially, governments could themselves use data-driven technologies in an unethical manner. Another practical problem in implementing privacy and security is the difficulty of keeping track of cyber-criminals who constantly devise innovative solutions to bypass privacy and security checks in digital technologies.[113] Finally, data regulation has significant geopolitical ramifications, including ensuring access to the data of important foreign intelligence partners or other strategic purposes.[114]

These multiple political dimensions of privacy and security can hinder governments from addressing data privacy and security purely from the perspective of data ethics. Implementing data ethics principles requires balancing different sets of policy objectives related to protecting rights of individuals, promoting efficient and reasonable regulations, and fostering a culture of digital innovation.[115] Expectedly, the balance that different countries strike between these policy objectives varies depending on the state of their economic and digital development and socio-cultural and political preferences.[116]

---

perma.cc/V9XB-LNSF] (discussing a U.S. cybersecurity framework that is largely driven by market and competitive security standards).

112. *See* Anthea Roberts et al., *The Geoeconomic World Order*, LAWFARE (Nov. 19, 2018), https://www.lawfareblog.com/geoeconomic-world-order [https://perma.cc/UD9Q-9W6N] (contrasting the approaches of the United States and China with respect to geoeconomic competition).

113. *Cybercriminals Continue to Evolve the Sophistication of Their Attack Methods*, HELP NET SEC. (May 23, 2019) https://www.helpnetsecurity.com/2019/05/23/cybercriminals-attack-methods/ [https://perma.cc/VCA2-7XKK].

114. *See generally* John Selby, *Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?*, 25 INT'L J.L. & INFO. TECH. 213 (2017) (arguing that data localization is driven not only by economic motives but also competition in intelligence gathering activities).

115. David J. Hand, *Aspects of Data Ethics in a Changing World: Where are We Now?*, 6 BIG DATA 176, 176 (2018).

116. *See* Ivan Szekely et al., *Regulating the Future? Law, Ethics, and Emerging Technologies*, 9 J. INFO., COMM. & ETHICS SOC'Y 180, 182 (2011) (discussing how E.U. standards of data ethics are likely to be much stronger than many other countries, although values such as respect for human dignity and human rights, freedom, democracy, rule of law, etc. are often universal).

III. Data Ethics Measures: Trade Barriers or Trade Facilitators

Compliance with the principles of data ethics can be both trade-facilitating and, in some cases, trade-restricting, depending on the content, design and implementation of the relevant measures. As data ethics principles generally facilitate digital trust, inform important data-related laws and regulations, and promote robust approaches in technical design and standards, they are likely to be beneficial to digital trade.[117] Companies offering data ethics-compliant services are more likely to be popular with internet savvy consumers, thus giving them a competitive advantage over other less secure technologies. For example, consumer surveys show that internet users prefer companies that provide trust-based solutions such as end-to-end encryption and transparent policies regarding the use and collection of data.[118] Further, despite the costs that businesses are likely to incur in complying with Data Ethics Measures, such measures could be advantageous in the long run. For example, they may facilitate the development of robust, reliable, and sustainable data-driven technologies and services. However, Data Ethics Measures could also become trade barriers. Given the potential dangers and abuses of facial recognition technology,[119] for instance, a government ban on software or devices facilitating facial recognition is not entirely inconceivable, especially for commercial purposes. Indeed, facial recognition technology was banned in the city of Boston for such

117. Mishra, *supra* note 95, at 501–03. R

118. *See* Timothy Morey et al., *Customer Data: Designing Transparency and Trust*, Harv. Bus. Rev., May 2015, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust [https://perma.cc/ZQ76-3Z72] (reporting that "consumers are aware that they're under surveillance . . . and are deeply anxious about how their personal information may be used.").

119. *See* Paul Muzor, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority*, N.Y. Times (Apr. 14, 2019), https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [https://perma.cc/Z28W-Y6DT] (discussing China's use of facial recognition technology to profile Uighur Muslims); Beth Holzer, *The Best Algorithms Struggle to Recognize Black Faces Equally*, Wired (July 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ [https://perma.cc/R769-5JK7] (highlighting how facial recognition is still cannot recognize black peoples with accuracy).

reasons.[120] Similarly, the use of AI/ML can also be curtailed in high-risk or sensitive sectors such as defense and law enforcement.[121] Finally, a de facto ban on a digital technology could have a trade-restrictive impact.

The requirement for digital technology providers to submit their algorithms and source code for government audit could also have a trade-restrictive impact.[122] Typically, such requirements are informed by policy rationales such as controlling disinformation campaigns,[123] ensuring high quality of digital products and services, and prohibiting discrimination of minority groups through racial profiling and targeting through facial recognition technologies or biased algorithms.[124] These measures can be trade-restrictive if they affect

120. Ally Jarmanning, *Boston Lawmakers Vote to Ban Use of Facial Recognition Technology by the City*, NPR (June 24, 2020) https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/24/883107627/boston-lawmakers-vote-to-ban-use-of-facial-recognition-technology-by-the-city [https://perma.cc/A866-8QPE].

121. *Autonomous Weapons that Kill Must be Banned, Insists UN Chief*, UN NEWS (Mar. 25, 2019), https://news.un.org/en/story/2019/03/1035381 [https://perma.cc/82H9-CWXW] (arguing that the use of AI in automated warfare must be banned); Taylor Hatmaker, *AI Researchers Condemn Predictive Crime Software, Citing Racial Bias and Flawed Methods*, TECH CRUNCH (June 24, 2020), https://techcrunch.com/2020/06/23/ai-crime-prediction-open-letter-springer/ [https://perma.cc/2PNG-5NTM] (citing a forthcoming report discussing the dangers of using AI in criminal investigations).

122. *See, e.g.*, Jonathan Vainan, *Microsoft Just Built a Special Version of Windows for China*, FORTUNE (May 23, 2017), https://fortune.com/2017/05/23/microsoft-windows-china/ [https://perma.cc/LM8G-N2LE] (reporting that Microsoft had to build a custom version of Windows 10 for the Chinese market to comply with domestic laws); Barb Darrow, *IBM Gives China Sneak Peek of Software Source Code: Report*, FORTUNE (Oct. 16, 2015), https://fortune.com/2015/10/16/ibm-source-code-china/ [https://perma.cc/JM4Y-Q4LL] (reporting that IBM was forced to share its source code with Chinese authorities). *See* Julia Ya Qin, *Forced Technology Transfer and the US–China Trade War: Implications for International Economic Law*, 22 J. INT'L ECON. L. 743, 745–46 (2019) (arguing that forced technology transfer requirements can violate various obligations in international investment law).

123. *See* Davey Alba & Adam Satariano, *At Least 70 Countries Have Had Disinformation Campaigns, Study Finds*, N.Y. TIMES (Sept. 26, 2019), https://www.nytimes.com/2019/09/26/technology/government-disinformation-cyber-troops.html [https://perma.cc/H7HW-P3BG] (quoting an expert's opinion that governments must look at the "algorithm and the underlying business model" to stop disinformation campaigns).

124. Daniel Munro, *How Tech Criticism Will Shape Our Digital Future*, CTR. FOR INT'L GOVERNANCE INNOVATION (Sept. 23, 2019), https://

companies' vital commercial interests, such as increasing chances of trade secret theft or compromising the security or integrity of their services.[125] Such measures may also prejudice the security of digital suppliers' global data operations[126] and cause reputational damage, particularly for multinational suppliers, as well as adversely impact digital innovation.[127]

As previously explained, demanding access to algorithms and source code is not always helpful in understanding the process of automated decision-making. Further, experts have pointed out that for some technologies such as autonomous vehicles, the accuracy and efficiency of the algorithms is more critical than transparency in order to ensure safety of users.[128] Further, if algorithms or source code are made public (i.e. open source), risks of misappropriation could increase, for example, by getting public disbursements or avoiding security checks.[129] Similarly, experts have suggested that open source code could potentially lead to autonomous and tacit algorithmic collusion to manipulate the market without human awareness or involvement,[130] thereby impeding the enforce-

---

www.cigionline.org/articles/how-tech-criticism-will-shape-our-digital-future [https://perma.cc/2EBC-X22J]. In addition, such measures may be necessary to prevent monopolization in specific markets such as online search. *See generally* PASQUALE, *supra* note 73, at 59–100 (arguing that market dominance in the search space by opaque players such as Google requires a revitalized regulatory approach). R

125. *See* WHITE HOUSE OFF. TRADE & MFG. POL'Y, HOW CHINA'S ECONOMIC AGGRESSION THREATENS THE TECHNOLOGIES AND INTELLECTUAL PROPERTY OF THE UNITED STATES AND THE WORLD (2018), https://www.hsdl.org/?view&did=812268 [https://perma.cc/2UDJ-BXAR] (discussing concerns related to trade secret theft in China).

126. Gabriel Wildau, *China Drafts Law to Ban Forced Tech Transfer from Foreign Partners*, FIN. TIMES (Dec. 24, 2018), https://www.ft.com/content/90cd02ba-0739-11e9-9fe8-acdb36967cfc [https://perma.cc/4GY6-T4VS].

127. Avi Goldfarb & Daniel Trefler, *AI and International Trade* 20–27 (Nat'l Bureau of Econ. Res., Working Paper No. 24254, 2018).

128. Letter from Daniel Castro, *supra* note 70, at 2. R

129. Kroll et al., *supra* note 34, at 633–34, 657; Kartik Hosnagar and Vivian Jair, *We Need Transparency in Algorithms, But Too Much Can Backfire*, HARV. BUS. REV., July 23, 2018, https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire [https://perma.cc/8TRH-8HPF] (referring to these risks as the "gaming" problem of transparent algorithms). R

130. *See* Lea Bernhardt and Ralf Dewenter, *Collusion by Code or Algorithmic Collusion? When Pricing Algorithms Take Over*, EUR. COMPETITION J. (Feb. 27, 2020) (discussing a common example of collusion by pricing algorithms and its potential anticompetitive effects).

ment of competition law in the digital age.[131] Finally, the construction of datasets has a deep impact on how data-driven technologies function.[132] This does not mean that digital technology providers should not be obligated to conduct necessary risk assessments or remain transparent about their technologies or data practices,[133] but rather that governments may need to employ varied methods to achieve effective compliance with the principles of data ethics.

Another set of Data Ethics Measures likely to be trade-restrictive are regulations for cross-border data transfer and processing to protect data privacy and security, including ensuring greater user control over who accesses their data, how this data is used and shared with third parties, and whether such data can be used in algorithmic decision-making. The most commonly discussed legislation in this regard is the GDPR, which incorporates various mechanisms to ensure that data processors comply with the high standards of data protection in the European Union, thereby protecting all E.U. citizens from unauthorized or unwanted surveillance and ensuring ethical use of personal data.[134] However, Big Data and AI/ML technologies often rely on using the same datasets in different ways to generate new services and more accurate results. Thus, excessive checks on the use and reuse of personal data through extensive consent mechanisms or authorization or licensing requirements can hamper the accuracy and predictability of AI/ML technologies. Similarly, restrictions on cross-border data flows often significantly increases compliance costs, especially for foreign companies, such as setting up new servers, applying for local permits, or leasing new domestic data facilities.[135]

---

131. *See generally* A. Ezrachi & M.E. Stucke, Org. for Econ. Coop. & Dev. [OECD], *Algorithmic Collusion: Problems and Counter-Measures*, at 18–25, DAF/COMP/WD(2017)25 (May 31, 2017), https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/WD%282017%2925&docLanguage=en [https://perma.cc/V5QL-VBS5] (discussing the enforcement challenges with respect to algorithmic collusion).

132. Lehr & Ohm, *supra* note 37, at 663–64. **R**

133. Oliver, *supra* note 78, at 177. **R**

134. *See* discussion *supra* Section II.

135. *See* Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?*, 19 World Trade Rev. 341, 343 (2020) (discussing various forms of market barriers arising from data localization).

A related example is data localization, which imposes direct or indirect requirements for the local storage of data.[136] These laws often result in economic and technological inefficiencies and reduced choice for consumers without significant impact on individual privacy and cybersecurity.[137] Data localization policies also often have a detrimental impact on the development and accuracy of AI technologies, as they can fragment global datasets.[138]

To respond to data governance concerns in the context of international trade, countries have started incorporating provisions requiring parties to achieve a basic level of data protection and high-level cooperation on cybersecurity in PTAs.[139] The Digital Economy Partnership Agreement (DEPA) between New Zealand, Singapore, and Chile goes a step further,[140] including a specific provision on Artificial Intelligence in Article 8.2:

> The Parties recognise that the use and adoption of AI technologies have grown increasingly widespread in a digital economy. The Parties recognise the economic and social importance of developing ethical and governance frameworks for the trusted, safe, and responsible use of AI technologies. In view of the cross-border nature of the digital economy, the Parties further acknowledge the benefits of developing mutual understanding and ultimately ensuring that such frameworks are internationally aligned, in order to facilitate, as far as possible, the adoption and use of AI technologies across the Parties' respective jurisdic-

136. *See* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2015) (defining data localization as "any obligation, prohibition, condition, limit or other requirement" in the "laws, regulations or administrative provisions of the Member States" imposing the location of data storage or other processing requirements for cross-border data processing).

137. Mishra, *supra* note 135, at 344–46. R

138. Joshua P. Meltzer, *The Impact of Artificial Intelligence on International Trade*, BROOKINGS (Dec. 13, 2018), https://www.brookings.edu/research/the-impact-of-artificial-intelligence-on-international-trade/.

139. *See* MARK WU, DIGITAL TRADE-RELATED PROVISIONS IN REGIONAL TRADE AGREEMENTS: EXISTING MODELS AND LESSONS FOR THE MULTILATERAL TRADE SYSTEM 25–26 (2017) (discussing PTA provisions on privacy and cybersecurity cooperation).

140. Unlike PTAs covering different issues in trade and investment, this agreement focuses only on issues pertaining to the digital economy.

> tions. . . . *In adopting AI Governance Frameworks, the Parties shall endeavour that such AI Governance Frameworks take into consideration internationally-recognised principles or guidelines, including: explainability, transparency, fairness, and human-centered values.*[141]

A provision on AI is also included in Article 31 of the Singapore – Australia Digital Economy Agreement (SADEA):

> 1. The Parties recognise that the use and adoption of Artificial Intelligence ("AI") technologies are becoming increasingly important within a digital economy offering significant social and economic benefits to natural persons and enterprises. The Parties shall cooperate, in accordance with their respective relevant policies, through: (a) sharing research and industry practices related to AI technologies and their governance; (b) promoting and sustaining the responsible use and adoption of AI technologies by businesses and across the community; and (c) encouraging commercialisation opportunities and collaboration between researchers, academics and industry.
>
> 2. The Parties also recognise the importance of developing ethical governance frameworks for the trusted, safe and responsible use of AI technologies that will help realise the benefits of AI. In view of the cross-border nature of the digital economy, the Parties further acknowledge the benefits of ensuring that such frameworks are internationally aligned as far as possible.
>
> 3. To this end, the Parties shall endeavour to: (a) collaborate on and promote the development and adoption of frameworks that support the trusted, safe, and responsible use of AI technologies ("AI Governance Frameworks"), through relevant regional and international fora; and (b) take into consideration internationally-recognised principles or guidelines when developing such AI Governance Frameworks.[142]

---

141. Digital Economy Partnership Agreement, Chile-N.Z.-Sing., NZTS. B2020-02, (signed June 12, 2020, not yet in force) art. 8.2 [hereinafter DEPA] (emphasis added).

142. *See Australia-Singapore Digital Economy Agreement*, signed 6 August 2020, [2020] ATNIF 11, art. 31[hereinafter SADEA].

These provisions are not binding and do not prescribe a specific AI governance framework. The phrase "internationally recognised principles or guidelines" in both the DEPA and the SADEA is likely to be interpreted in light of the political motivations of the parties.[143] The DEPA contains a list of illustrative examples of AI principles such as explainability, transparency, fairness, and human rights-centric values,[144] which indicates that the DEPA parties are inclined towards developing consensus on AI principles based on prevalent data ethics principles. Although the analogous provision in the SADEA does not include such an illustrative list, it does provide for a broad scope for cooperation between Singapore and Australia on AI research and governance, acknowledges the important role of regulatory frameworks on ethical AI and international alignment of AI frameworks, and encourages the development of AI frameworks consistent with internationally recognized principles and guidelines.[145] The focus on cross-border regulatory cooperation and alignment and the recognition of international norms and guidelines in SADEA, therefore, suggests that both Singapore and Australia also intend to establish high-quality AI governance frameworks domestically consistent with international principles. Therefore, it can be at least theoretically argued that both these provisions could help in building a stronger foundation for the development of transnational frameworks on data governance. However, it remains to be seen whether the DEPA or SADEA parties will utilize these provisions in domestic or transnational practice.

Internet governance experts are likely to question the expanded role of digital trade agreements in addressing AI governance frameworks. However, it could be argued that these provisions incentivize parties to implement AI governance frameworks consistent with internationally recognized principles or guidelines, incorporating global norms and best practices by reference rather than prescribing specific principles or guidelines. Being best endeavors provisions, they will not require trade tribunals to assess whether a certain AI governance framework is consistent with international norms. However, for this very reason, such provisions may also become superflu-

143. DEPA, *supra* note 141, art. 8.2.4; SADEA, *supra* note 142, art. 31.3. **R**

144. DEPA, *supra* note 141, art. 8.2.4. **R**

145. SADEA, *supra* note 142, art. 31. **R**

ous in circumstances where parties lack the political capability to enforce AI frameworks domestically.

With the expanding role of digital technologies in the global economy, Data Ethics Measures are more likely to be scrutinized under international trade law in the near future. Data Ethics Measures can play a critical role in strengthening digital trust and thereby facilitating digital trade. At the same time, certain Data Ethics Measures are clearly trade-restrictive and can be especially cumbersome for foreign companies to implement due to varying regulatory frameworks across countries. Consequently, such measures are likely to implicate different obligations contained in international trade agreements.

IV. Data Ethics and International Trade Agreements

This section discusses whether Data Ethics Measures are consistent with international trade agreements. Section IV(A) focuses on the consistency of Data Ethics Measures with nondiscrimination and market access obligations, while Section IV(B) focuses on domestic regulation disciplines in GATS. These two sections argue that the lack of multilateral technical standards on digital services and the uncertainties in the classification of digital services under GATS often complicates the application of these obligations to Data Ethics Measures. Sections IV(C) and IV(D) assess whether general exceptions and specific exceptions related to data flows in Electronic Commerce/Digital Trade Chapters of recent PTAs can justify trade-restrictive Data Ethics Measures. These sections argue that exceptions in international trade agreements can be interpreted to justify trade-restrictive measures with a legitimate data ethics rationale. However, trade tribunals must exercise caution in assessing the ethical element of such measures and their necessity in achieving data ethics objectives, including compliance with requirements in domestic privacy or cybersecurity laws. The lack of sufficient technological certainty and regulatory heterogeneity in emerging sectors such as AI will be a significant hurdle in assessing the necessity of such measures. Finally, Section IV(E) explains how provision on protection of trade secrets in the TRIPS Agreement and prohibitions on disclosure of source code in recent PTAs apply to Data Ethics Measures, as well as their impact on algorithmic accountability

and transparency. This section argues that while provisions on trade secrets can be interpreted fairly to balance public and commercial interests, governments must exercise the available exceptions for trade secret disclosures in good faith.

A. *Non-Discrimination and Market Access*

A common tool that governments adopt to achieve sound data governance and privacy and security in data-driven services is regulating how companies transfer and process data. As discussed in Section III, some of these restrictions are more direct, such as data localization laws, while others tend to be indirect, such as conditional restrictions on cross-border data transfers and other processing restrictions in data protection laws. Governments can also ban specific data-driven technologies, such as facial recognition software, either completely or at least from some or all foreign companies. This section argues that such restrictions may violate obligations on non-discrimination, specifically National Treatment (NT) and Most Favored Nation Treatment (MFN), as well as market access.

MFN and NT are the core obligations on non-discrimination in international trade law. The MFN obligation is breached if a country favors or disfavors digital services or service suppliers from specific countries in comparison to all other countries. For example, MFN treatment obligation in Article II of the GATS applies when a WTO member state fails to "accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favourable than that it accords to like services and service suppliers of any other country."[146] However, if a WTO member has listed specific service sectors in its Annex on Article II Exemptions, the MFN obligation does not apply to such sectors.[147] In contrast, NT requires that a country accord foreign services and service suppliers "treatment no less favourable than it accords to its own like services and service suppliers."[148] Essentially, this obligation prevents countries from favoring domestic services or service suppliers, disfavoring foreign services or service suppliers, or both. This obligation applies only in those

146. GATS, *supra* note 21, art. II:1.

147. *Id.* art. II:2.

148. *Id.* art. XVII:1.

service sectors and modes of delivery in which WTO members have inscribed commitments in their GATS Schedule.

The obligation of market access, such as Article XVI of the GATS, prohibits members from adopting or maintaining measures in service sectors where they have made commitments that limit the "number of service suppliers," the "total value of service transactions or assets," the "total number of service operations or . . . total quantity of service output," the "total number of persons that may be employed in a particular service sector or that a service supplier may employ," "the participation of foreign capital," and the "specific types of legal entity or joint venture through which a service supplier may supply a service."[149] Provisions on market access and non-discrimination are also found in many PTAs.[150]

Non-discrimination obligations apply only if the domestic and various foreign services and service suppliers are like. When a measure differentiates domestic and various foreign services or service suppliers exclusively based on country of origin, "likeness can be presumed."[151] A straightforward example is banning a software service or service supplier originating in one country.[152] If no instance of origin-based discrimination exists, the test of likeness primarily entails determining whether a "competitive relationship" exists between foreign and domestic services or service suppliers.[153] The pertinent

149. *Id.*, art. XVI: 2.

150. However, PTAs may have different Scheduling mechanisms. For example, where market access and NT commitments under GATS apply only in those sectors which members have expressly included in their respective Schedules, several U.S. PTAs provide for a negative list of all sectors in which market access and NT commitments are not applicable.

151. Appellate Body Report, *Argentina—Measures Relating to Trade in Goods and Services*, ¶ 6.38, WTO Doc. WT/DS453/AB/R (adopted May 9, 2016) [hereinafter *Argentina—Financial Services* Appellate Body Report].

152. For instance, the ban on Huawei and TikTok in several countries will qualify as an example of MFN violation under GATS Article II. Zhongdong Niu, *Huawei and TikTok Are at the Forefront of a New Drift to Regionalism – Many Others Will Follow*, CONVERSATION (July 29, 2020), https://theconversation.com/huawei-and-tiktok-are-at-the-forefront-of-a-new-drift-to-regionalism-many-others-will-follow-143306 [https://perma.cc/VD3U-G69B].

153. *E.g.*, Panel Report, *China—Certain Measures Affecting Electronic Payment Services*, ¶ 7.700, WTO Doc. WT/DS413/R (adopted Aug. 31, 2012); *see also* Panel Report, *Argentina—Measures Relating to Trade in Goods and Services*, ¶ 7.161, WTO Doc. WT/DS453/R (adopted May 9, 2016) ("In our view, the likeness analysis under Article II of the GATS does not differ from the like-

factors in evaluating competition between different services are the intrinsic character or nature and property (including quality) of the services, their end use, and consumer perceptions.[154]

Data Ethics Measures can be challenged under non-discrimination provisions in international trade agreements if they discriminate against like foreign services or service suppliers. WTO tribunals have developed the test of likeness as a case-by-case inquiry.[155] In the context of digital services, this means that WTO panels will likely apply existing criteria and determine the likeness of data ethics-compliant digital services and non-compliant services based on their online functions, their purposes for end users, and their sectoral classification. With the increasing digitalization of human activities, data ethics considerations may affect consumer choices more prominently in the future; privacy considerations arguably already play a pivotal role in consumer choices in several E.U. countries.[156] In this case, discrimination claims against such Data Ethics Measures may not be sustainable under the GATS because consumers may clearly differentiate between services that do and do not comply with ethics principles.

An unresolved question in the context of data-driven services is whether the scale or size of a digital service supplier

---

ness analysis under Article XVII of the GATS in the sense that it requires an approach based on the competitive relationship."); *Argentina—Financial Services* Appellate Body Report, *supra* note 151, ¶ 6.22 (holding that "Article XVII is concerned with competitive opportunities for like services and service suppliers of another Member"); *id.* ¶ 6.24 (holding that "in the context of Article II of the GATS, the determination of 'likeness' of services and service suppliers must focus on the competitive relationship of the services and service suppliers at issue"). R

154. *Argentina—Financial Services* Appellate Body Report, *supra* note 151, ¶¶ 6.57, 6.61; NICHOLAS F. DIEBOLD, NON-DISCRIMINATION IN INTERNATIONAL TRADE IN SERVICES: LIKENESS IN WTO/GATS 245, 353 (2010). R

155. Appellate Body Report, *Japan—Taxes on Alcoholic Beverages*, at 20–21, WTO Doc. WT/DS8/AB/R, WT/DS10/AB/R, WT/DS11/AB/R (adopted Nov. 1, 1996).

156. *See, e.g.*, Stephen White, *More European Citizens* Are Aware of Data Privacy Rights, Survey Shows, PRIVSEC REP. (June 14, 2019), https://gdpr.report/news/2019/06/14/more-european-citizens-are-aware-of-data-privacy-rights-survey-shows/ [https://perma.cc/59BP-VMVL] (discussing results of a survey by the European Commission suggesting enhanced awareness of privacy rights in the European Union).

should be a relevant factor in determining likeness.[157] For example, can a Big Tech company like Amazon or Microsoft be considered competitive in the same market as local Small and Medium-sized Enterprises (SMEs) providing similar online services? For instance, one could argue that these two services are not competitors in the same market because the data capabilities of Big Tech companies far exceed any local SMEs, thus leading to huge qualitative differences in services, even though these services prima facie appear similar in nature.[158] However, WTO panels may not consider these factors relevant if they adhere to the traditional criteria of likeness in determining market competition. While this question is not discussed in this article, further analysis may be helpful to understand if panels should adjust the likeness test for data-driven service sectors.[159]

In the future, governments may distinguish digital services or service suppliers adhering to high standards of data ethics from those that do not. A government may develop a certification or verification mechanism to monitor all digital services and service suppliers or ban digital services originating in countries with known records of data ethics violations. A relevant example is the development of a data ethics seal prototype in Denmark by the Ministry of Industry, Business and Financial Affairs to provide certification to companies that comply with good data ethics practices and use data responsibly.[160] A data ethics seal is likely to be considered a regulatory mea-

157. I thank Neeraj R.S. for raising this interesting question in our discussions.

158. An alternate means of determining market competition is to use a test common in competition law, i.e., whether a small but significant and non-transitory increase in price in the big foreign services would lead consumers to switch to local digital services or vice versa. However, this test may be difficult to employ for so-called free digital services, such as those offered by Google or Facebook.

159. Indeed, the Appellate Body in *Argentina—Financial Services* already indicated that the likeness test cannot be wholesale incorporated from GATT to GATS and may need to be adapted given the specific context of services. *Argentina – Financial Services* Appellate Body Report, *supra* note 151, ¶¶ 6.33, 6.41. R

160. *New Seal for IT-Security and Responsible Data Use is in its Way*, MINISTRY FOR INDUS., BUS. & FIN. AFFS. (Oct. 31, 2019) https://eng.em.dk/news/2019/oktober/new-seal-for-it-security-and-responsible-data-use-is-in-its-way/ [https://perma.cc/85Q7-7HZM].

sure based on the relevant data ethics standards and regulations within the country rather than based on market competition or differentiation.[161] In the future, the possible implications of such data certification mechanisms on market competition cannot be ruled out. However, given that current consumer preferences across most countries are not significantly shaped by data ethics considerations,[162] data ethics-compliant digital services are difficult to distinguish from other services, at least from the perspective of market competition enshrined in the GATS likeness test. Thus, the remaining part of this section analyzes whether Data Ethics Measures violate non-discrimination obligations under international trade law.

The restrictions contained in data protection and cybersecurity laws on cross-border data transfers and other processing requirements can violate non-discrimination obligations. For instance, strict data localization—like the relevant law in Russia—compels the majority of foreign service suppliers to relocate their data operations domestically, which increases their compliance costs and significantly reduces their competitiveness.[163] Although this requirement prima facie applies to all companies, foreign companies using global servers for their data processing operations are more likely to be affected by this measure than domestic digital companies. Therefore, if countries have offered relevant commitments in their GATS Schedule in sectors such as computer and related services,

---

161. It is possible that competition may develop between different data seals devised by different regulators, but this kind of regulatory competition can be distinguished from market competition.

162. *See, e.g.*, Sheila Colclasure, *On the Ethical Use of Data Vs. the Internet of Things*, FORBES (Dec. 21, 2016), https://www.forbes.com/sites/ciocentral/2016/12/21/on-the-ethical-use-of-data-vs-the-internet-of-things/#5a8ec05a1247 [https://perma.cc/B9YW-XKQM] (arguing that "[m]ost consumers are not preoccupied with knowing exactly how data about themselves is collected, analyzed and used").

163. Federal'nyi Zakon no. 242-FZ o vnesenii izmeneniy v nekotoryye zakonodatel'nyye akty Rossiyskoy Federatsii v chasti utochneniya poryadka obrabotki personal'nykh dannykh v informatsionno-telekommunikatsionnykh setyakh (Федеральный закон № 242-ФЗ о внесении изменений в некоторые законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях) [Federal Law No. 242-FZ on Amending Certain Legislative Acts of the Russian Federation Regarding Clarifying the Personal Data Processing Procedure in Information and Telecommunication Networks], July 21, 2014. art 2.

data localization laws are likely to violate NT.[164] Similarly, aspects of data protection laws can breach certain non-discrimination obligations.[165] For instance, under the GDPR, cross-border data transfers are allowed only to specific groups of countries based on the European Commission's assessment of the adequacy of their data protection framework.[166] This arrangement may violate the MFN obligation under the GATS, as data transfer is not permitted to countries that have not attained a positive adequacy assessment from the European Commission.[167] However, in examining this question, the WTO panels must take into account the competitive conditions between E.U. and non-E.U. digital services or service suppliers in the relevant sectors, as the adequacy arrangement is likely to be viewed as origin-based discrimination based on legitimate regulatory differences between different groups of countries.[168]

---

164. The main question for assessment would be the sector(s) in which the data localisation law applies and how the Member has scheduled commitments in those sectors on NT and market access. For example, data localization for all e-payment services would require an assessment of whether a Member has inscribed any NT or market access commitments on e-payment services.

165. Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfers*, 19 YALE J.L. & TECH. 194, 199 (2018); Svetlana Yakovleva & Kristina Irion, *Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation*, 114 AJIL UNBOUND 10, 11–12 (2020). *See also* Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy, the Conflict and Its Resolution*, 21 J. INT'L ECON. L. 769, 777–79 (2018) (noting that India does not provide adequate privacy protection under the GDPR).

166. GDPR, *supra* note 64, art. 45. **R**

167. The same argument could have applied to the data transfer agreement between the European Union and the United States (Privacy Shield), which was recently invalidated in the *Schrems-II* decision. Case C-311/18, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (July 16, 2020), http://curia.europa.eu/juris/document/document.jsf;jsessionid=A582C83AB28063A9F56B8218682A9C90?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=12744516 [https://perma.cc/BMH4-TX2H].

168. *Argentina – Financial Services* Appellate Body Report, supra note 151, ¶ 6.61. I thank Tsai Fang Chen for pointing out the implications of this finding in the context of the GDPR in a presentation at the 2019 AIELN conference. **R**

Data Ethics-related Measures can also violate market access obligations, such as Article XVI of the GATS.[169] For example, subject to E.U. commitments in different service sectors and modes of delivery on market access, the restrictions on cross-border data transfers in the GDPR can restrict the number of non-E.U. suppliers, especially small-sized companies.[170] This could be a violation of Article XVI of the GATS.[171] An example of a more blatant violation of market access would be a complete ban on a specific kind of data-driven technology, like facial recognition.[172] Although a detailed discussion is outside the scope of this article, the classification of various data-driven services remains contentious given the fast evolution of these technologies, the dated nature of the majority of GATS Schedules, and the converging nature of digital services combining software, audiovisual, and telecommunications services into a single platform or service.[173]

B. *Domestic Regulation*

International trade agreements also contain disciplines on domestic regulation. The most prominent example is Article VI of the GATS, which imposes an obligation to administer domestic regulations affecting trade in services in a "reasonable, objective and impartial manner."[174] Further, Article VI of the GATS contains general obligations requiring WTO mem-

169. GATS, *supra* note 21, art. XVI.

170. *See* Mishra, *supra* note 135, at 343 (arguing that "a data localization law forcing local data storage or processing increases compliance costs for foreign service providers and reduces market access, particularly for small and medium-sized enterprises"). R

171. GATS, *supra* note 21, art. XVI (banning measures limiting the number of service suppliers).

172. Further, if the ban only applied to digital services being supplied from foreign countries, then it would be a violation of NT (if all foreign companies were banned) or MFN (if foreign companies from specific countries were banned).

173. *See* ROLF H WEBER & MIRA BURRI, CLASSIFICATION OF SERVICES IN THE DIGITAL ECONOMY (2013) (discussing various examples of difficult classification of modern digital services under GATS).

174. GATS, *supra* note 21, art. VI:1. *See also* Comprehensive and Progressive Agreement on Trans-Pacific Partnership art. 10.8, Mar. 8, 2018, [2018] A.T.S. 23 (stating that parties "shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner.") [hereinafter CPTPP].

bers to institute tribunals and proper procedures for reviewing, approving, and providing remedies for administrative decisions.[175] For sectors in which members have offered specific commitments, Article VI:5 of the GATS prohibits members from imposing licensing requirements or technical standards that would "nullify and impair" those commitments, including requirements that are burdensome or not based on objective and transparent criteria,[176] or that "could not reasonably have been expected of that Member at the time the specific commitments in those sectors were made."[177] In assessing whether the licensing and qualification requirements and technical standards are reasonable and based on objective criteria, WTO panels can consider international standards set by "relevant international organizations."[178]

Provisions on domestic regulation can be relevant in the context of Data Ethics Measures. For example, certain aspects of the GDPR, such as the principle of data minimization, requiring that data collected and processed should not be held or further used unless clearly stated in advance or the requirement to obtain fully informed consent for data processing activities, could limit the manner in which personal data of E.U. residents is used for commercial data operations.[179] Further, such checks impose restrictive standards or authorization and licensing requirements on data use and reuse, especially for foreign companies, potentially violating obligations on domestic regulation.[180] Similarly, certain available safeguards in the GDPR for transferring data to non-E.U. countries such as standard contractual clauses for inter-company transfers and binding corporate rules for intra-company transfers[181] are disproportionately burdensome and expensive, especially for smaller

175. GATS, *supra* note 21, arts. VI:2, VI:3.

176. *Id.*, arts. VI:5(a)(i), VI:4.

177. *Id.*, art.VI:5(a) (ii).

178. *Id.*, art.VI.5(b).

179. GDPR, *supra* note 64, art. 5. **R**

180. GATS, *supra* note 21, art. VI.

181. GDPR, *supra* note 64, art. 46. *Cf.* European Commission Memorandum MEMO/05/03, Standard Contractual Clauses for the Transfer of Personal Data to Third Countries – Frequently Asked Questions (May 5, 2007) (explaining standard contractual clauses). **R**

foreign companies[182] and, thus could violate obligations on domestic regulation.

Government mandated technical standards for data-driven services could also become a trade barrier, particularly if the standard imposed is inconsistent with global industry standards. The AI race has resulted in fierce competition among certain countries, especially China and the United States,[183] to develop their own domestic standards that can eventually become de facto global standards, thereby giving these domestic players a greater share in the global markets.

Article VI:5 read with Article VI:4 of the GATS requires that any standards or technical requirements imposed by governments on service suppliers be reasonable, objective, and not unnecessarily restrictive.[184] In making this assessment, trade tribunals could look at standards developed by relevant organizations, but this definition is limiting because the GATS defines relevant organizations as "international bodies whose membership is open to the relevant bodies of at least all Members of the WTO."[185] This definition is more likely to cover multilateral institutions and exclude transnational and multistakeholder bodies that allow participation of non-state entities. This is because many private standard-setting bodies do not allow for traditional state membership or participation by state regulatory agencies.[186] Although private bodies play a central role in technical standard-setting in the digital sector,[187] AI

182. Mattoo and Meltzer, *supra* note 165, at 777. R

183. Kaveh Waddell, *The Global Race Between China and the U.S. to Set the Rules for AI*, Axios (July 14, 2019), https://www.axios.com/artificial-intelligence-china-united-states-5bea5020-c5c6-4527-8d25-7bf0036f6384.html [https://perma.cc/UC3E-YQ9W].

184. GATS, *supra* note 21, arts. VI:5(a)(i), VI:4.

185. *Id.*, art. VI(5)(b) n.3.

186. For instance, the Internet Engineering Task Force (IETF), which produces technical documents and standards for the internet, only allows network designers, operators, vendors, researchers, etc. to be members. *Who We Are*, IETF, https://ietf.org/about/who/ [https://perma.cc/7HXQ-QMQP] (last visited Sep. 28, 2020). The IEEE, a professional organization developing technical standards for digital technologies, only grants membership to individuals who are recognized in the profession. *IEEE Membership*, IEEE, https://www.ieee.org/membership/index.html [https://perma.cc/CH5A-VTSU] (last visited Sep. 28, 2020).

187. For a summary of role of the main private internet standard setting bodies, see Craig Bicknell, *Standards Bodies: A Field Guide*, Wired (Aug. 20,

standards developed by internet technical bodies or private bodies are unlikely to be covered by the GATS, even if they are well-accepted industry standards. Therefore, the existing rules on trade in services can fall short of facilitating open and competitive standard-setting practices. Considering that the majority of technical standards prevalent in the digital sector are developed by multistakeholder and private bodies, this deficiency in the rules on trade in services is an evident gap in international trade law.

C. *Justifying Data Ethics Measures Under WTO General Exceptions*

Although Data Ethics Measures can violate obligations in international trade agreements, they are often informed by public interest. This section examines the relevance of general exceptions in international trade agreements to justify Data Ethics Measures.[188] The general exceptions contained in WTO treaties are discussed first as they have been incorporated in several PTAs. Section IV(D) then covers specific exceptions in PTAs in electronic commerce or digital trade chapters that can apply to Data Ethics Measures.

1. *The Relevance of GATS General Exceptions in Justifying Data Ethics Measures*

Countries may defend Data Ethics Measures enforced through domestic data protection or cybersecurity laws under GATS art XIV(c)(ii). This provision applies if a measure: (a) is implemented to secure compliance with domestic "laws and regulations,"[189] including those protecting the privacy of indi-

---

1997), https://www.wired.com/1997/08/standards-bodies-a-field-guide/ [https://perma.cc/KC2F-V2WS].

188. Military applications of AI and the use of security exceptions in international trade agreements are outside the scope of this article, but for a discussion on this topic, see Amandeep Singh Gill, *Artificial Intelligence and International Security: The Long View*, 33 ETHICS & INT'L AFF. 169, 169–79 (2019); Steven Hill, *AI's Impact on Multilateral Military Cooperation: Experience from NATO*, 114 AJIL UNBOUND 147, 147–51 (2020).

189. *See* Appellate Body Report, *Mexico—Taxes on Soft Drinks and Other Beverages*, ¶ 79, WTO Doc. WT/DS308/AB/R (adopted Mar. 24, 2006) [hereinafter *Mexico—Taxes on Soft Drinks* Appellate Body Report] (holding that "laws and regulations" refer to domestic laws and regulations and does not include international law unless it is incorporated into domestic law).

viduals' personal data, records, and accounts; (b) is consistent with WTO law; and (c) is necessary to comply with laws and regulations.[190] Article XIV(c)(ii) can be interpreted in an evolutionary manner to cover aspects of digital privacy falling within the broad spectrum of data ethics.[191] For instance, "protection of the privacy of individuals"[192] can be interpreted to cover laws preventing unauthorized online government surveillance of individuals and indiscriminate use of personal data by companies without express user content. Similarly, domestic cybersecurity laws may be related to certain aspects of data ethics and broadly covered under domestic laws pertaining to safety[193] or prevention of fraudulent or deceptive practices.[194] In Article XIV(c), the term "secures compliance" implies that domestic laws and regulations should "enforce 'obligations' contained in [those] laws and regulations."[195] For example, data processing outside a state's borders may be restricted to prohibit illegal third-party use of personal data. However, the WTO Appellate Body (AB) has found that "se-

190. GATS, *supra* note 21, art. XIV(c)(ii). The specific steps for testing the necessity of measures under Article XIV(c) were set out in Panel Report, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶¶ 6.536–6.537, WTO Doc. WT/DS285/R (adopted Apr. 20, 2005) [hereinafter *US—Gambling* Panel Report]. *See also* Panel Report, *Colombia—Indicative Prices and Restrictions on Ports of Entry*, ¶ 7.514, WTO Doc. WT/DS366/R (adopted May 20, 2009) (holding that in raising a defence under the analogous provision of the GATT, Article XX(d), a WTO Member must "identify the laws or regulations for which it seeks to secure compliance, establish that those laws or regulations are not themselves WTO-inconsistent, and demonstrate that the particular measure at issue is itself designed to secure compliance with the relevant laws or regulations."); Appellate Body Report, *Korea—Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, ¶ 157, WTO Doc. WT/DS161/AB/R, WT/DS169/AB/R (adopted Jan. 10, 2001) [hereinafter *Korea—Various Measures on Beef* Appellate Body Report] (ruling in the context of Article XX(d) of the GATT); Appellate Body Report, *Thailand—Customs and Fiscal Measures on Cigarettes from the Philippines*, ¶ 177, WTO Doc. WT/DS371/AB/R (adopted July 15, 2011) (setting out the key elements of defence under Article XX(d) of the GATT).

191. *See* Appellate Body Report, *United States—Import Prohibition of Certain Shrimp and Shrimp Products*, ¶ 129, WTO Doc. WT/DS58/AB/R (adopted Nov. 6, 1998) [hereinafter *US—Shrimp* Appellate Body Report] (applying evolutionary interpretation to Article XX(g)).

192. GATS, *supra* note 21, art. XIV(c)(ii).

193. *Id.* art. XIV(c)(iii).

194. *Id.* art. XIV(c)(i).

195. *US—Gambling* Panel Report, *supra* note 190, ¶ 6.538. R

curing compliance" does not imply that the results of the measure can be guaranteed with "absolute certainty."[196] Article XIV(c)(ii) applies to measures necessary for the protection of individual privacy. Thus, it may not be relevant for Data Ethics Measures addressing group privacy or discrimination, transparency of digital technologies, or other human rights concerns such as providing adequate remedies for violating individual rights. As argued below, these concerns fit better into the exception for public morals or public order.

Under Article XIV(a) of the GATS, WTO members can impose measures "necessary to protect public morals or to maintain public order."[197] The term public morals is not defined in the GATS, but public order is defined as "a genuine and sufficiently serious threat" to "one of the fundamental interests of society."[198] While the wording of the article indicates that public morals and public order have distinct meanings, WTO tribunals have acknowledged that these two concepts can be overlapping.[199]

Theoretically, the concept of public morals can be interpreted with reference to universal morals, norms, or values, or to the specific values or culture of a country or community.[200] As the GATS defines public order with reference to the fundamental interests of society—and not the international community—it may be argued that public morals must also be interpreted with reference to the specific values and culture of a

196. *Mexico—Taxes on Soft Drinks* Appellate Body Report, *supra* note 189, ¶ 74. R

197. GATS, *supra* note 21, art. XIV(a). *See also* General Agreement on Tariffs and Trade 1994, art. XX(a), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1867 U.N.T.S. 187 (1994) [hereinafter GATT 1994] (allowing all WTO Members to impose any measures necessary to protect public morals, but does not include any reference to public order).

198. GATS art. XIV(a) n 5.

199. *See, e.g.*, *US—Gambling* Panel Report, *supra* note 190, ¶ 6.468 ("[T]o the extent that both concepts [public morals and public order] seek to protect largely similar values, some overlap may exist."). R

200. *Compare* Mark Wu, *Free Trade and the Protection of Public Morals: An Analysis of the Newly Emerging Public Morals Clause Doctrine*, 33 YALE J. INT'L L. 215 (2008) (arguing that WTO tribunals can adopt an outward-looking notion of public morals only if supported by "additional evidence"), *with* Steve Charnovitz, *The Moral Exception in Trade Policy*, 38 VA. J. INT'L L. 689, 742–43 (1998) (arguing the WTO should use international human rights law to inform public morals and reject trade actions based on "nationalistic aims").

country rather than the international community. Further, while the tension between universal and local values has not been addressed in WTO disputes,[201] WTO tribunals have generally deferred to local values, despite occasional references to declarations and policy goals of the international community. For example, although a panel considered the importance of bridging the digital divide in Brazil with reference to the Millennium Development Goals in *Brazil—Taxation,*[202] it did not suggest that members need to demonstrate that their public morals goals are aligned with or derived from international treaties or declarations.

WTO tribunals have considered varied policy objectives within the ambit of public morals and public order under Article XIV(a).[203] For instance, in *China—Publications and Audiovisual Products*, the panel held that censorship of printed and digital content fell within the scope of Article XIV(a).[204] In *US – Gambling*, the AB looked at various domestic laws and interpreted public morals to cover public order concerns related to "money laundering, organized crime, fraud, underage gambling and pathological gambling."[205] The panel stated that public morals under Article XIV(a) "denotes standards of

201. *See, e.g.*, Ming Du, *Permitting Moral Imperialism? The Public Morals Exception to Free Trade at the Bar of the World Trade Organization*, 50 (4) J. WORLD TRADE 675 (2016) (discussing the risks of moral imperialism if public morals would include extraterritorial application of particular norms).

202. Panel Report, *Brazil—Certain Measures Concerning Taxation and Charges*, ¶ 7.592, WTO Doc. WT/DS472/R, WT/DS497/R (adopted Jan. 11, 2019) [hereinafter *Brazil—Taxation* Panel Report]. *See also* Gillian Moon, *A 'Fundamental Moral Imperative': Social Inclusion, the Sustainable Development Goals and International Trade Law After Brazil—Taxation*, 52 J. WORLD TRADE 995, 1004 (2018) (discussing the various implications for public morality defence under GATT in the *Brazil – Taxation* case).

203. For a discussion of the relevant disputes on public morals, see Regis Y. Simo, *Trade and Morality: Balancing Between the Pursuit of Non-Trade Concerns and the Fear of Opening the Floodgates*, 51 GEO. WASH. INT'L L. REV. 407 (2019).

204. *See* Panel Report, *China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, ¶¶ 7.751–7.781, WTO Doc. WT/DS363/R (adopted Jan. 19, 2010) [hereinafter *China—Publications and Audiovisual Products* Panel Report] (examining various domestic laws on regulating published and audiovisual context in China and its connection to public morality).

205. Appellate Body Report, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 296, WTO Doc. WT/DS285/AB/R (adopted May 22, 2007) [hereinafter *US—Gambling* Appellate Body Report].

right and wrong conduct maintained by or on behalf of a community or nation," and such standards "can vary in time and space, depending upon a range of factors, including prevailing social, cultural, ethical and religious values."[206] In another dispute, *EC—Seal Products*, the AB held that public morals covered animal welfare concerns.[207] In *Brazil—Taxation*, the panel held that a measure imposed to bridge the digital divide and promote social inclusion fell within the scope of public morals.[208] Finally, in *Colombia—Textiles*, the panel held that a domestic tariff intended to combat money laundering fell within the scope of public morals.[209] Thus, the interpretation of Article XIV(a) of the GATS has generally been broad, flexible and evolutionary in light of contemporary policy concerns.[210]

Given such a broad formulation of "public morals," the international community has generally pushed towards interpreting general exceptions in a broad and flexible manner, including covering international human rights and transnational norms.[211] However, scholars have warned that an excessively broad interpretation of this exception can lead to pretextual uses and even the breakdown of the multilateral WTO system, allowing members to obscure protectionist objectives under a broad, ambivalent category of public morals or public order.[212]

How, then, should trade tribunals ascertain whether a measure genuinely qualifies as exceptional under public morals? Should they look at the broader context and rationale

---

206. *US—Gambling* Panel Report, *supra* note 190, ¶¶ 6.461, 6.465. **R**

207. Appellate Body Reports, *European Communities—Measures Prohibiting the Importation and Marketing of Seal Products*, ¶ 5.199, WTO Doc. WT/DS400/AB/R/, WT/DS401/AB/R (adopted June 16, 2014) [hereinafter *EC—Seal Products* Appellate Body Report].

208. *Brazil—Taxation* Panel Report, *supra* note 202, ¶ 7.592. **R**

209. Panel Report, *Colombia—Measures Relating to the Importation of Textiles, Apparel and Footwear*, ¶¶ 7.338–7.339, WTO Doc. WT/DS461/R (adopted June 22, 2016); Appellate Body Report, *Colombia—Measures Relating to the Importation of Textiles, Apparel and Footwear*, ¶ 5.105, WTO Doc. WT/DS461/AB/R (adopted June 22, 2016).

210. For an overview of the jurisprudence on evolutionary interpretation in WTO law, see generally Gabrielle Marceau, *Evolutive Interpretation by the WTO Adjudicator*, 21 J. INT'L ECON. L.791 (2018).

211. Wu, *supra* note 200, at 217, 224; Moon, *supra* note 202, at 1004. **R**

212. Wu, s*upra* note 200, at 248. **R**

behind the related measure, or is it enough for governments to state that the concerned measure relates to public morality?[213] In *EC – Seal Products*, the panel held that there are two key steps involved in this assessment: First, the stated policy concern must actually exist in the society, and second, the concern must fall within the scope of public morals.[214] Each WTO member has the discretion to decide what constitutes a question of public morality, consistent with its values and systems.[215] However, the AB has also held that there is no specific need to identify the existence of a risk[216] or "identify the exact content of public morals standard" at issue because there can be "variations" of public morals from country to country.[217] Further, members have the right to set "different levels of protection when responding to similar moral concern."[218] Unsurprisingly, no WTO tribunal has explicitly challenged a member's understanding of what constitutes public morals or public order and what they perceive to be a risk to these values. Instead, investigation has been limited to the necessity of the measure to protect the state-identified public morals or maintain public order.

In light of the deference of WTO tribunals, Data Ethics-related Measures are very likely to be justified under the public morals or public order exception. Governments could argue that their regulatory requirements for algorithmic accountability or ethical design are important elements of their domestic public policy, even when they have a trade-restrictive impact. Additionally, a respondent state may claim that its Data Ethics Measures preserve individual rights recognized under domestic and international law and policy.[219] However, as WTO

213. Oisin Suttle, *What Sorts of Things Are Public Morals? A Liberal Cosmopolitan Approach to Article XX GATT*, 80 MODERN L. REV. 569, 570–71 (2017).

214. Panel Report, *European Communities—Measures Prohibiting the Importation and Marketing of Seal Products*, ¶ 7.383, WTO Doc. WT/DS400/R/WT/DS401/R (adopted June 16, 2014) [hereinafter *EC—Seal Products* Panel Report].

215. *Id.* ¶ 7.381. This should also hold true for public order—governments can assess immediate and urgent threats to internal law and order or public security.

216. *See EC—Seal Products* Appellate Body Report, *supra* note 207, ¶ 5.198. **R**

217. *Id.* ¶ 5.199.

218. *Id.* ¶ 5.200.

219. In general, scholars have supported the idea that public morals could be extended to universal human rights standards. *E.g.*, Carola Glinski, *CSR*

tribunals resolve trade disputes and not human rights disputes, they cannot use Article XIV(a) for the purpose of enforcing international human rights.[220] Rather, in applying Article XIV(a) to Data Ethics Measures, panels could read the provision in a manner that does not interfere with a human rights-centric approach in data governance at a domestic level.

Privacy can also be a moral issue, as it is intrinsically tied to cultural, religious, and social values in many societies.[221] For instance, WTO members can argue that their privacy-related measures fall within the scope of Article XIV(a) of the GATS. For example, data related to one's sexual preferences (a common data point for dating applications, for example) may be considered highly private, evoking moral concerns around harassment or discrimination. Similarly, a digital device may track information regarding the places the device holder is visiting and may therefore implicate spatial privacy concerns. Further, the emergence of Big Data analytics raises concerns around group privacy, discrimination against specific minority groups, and targeting dissidents of a political regime. Depending on the social context, Data Ethics Measures addressing these concerns can also broadly fall within the scope of public morals and public order under Article XIV(a).

2. *Assessing the Necessity of Data Ethics Measures*

In *Korea – Various Measures on Beef*, the AB set out a two-factor test to examine the necessity of a measure falling under the general exceptions contained in Article XX of the GATT: (i) the relative importance of the interests and values underlying the measure; and (ii) a "weighing and balancing" of those

---

and the Law of the WTO – The Impact of Tuna Dolphin II and EC—Seal Products, 1 NORDIC J. COM. L. 121, 132–33 (2017).

220. *See* Gabrielle Marceau, *WTO Dispute Settlement and Human Rights*, 13 EUR. J. INT'L L. 753, 761, 777, 813–14 (2002) (arguing that while WTO dispute settlement bodies cannot adjudicate violations of human rights, WTO members must act consistent with both WTO law and human rights law); Sayed M. Zonaid, *Trading in Human Rights: Questioning the Advance of Human Rights into the World Trade Organization*, 27 FLA. J. INT'L L. 261, 286 (2015) (discussing the "undesirable consequences" of "embroiling" the WTO with the "nebulous" international human rights treaties).

221. *See, e.g.*, James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1154 (2004).

policy objectives[222] considering various factors such as contribution of the measure to the policy objective, the restrictive impact of the measure on international commerce, and availability of reasonable and less trade-restrictive alternatives as proposed by the complainant in the dispute.[223] Usually, the more "vital" or "important" the policy objective behind a measure is, the easier it is for panels to accept the necessity of the measure.[224]

If a measure falls under Article XIV of the GATS, the panel must examine the necessity of the measure to protect public morals or maintain public order under Article XIV(a) or to achieve compliance with domestic privacy or cybersecurity or other relevant laws under Article XIV(c). The first step in this test is assessing the contribution of the measure to the stated policy objective, i.e. determining whether there is "sufficient nexus" between the measure and the policy objective.[225] This test requires an objective assessment of a variety of factors, including the "design, architecture, and revealing structure of a measure."[226] For example, if a government imposes a restriction on cross-border data flows in order to safeguard individual privacy (e.g., a data localization requirement), a panel can investigate whether this measure contributes to enhancing privacy protection. Such a panel would likely note that several studies indicate that severe restrictions on data flows are generally ineffective in enhancing privacy.[227] Similarly, locating data within domestic borders does not automatically increase individual control or access over data. To

222. *Korea—Various Measures on Beef* Appellate Body Report, *supra* note 190, ¶ 164. R

223. *Id.*; Appellate Body Report, *Brazil—Measures Affecting Imports of Retreaded Tyres*, ¶ 178, WTO Doc. WT/DS332/AB/R (adopted Dec. 17, 2007) [hereinafter *Brazil—Retreaded Tyres* Appellate Body Report]; *US—Gambling* Appellate Body Report, *supra* note 205, ¶¶ 305–07. R

224. *Korea—Various Measures on Beef* Appellate Body Report, supra note 190, ¶162. R

225. *US—Gambling* Appellate Body Report, *supra* note 205, ¶ 292. R

226. *EC—Seal Products* Appellate Body Report, *supra* note 207, ¶ 5.302. R

227. *See, e.g.*, Tim Maurer et al., *Technological Sovereignty: Missing the Point?*, *in* ARCHITECTURES IN CYBERSPACE 61–62 (M. Maybaum et al. eds., 2015) (identifying the various security risks of data localization); Konstantinos Komaitis, *The "Wicked Problem" of Data Localization*, 3 J. CYBER POL'Y 355, 361–62 (2017) (discussing the "security and privacy fallacy" of data localization).

the contrary, such measures increase the possibility of unauthorized government surveillance and violation of human rights and interfere with the development of a healthy and competitive domestic digital market, especially when few domestic companies own all the data centers within a country.

Requirements imposed on digital companies to ensure that their algorithms and technical designs comply with the fundamental principles of data ethics, such as protecting human rights, prohibiting discrimination or bias, promoting accountability, and ensuring security and privacy of data provide another illustration of how the necessity test may be applied. For example, the GDPR requires data controllers to conduct a data protection impact assessment of technologies that are "likely to result in a high risk to the rights and freedoms of natural persons."[228] This could theoretically cover most AI/ML technologies, given the human rights risks inherent in their use.[229] Countries might also impose domestic regulations requiring all digital technology companies to comply with internationally recognized technical standards, adopt designs that protect privacy and security by default, or certify their compliance with certain basic principles of ethical design.[230] In contrast to blatant cross-border data transfer restrictions, such high-level requirements could be more effective in facilitating inclusive social behavior, preventing disinformation campaigns, and ensuring technologically robust solutions. Accordingly, such measures are more likely to satisfy the necessity test.

The next step in evaluating the necessity of a measure under Article XIV of the GATS is assessing "the restrictive impact of the measure on international commerce."[231] This could involve an assessment of all sectors affected by the measure. Indeed, as data-driven technologies, including AI, are used across several industries, highly restrictive measures will impact multiple sectors. Joshua P. Meltzer, an expert on digital trade, has argued that data localization measures have a very

228. GDPR, *supra* note 64, art. 35(1). R

229. I thank Svetlana Yakovleva for pointing out this nuance.

230. IEEE, *supra* note 29, at 28. R

231. Appellate Body Report, *China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, ¶ 306, WTO Doc. WT/DS363/AB/R (adopted Jan. 19, 2010) [hereinafter *China—Publications and Audiovisual Products* Appellate Body Report].

strong negative impact on AI-driven technologies.[232] Another example is the restriction on automated repurposing of data that can adversely impact the scope and accuracy of Big Data analytics.[233] These negative impacts will have to be balanced against the positive contributions of such measures in achieving their policy objectives.

Finally, in assessing the necessity of a measure under Article XIV of the GATS, WTO panels will consider if any of the complainant's proposed less trade-restrictive alternatives are "reasonably available" or feasible for the defendant to implement.[234] These alternatives must advance the stated policy objective to the same extent as the impugned trade-restrictive measure,[235] and any proposed alternative could entail additional risks and be subject to further regulatory constraints.[236] The test regarding less trade-restrictive alternatives is not fully clear in WTO law and can sometimes lead to counterproductive outcomes. For example, in *China – Publications and Audiovisual Products*, the panel effectively concluded that content censorship by the Chinese government was a less trade-restrictive alternative to censorship by Chinese state-owned enterprises,[237] a seemingly poor alternative in terms of protecting human rights.

---

232. Meltzer, *supra* note 138. R

233. Goldfarb and Trefler, *supra* note 127, at 20–27. R

234. *See US—Gambling* Appellate Body Report, *supra* note 205, ¶ 308 (holding that a measure is not "reasonably available" if it is "merely theoretical in nature, for instance, where the responding Member is not capable of taking it, or where the measure imposes an undue burden on that Member, such as prohibitive costs or substantial technical difficulties"); *China—Publications and Audiovisual Products* Appellate Body Report, *supra* note 231, ¶¶ 326–27 (stating that an alternative with "*some* change or administrative costs," may still be "reasonably available"). R

235. *See US—Gambling* Appellate Body Report, *supra* note 205, ¶ 308 (holding that a reasonably available alternative measure "would preserve for the responding Member its right to achieve its desired level of protection with respect to the objective pursued under paragraph (a) of Article XIV"); *see also Brazil—Retreaded Tyres* Appellate Body Report, *supra* note 223, ¶ 156 (setting out what constitutes a reasonably available alternative). R

236. Panagiotis Delimatsis, *Protecting Public Morals in a Digital Age: Revisiting the WTO Rulings on US—Gambling and China—Publications and Audiovisual Products*, 14 J. INT'L ECON. L. 257, 286 (2011).

237. *China—Publications and Audiovisual Products* Panel Report, *supra* note 204, ¶¶ 7.894, 7.900. R

Some experts consider self-regulatory and principles-based approaches to be more effective and efficient in the digital sector than highly prescriptive laws and regulations.[238] For example, allowing companies to adopt globally competitive standards would better enhance trade than imposing specific technical standards. Global standards are also likely to be more transparent and secure than domestic technical standards. In general, however, many alternatives, such as self-regulatory mechanisms and data certification mechanisms, are viewed as complementary measures rather than alternatives to prescriptive laws and regulations.[239] This is because countries are concerned about the robustness of these mechanisms and the representativeness of standards, especially if they are developed in private bodies without sufficient public oversight.[240] Further, Least Developed Countries (LDCs) and several developing countries are expected to lack adequate regulatory resources and expertise to participate in the development of these standards and market-driven certification mechanisms.

From a technological perspective, assessing the effectiveness of means to achieve data ethics compliance is challenging. For example, as discussed previously, mandatory disclo-

238. Or, experts at least believe both approaches are necessary to regulate data-driven technologies. Shin-yi Peng, *The Rule of Law in Times of Technological Uncertainty: Is International Economic Law Ready for Emerging Supervisory Trends?*, 22 J. INT'L ECON. L. 1, 13–15 (2019).

239. *See Brazil—Retreaded Tyres* Appellate Body Report, *supra* note 223, ¶¶ 151, 211 (acknowledging that certain complex policy problems need to addressed through a "multiplicity of interacting measures" and that some alternatives may simply be "complementary measures" rather than less trade restrictive alternatives due to their own risks or costs); Panel Report, *Australia—Certain Measures Concerning Trademarks, Geographical Indications and Other Plain Packaging Requirements Applicable to Tobacco Products and Packaging*, ¶¶ 7.1384–7.1391, WTO Doc. WT/DS435/R, WT/DS441/R, WT/DS458/R, WT/DS467/R (adopted Aug. 27, 2018) (discussing how a "complex suite of measures" may be necessary to address a complex policy concern and how all such measures would be complementary). *See also EC—Seal Products* Panel Report, *supra* note 214, ¶ 7.496 (holding that labelling requirements certifying compliance with animal welfare standards were not a less trade restrictive alternative). R R

240. Laura DeNardis & Mark Raymond, *The Internet of Things as a Global Policy Frontier*, 15 U.C. DAVIS L. REV. 475, 493 (2017) (discussing how information and communication technology firms have not adopted interoperable and open standards for Internet of Things technologies); Glinski, *supra* note 219, at 148. R

sure of algorithms does not always ensure transparency or predictability of outcomes as policymakers may not understand why AI programs reach certain decisions in specific cases. In the case of complex AI technologies, such as automated cars, demanding explainability of algorithms could result in reduced accuracy, thus compromising the safety of the user.[241] As debates around explainability and understandings of how algorithmic accountability can be enhanced for complex AI evolve, trade tribunals must be prepared to engage in a more complex legal and technical analysis of Data Ethics Measures. In doing so, they may also be required to rely upon expert evidence from the internet technical community and engineers from transnational standard-setting organizations.

If a trade-restrictive measure provisionally satisfies the necessity test under one the sub-clauses of Article XIV of the GATS, it will be further examined for consistency with the chapeau requirement that application of the measure does not "constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on international trade in services[.]"[242] This provision prevents members from abusing the Article XIV exceptions.[243] In conducting this assessment, the panel examines the implementation and operation of the measure[244] to ensure that it is implemented in good faith.[245] This requires an inquiry into the "design, architecture, and revealing structure of a measure"[246] to assess if the measure violates the chapeau in "its actual or expected application."[247]

For Data Ethics Measures, this step will entail examining how the measure is implemented, including instances of arbitrary discrimination or disguised protectionism. An example is where countries deliberately exclude foreign service suppliers from obtaining licenses or authorization to provide their services, irrespective of the quality and robustness of the techni-

241. Letter from Daniel Castro, *supra* note 70, at 2. **R**

242. GATS, *supra* note 21, art. XIV.

243. NELLIE MUNIN, LEGAL GUIDE TO GATS 372 (2010).

244. Appellate Body Report, *United States—Standards for Reformulated and Conventional Gasoline*, at 22, WTO Doc. WT/DS2/AB/R (adopted May 20, 1996).

245. *US—Shrimp* Appellate Body Report, *supra* note 191, ¶158. **R**

246. *EC—Seal Products* Appellate Body Report, *supra* note 207, ¶ 5.302. **R**

247. *Id.*

cal standards and algorithms used in these services. Another example is where governments illegally share the vital technical information of foreign service suppliers with domestic competitors, making it harder for foreign companies to compete in that market and causing IP or commercial losses. However, pragmatic difficulties might arise in proving that foreign governments are furthering domestic interests by leaking the trade secrets of foreign technology providers.

In conclusion, general exceptions in international trade agreements can be interpreted in a manner that supports principles of data ethics. Thus, international trade law does not prohibit governments from adopting or maintaining Data Ethics Measures outright. The exceptions are only a tool to ensure that the imposed measure is necessary to achieve the said moral or ethical policy objective(s) and does not contain arbitrary or protectionist elements. In fact, the WTO tribunals have thus far never interfered with how members define their policy agenda on preserving public morality or order. However, several questions remain uncertain in applying the necessity test. For instance, it is unclear what the limits for public morality should be as a justifiable policy basis for accommodating data ethics. Similarly, given the technological and policy uncertainty in this space, especially for complex AI, the standard of review that trade tribunals should adopt remains an open question.

D. *Provisions in Electronic Commerce Chapters in PTAs on Data Flows*

In addition to the abovementioned WTO treaties, rules in PTAs may also be relevant to Data Ethics Measures. Certain recent PTAs on data flows contain specific prohibitions on data localization measures and other forms of data restrictive measures in Electronic Commerce Chapters. Since several recent PTAs containing binding provisions on data localization and related measures are more or less directly derived from the Electronic Commerce Chapter of the Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP), this section focuses on the consistency of Data Ethics Measures with the CPTPP.

Article 14.11.2 of the CPTPP requires all parties to "allow the cross-border transfer of information by electronic means,

including personal information, when this activity is for the conduct of the business of a covered person," with "covered person" excluding financial institutions.[248] Similarly, Article 14.3.2 prohibits parties from requiring a "covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."[249] The net impact of both these provisions is that several data restrictions imposed for data ethics policy objectives are likely to prima facie violate the CPTPP.[250] However, the CPTPP also provides an exception that allows parties to adopt or maintain data localization measures or prohibit cross-border data flows if they are necessary to achieve legitimate public policy objectives. Such measures should not be applied in a manner that constitutes an arbitrary or unjustifiable discrimination or is a disguised restriction on international trade.[251] One notable difference is that the United States-Mexico-Canada Agreement (USMCA)[252] does not provide any exception for data localization measures in its Digital Trade chapter, although the general exceptions incorporated by reference will still apply.[253] Unlike the exhaustive WTO general exceptions, the provision in the CPTPP, USMCA, and other recent PTAs do not provide a specific list of policy objectives, instead referring to undefined "legitimate public policy objective[s]."[254]

Data Ethics Measures contrary to PTA provisions on data localization and cross-border data flows can be defended under the exception for legitimate public policy objectives.

248. CPTPP, *supra* note 174, art. 14.11.2. R

249. *Id.* art. 14.13.2.

250. This is subject to exceptions for the financial sector, *id.* art. 14.11.1, government data, *id.* art. 14.12.3, and non-conforming measures listed in parties' respective Schedules. *Id.* art 14.2.6.

251. *See id.* art. 14.11.3 (applying to the free flow of data); *id.* art. 14.13.3 (applying to data localization).

252. Agreement Between the United States, the United Mexican States, and Canada, Nov. 30, 2018, *available at* https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between [https://perma.cc/27YB-2HLG] [hereinafter USMCA].

253. *Id.* art. 32.1.2 ("For the purposes of . . . Chapter 19 (Digital Trade) . . . paragraphs (a), (b), and (c) of Article XIV of GATS are incorporated into and made part of this Agreement, *mutatis mutandis.*") (footnotes omitted).

254. CPTPP, *supra* note 174, arts. 14.11.3, 14.13.3; USMCA, *supra* note 252, art.19.11. R R

Given the wording and structure of these provisions, a necessity test similar to that of the WTO general exceptions is likely to apply, assessing whether a Data Ethics Measure that restricts cross-border data flows is necessary to achieve a legitimate domestic public policy objective. Legitimate public policy objectives may be broadly understood to cover several aspects of data ethics, including privacy and security, algorithmic accountability, protection of human rights, and ethical design. A broad interpretation is especially justified as many PTAs generally acknowledge that countries have their own domestic regulatory requirements for data flows.[255]

While governments may be able to use domestic policy objectives to impose data-restrictive measures through this exception, there may also be resulting legal uncertainty and potential misuse. Therefore, to ensure that exceptions are used solely for legitimate public policy objectives, PTA tribunals should apply the necessity test strictly. In other words, data localization measure or any other restriction on cross-border data transfer should contribute to promoting data ethics and should be the least trade restrictive means to do so. Further, tribunals must ensure that the measure is implemented in an even-handed manner, with no disguised protectionist intent.

E. *Protection of Trade Secrets and Algorithmic Disclosure*[256]

Article 39 of the TRIPS Agreement provides some protection to trade secrets to ensure that foreign companies are not subject to unfair competition, requiring members to "protect undisclosed information."[257] The core protection is contained in Article 39(2):

> Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by

255. *See, e.g.*, CPTPP, *supra* note 174, arts. 14.11.1, art. 14.13.1. **R**

256. Although algorithms could also possibly be covered under other branches of IP law, such as patent law, that discussion lies outside the scope of this article.

257. TRIPS Agreement art. 39(1). According to the TAPED dataset, seventy-three PTAs contain provisions protecting trade secrets, though not all of them are binding. *TAPED: A New Dataset on Data-related Trade Provisions*, UNIVERSITÄT LUZERN, https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped [https://perma.cc/ZSA7-T4GC] (last visited Nov. 11, 2020).

> others without their consent in a manner contrary to honest commercial practices so long as such information:
>
> (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
>
> (b) has commercial value because it is secret; and
>
> (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[258]

This provision has not been interpreted in WTO disputes to date.[259] However, reading both these provisions together, it could be argued that Article 39 of the TRIPS Agreement requires WTO members to ensure protection of undisclosed information so as to provide natural or legal persons with the possibility to protect information within their control from being acquired, disclosed, or used without their consent in a way that contravenes honest commercial practice. Such information must satisfy three requirements: (i) it should be a secret (i.e. not publicly available or readily accessible); (ii) it should have commercial value or competitive advantage because of its secrecy; and (iii) the business entity or individual should use reasonable steps to keep it secret.

Algorithms used in data-driven technologies qualify as information under Article 39(2) of the TRIPS Agreement because companies fiercely safeguard their algorithms, the basis of their competitive advantage in the digital market, from government or public scrutiny. Further, as trade secrets are not specifically defined, they can broadly include technical and business information that is not publicly available. Even

---

258. TRIPS Agreement art. 39(2) (footnote omitted).

259. However, the European Union has requested consultations with China on the ground that China's foreign technology transfer measures are inconsistent with Article 39 of the TRIPS Agreement. Request for Consultations by the European Union, *China—Certain Measures on the Transfer of Technology,* at 3, WTO Doc. WT/DS549/1, G/L/1244, IP/D/39 (June 6, 2018). Japan has also requested to join these consultations. Request to Join Consultations by Japan, *China—Certain Measures on the Transfer of Technology,* WTO Doc. WT/DS549/6 (Jan. 21, 2019).

databases such as training data can fall within the scope of Article 39(2); although some database entries may be publicly known, the process of assembling such datasets can be proprietary information.[260]

Article 39 of the TRIPS Agreement also requires all WTO members to provide avenues for companies to protect their algorithms, source code and other technical or proprietary information from unauthorized use, disclosure or acquisition in contravention of "honest commercial practices," defined as including "practices such as breach of contract, breach of confidence and inducement to breach, and [ ] the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition."[261] Cases of commercial espionage through targeted cyber-attacks, for example, qualify as contrary to honest commercial practices.[262] However, Article 39(2) does not explicitly state that governments should not contravene honest commercial practices. In fact, in practice governments can so act: for instance, when governments acquire information about algorithms and source code by imposing regulatory requirements and then illegally reveal such information to domestic competitors. While the provision is not explicit, Article 39(2) requires any party that is not the owner of confidential information or trade secrets to conform with honest commercial practices. Thus, when a government abuses its public powers to illegally benefit domestic companies, such action must be considered contrary to honest commercial practices. This interpretation is arguably consistent with the discussions among WTO members during the negotiation of the TRIPS Agreement provision on trade secrets.[263] In

260. Ingo Meitinger & Mira Burri, *Protection of Undisclosed Information: Commentary on Article 39 of the Trade-related Aspects of Intellectual Property Rights*, *in* CONCISE INTERNATIONAL AND EUROPEAN IP LAW: TRIPS, PARIS CONVENTION, EUROPEAN ENFORCEMENT AND TRANSFER OF TECHNOLOGY 119, 119 (2014).

261. TRIPS Agreement art. 39(2) n 10.

262. World Intell. Prop. Org. [WIPO], *Frequently Asked Questions: Trade Secrets*, https://www.wipo.int/tradesecrets/en/tradesecrets_faqs.html [https://perma.cc/FC77-6EJ7] (last visited Nov. 11, 2020).

263. *See* Negotiating Group on Trade-Related Aspects of Intellectual Property Rights, including Trade in Counterfeit Goods, *Synoptic Table Setting Out Existing International Standards and Proposed Standards and Principles*, WTO Doc. MTN.GNG/NG11/W/32/Rev.2, at 130–31 (Feb. 2, 1990) (indicating

practice, however, proving illegal state surveillance or trade secret theft is difficult.[264]

The next question is whether protection of algorithms as trade secrets under Article 39 of the TRIPS Agreement hampers algorithmic accountability. Article 39 requires WTO members to provide a route for companies to safeguard their trade secrets from espionage and illegal surveillance. However, it does not explicitly prohibit governments from demanding access to technical information when it is necessary to protect public interests. Therefore, legitimate measures that seek to verify algorithms for bias, compliance with domestic laws, or the technical security of code can be consistent with Article 39.

Further, Article 81(1) of the TRIPS Agreement provides that members may "adopt measures necessary to protect public health and nutrition, and to *promote the public interest* in sectors of vital importance to their socio-economic and technological development, provided that such measures are consistent with the provisions of this Agreement."[265] Under this provision, a member imposing mandatory algorithm or source code disclosure requirements for operating or selling in domestic markets could argue that such a measure is necessary to promote the public interest in data-driven sectors critical to socioeconomic and technological development. Here, legitimate public interests such as investigating algorithms for bias or technical flaws should be distinguished from ulterior motives such as stealing trade secrets to help domestic competitors. This distinction is important, as certain governments have been accused of misusing technical information to conduct illegal surveillance by, for instance, embedding secret backdoors in digital technologies or services in violation of individual privacy.[266] One means of preventing such illegal practices is examining how governments conduct software audits.

---

that disclosure of trade secret should only be compelled during major emergencies).

264. OECD, ENQUIRES INTO INTELLECTUAL PROPERTY'S ECONOMIC IMPACT 140 (Aug. 10, 2015), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2014)17/CHAP1/FINAL&docLanguage=en [https://perma.cc/8NYV-CBE3].

265. TRIPS Agreement art. 8(1) (emphasis added).

266. Kim Zetter, *Hacker Lexicon: What Is a Backdoor*, WIRED (Nov. 12, 2014), https://www.wired.com/2014/12/hacker-lexicon-backdoor/ [https://perma.cc/B4L7-AS3L].

Further, Article 8(1) states that such measures must be "necessary,"[267] implying that countries will need to show a causal link between their refusal to protect certain trade secrets and the underlying public interest. Illegitimate government activities, such as stealing IP secrets of foreign companies or conducting illegal surveillance, do not constitute a public interest under Article 8(1).

Some recent PTAs contain specific provisions that prohibit parties from requiring transfer of or access to source code "as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory."[268] However, in many PTAs, including the CPTPP,[269] this prohibition only applies to mass-market software, not critical infrastructure. Given that critical infrastructure is usually defined ambiguously, this prohibition may not apply to software used in several sectors.[270] The USMCA, the European Union-Mexico Global Agreement, and the Agreement Be-

267. TRIPS Agreement art. 8(1).

268. *E.g.,* Agreement Between Japan and Mongolia for an Economic Partnership, Japan-Mong., art. 9.11, Oct. 2, 2015, https://www.mofa.go.jp/files/000067716.pdf [https://perma.cc/JK4V-GAPV] [hereinafter Japan-Mongolia FTA]; CPTPP, *supra* note 174, arts. 14.17.1, 14.17.2; *Free Trade Agreement Between Australia and the Republic of Peru*, signed 12 February 2018, [2020] ATS 6 (entered into force 11 February 2020) art. 13.16.1 [hereinafter PAFTA]; Agreement Between the United States and Japan Concerning Digital Trade, Japan-U.S., art. 17.1, Oct. 7, 2019, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf [https://perma.cc/5ER8-SVPG] ; USMCA, *supra* note 252, art. 19.16.1. *See also* EU-Mexico Global Agreement: Chapter on Digital Trade, EU-Mex., art. 9.1, Apr. 21, 2018, https://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf [https://perma.cc/X6PQ-YM9S] ("No Party may require the transfer of, or access to, source code of software owned by a juridical or natural person of the other Party."); Agreement Between the European Union and Japan for an Economic Partnership, EU-Japan, art. 8.73.1, July 17, 2018, http://trade.ec.europa.eu/doclib/docs/2018/august/tradoc_157228.pdf [https://perma.cc/3B9C-RNEB] hereinafter EU-Japan EPA] ("A Party may not require the transfer of, or access to, source code of software owned by a person of the other Party."). The USMCA additionally prohibits parties from requiring transfer of or access to the "algorithms expressed in that source code." USMCA, *supra* note 252, art. 19.16.1. R R R R

269. CPTPP, *supra* note 174, art. 14.17.2. R

270. Neha Mishra, *The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?*, 20 J. INT'L ECON. L. 31, 49 (2017).

tween the European Union and Japan for an Economic Partnership do not contain a carve out for critical infrastructure, but they do contain relatively broad exceptions allowing governments to demand access to source code.[271]

The question then arises whether these PTA provisions prohibit governments from demanding access to source code or algorithms in order to ensure compliance with domestic laws and regulations and with the principles of data ethics, such as ensuring algorithmic accountability and reducing disinformation campaigns. A closer scrutiny of the relevant provisions in different PTAs indicates that the prohibitions on mandatory disclosure of source code and algorithms do not necessarily interfere with governments' ability to regulate data-driven sectors for ethical reasons. This is because such provisions cover various circumstances in which governments may still demand access to source code for ensuring compliance with data ethics principles.[272]

First, the CPTPP and subsequent agreements that borrow CPTPP language, including the Peru-Australia Free Trade Agreement (PAFTA) and Indonesia-Australia Free Trade Agreement, allow governments to demand modification of source code to ensure compliance with domestic laws and regulations.[273] It can be implied from these provisions that, to require modification of source code, governments must be able to demand access to companies' source code for verification. However, the lack of an explicit provision allowing regulatory access to source code for legal purposes in the CPTPP creates some uncertainty.

Second, the USMCA and the Agreement between Japan and the United States on Digital Trade provide for a broader exception allowing a regulatory body or judicial authority to require access to source code and algorithms for "specific in-

271. USMCA, *supra* note 252, art.19.16.2; EU-Mexico Global Agreement: Chapter on Digital Trade, *supra* note 290, art. 9.3; EU-Japan EPA, *supra* note 290, art. 8.73.2. R

272. The Japan-Mongolia FTA is the only PTA to date containing no specific exceptions allowing governments to demand access to source code/algorithms for public policy reasons.

273. CPTPP, *supra* note 174, art. 14.17.3; PAFTA, *supra* note 268, art. 13.16.3; *Indonesia–Australia Comprehensive Economic Partnership Agreement*, signed 4 March 2019, [2020] ATS 9 (entered into force 5 July 2020), art. 13.13.3 [hereinafter Indonesia-Australia FTA]. R

vestigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure."[274] These provisions provide greater legal certainty to governments' ability to regulate algorithms that may be discriminatory (and are thus better worded than the CPTPP provision discussed above). Further, the safeguard against unauthorized disclosure is critical in preserving the commercial interests of digital companies.

Third, the European Union-Mexico Global Agreement and European Union-Japan Free Trade Agreement recognize that prohibitions on disclosure of source code do not apply to enforcement of intellectual property rights or affect any requirements for providing remedies in domestic competition law.[275] The CPTPP and PAFTA specify that the requirements on source code disclosure do not affect any requirements pertinent to patent applications.[276] Under the Indonesia-Australia FTA and the European Union-Mexico Global Agreement, parties are permitted to require access to source code for protection of their "essential security interests."[277] The European Union-Mexico Agreement also explicitly states that parties are permitted to adopt or maintain measures for achieving "a legitimate public policy objective, including to ensure security and safety, for instance in the context of a certification procedure."[278] Therefore, although certain countries have signed PTAs that prohibit them from imposing disclosure or transfer of source code requirements as a domestic market access condition, the broad exceptions available under most of these PTAs allow for measures necessary to ensure algorithmic accountability and transparency.

---

274. USMCA, *supra* note 252, art. 19.16.2; Agreement Between the United States and Japan Concerning Digital Trade, *supra* note 268, art. 17.2. R R

275. EU-Mexico Global Agreement: Chapter on Digital Trade, *supra* note 268, art. 9.3; EU-Japan EPA, *supra* note 268, art. 8.73.2. R

276. CPTPP, *supra* note 174, art. 14.17.4; PAFTA, s*upra* note 268, art. 13.16.4. R

277. Indonesia-Australia FTA, *supra* note 273, art. 13.13.5; EU-Mexico Global Agreement: Chapter on Digital Trade*, supra* note 268, art. 16.9.3. R R

278. EU-Mexico Global Agreement: Chapter on Digital Trade*, supra* note 268, art. 9.2 (a). R

V. Policy Challenges of Data Ethics Measures

This section focuses on the policy challenges underlying the interface of international trade law and data ethics. It explores the various ways in which these challenges can be addressed, using existing trade law tools and incorporating new rules and mechanisms that align international trade law with data ethics principles. Section V(A) argues that exceptions in international trade agreements can accommodate Data Ethics Measures, but trade tribunals must adopt a coherent and balanced standard of review in evaluating both the ethics rationale and necessity of such measures in achieving compliance with data ethics principles. Section V(B) argues that trade secret protection provisions can play a critical role in balancing commercial interests and public concerns over data ethics, but such provisions must be implemented in good faith and subject to local and transnational accountability structures. These provisions have limited application, indicating the need for reforms to ensure a holistic approach in aligning international trade law with data ethics. Thus, Section V(C) explains how multilateral trade rules can accommodate multistakeholder norms, standards, and best practices in data governance through new rules and mechanisms in international trade agreements.

A. *The Ethical Dimension of Data Regulation: Using Exceptions Meaningfully*

Exceptions in international trade agreements are "safety valves" to accommodate unique domestic interests.[279] This article emphasizes the importance of the general exceptions in the GATS as well as the legitimate public policy exception in the Electronic Commerce/Digital Trade Chapters in PTAs. Since the concepts of public morals and public order in Article XIV(a) of the GATS has generally been interpreted in the context of the values and ethics of a society or community,[280] Data Ethics Measures are likely to qualify under the general exceptions. Similarly, exceptions for legitimate public policy objectives in PTAs can broadly cover data ethics concerns. Fi-

279. Delimatsis, *supra* note 236, at 261; Chien Huang, *Public Morals with Chinese Characteristics: Explaining China's Adoption of WTO Rules*, 41 Asian J. Soc. Sci. 333, 348 (2013). R

280. *See supra* notes 215–17 and accompanying text.

nally, countries can argue that certain Data Ethics Measures related to protecting individual privacy are justified under Article XIV(c)(ii) of the GATS as necessary to ensure compliance with domestic laws.

However, a very broad interpretation of the above exceptions may lead to potential abuse: for instance, if countries disguise their protectionist intent or ulterior motives in measures claimed as necessary to promote higher standards of data ethics. Scholars such as Ming Du have warned that a weak formulation of GATS exceptions on public morality and public order can render those exceptions "empty procedural requirement[s]."[281] In order to minimize misuse, trade tribunals must adopt a coherent and balanced standard of review in investigating Data Ethics Measures. However, difficult questions arise about the degree of discretion tribunals should have in dealing with technological and policy uncertainty. Similarly, the potential tension between universal values and specific domestic preferences on data ethics implicates difficult judgments regarding the normative boundaries of the exceptions contained in international trade agreements. International trade tribunals must employ both legal and technological evidence to make a holistic assessment of Date Ethics Measures under the necessity test. They should refrain from engaging in a de novo review, but they must also not adopt a standard so deferential as to limit their ability to curtail instances of blatant protectionism. Thus, striking the right balance is critical for a meaningful application of general exceptions to justify Data Ethics Measures.

One means of reducing blatant abuse of the exceptions in the GATS and PTAs is to align trade tribunal decisions with policy developments in the international community on data governance. However, despite the increasing international engagement on such issues, WTO tribunals are likely to continue reading general exceptions with a fair degree of deference to local values, especially since WTO law recognizes the right to regulate.[282] The same holds true for exceptions contained in

281. Du, *supra* note 201, at 692. **R**

282. *See, e.g.*, GATS, *supra* note 21, pmbl. (recognizing "the right of Members to regulate, and to introduce new regulations, on the supply of services within their territories in order to meet national policy objectives and, given asymmetries existing with respect to the degree of development of services

Electronic Commerce Chapters of PTAs, where legitimate public policy objectives will inevitably be tested against local values and systems.

A second route is to adopt a more stringent application of the weighing and balancing test under the exceptions.[283] The necessity test is generally meaningful in detecting discriminatory or unnecessarily trade-restrictive measures,[284] and looking at the technical aspect of a measure is less controversial than examining its moral or ethical elements, which often implicate sensitive political or cultural questions.

A more radical approach is to acknowledge the relevance of technological mechanisms to the regulation of data-driven technologies (provided these mechanisms meet the due process and rule of law requirements within the domestic jurisdiction). Kroll and others have argued that computer scientists or engineers are likely to play a critical role in verifying that designs and codes of data-driven technologies actually support a fair decision-making process. Precision in understanding algorithmic decision-making thus requires computer scientists to fully understand policy processes, so they can design technologies that meet necessary specifications and can be verified with considerable certainty.[285] This approach is not supported by the majority of domestic laws and regulations, which appear to be deliberately ambiguous.

Several governments impose requirements to disclose source code and other vital technical information for software

---

regulations in different countries, the particular need of developing countries to exercise this right").

283. *See* Silvia Nuzzo, *Tackling Diversity Inside WTO: GATT Moral Clause After Colombia – Textiles*, 10 EUR. J. LEGAL STUD. 267, 290–93 (2017) (discussing the "Weighing and Balancing" formula and the "Least Trade-Restrictive Means" approaches); Jeremy C. Marwell, *Trade and Morality: The WTO Public Morals Exception After Gambling*, 81 N.Y.U. L. REV. 802, 805 (2006) (discussing the approach taken in US—Gambling). *See also* Robert Howse et al., *Pluralism in Practice: Moral Legislation and the Law of the WTO After Seal Products*, 48 GEO. WASH. INT'L L. REV. 81, 87 (2015) (arguing that the discriminatory aspects of a measure should be assessed under WTO rules, not the element of public morality itself).

284. *See generally* Mishra, *supra* note 135 (arguing that protectionist measures disguised as privacy and cybersecurity measures are unlikely to meet the threshold of GATS Article XIV). R

285. Kroll et al., *supra* note 34, at 642. R

testing.[286] However, this approach is arguably less effective than requiring companies to comply with ethical design thresholds for fair and transparent automated decision-making.[287] In the past, WTO tribunals have respected states' choices to rely upon minority scientific opinion rather than mainstream science, as national authorities are better able to assess which risks are compatible with unique local values.[288] Therefore, WTO panels may not consider these mechanisms relevant. But as they become more widespread and effective, they could be viable alternatives to more trade-restrictive mechanisms that compromise the proprietary trade secrets of

286. China has imposed requirements on digital service suppliers to share their source code. Tekendra Parmar, *Tech Giants Push Back Against China's New Cyber Security Bill*, FORTUNE (Dec. 2, 2016), https://fortune.com/2016/12/02/cyber-security-bill-source-code/ [https://perma.cc/NG7S-ZBH9]. However, this requirement has been eased in recent amendments to domestic cybersecurity and encryption laws. Karen Ip et al., *China Cybersecurity and Data Protection: China Publishes First Law on Encryption*, HERBERT SMITH FREEHILLS (Nov. 12, 2019), https://sites-herbertsmithfreehills.vuturevx.com/95/21217/compose-email/china-cybersecurity-and-data-protection—china-publishes-first-law-on-encryption.asp [https://perma.cc/U6S7-H77D]. Recent press reports indicate that source code disclosure requirements are now being considered in Australia. Rohan Pearce, *Kaspersky Calls for Limits on Forced Source-Code Disclosure*, COMPUTERWORLD (July 5, 2019) https://www.computerworld.com/article/3480899/kaspersky-calls-for-limits-on-forced-source-code-disclosure.html [https://perma.cc/8SA9-TJSK]. Similar reports have surfaced about Russia. *See* Dustin Volz et al., *Tech Firms Let Russia Probe Software Widely Used by the U.S. Government*, REUTERS (Jan. 26, 2018), https://www.reuters.com/article/us-usa-cyber-russia/tech-firms-let-russia-probe-software-widely-used-by-u-s-government-idUSKBN1FE1DT [https://perma.cc/F7J6-HXSN] (reporting that a Russian defence agency went through tech companies' codes in return for market access).

287. Kroll et al., *supra* note 34, at 644–45. One proposed approach is to design modular programmes and then test each individual module against the necessary specifications. White box testing, randomised processes, and zero knowledge proof with cryptographic commitments are other options to achieve fair outcomes in automated decision-making. *Id.* at 663, 665, 669, 672–73. *See also* Desai & Kroll, *supra* note 55, at 10 ("[H]anding over code often will not enable the political accountability results those in favor of so-called algorithmic transparency desire.").

288. Nuzzo, *supra* note 283, at 276–77; Appellate Body Report, *United States–Continued Suspension of Obligations in the EC–Hormones Dispute*, ¶ 598, WTO Doc. WT/DS320/AB/R (adopted Oct. 18, 2008). *See also* Michael M. Du, *Standard of Review under the SPS Agreement after EC-Hormones II*, 59 INT'L COMP. & L. Q. 444, 451(2010) (arguing that the AB in *EC-Hormones II* "endorsed a more deferential, procedurally-focused standard of review.").

technology companies and disincentivize digital innovation. In that regard, the development of Explainable AI (XAI) will be a welcome development for digital trade.

Finally, digitally developed countries may also experiment with regulatory sandboxes (e.g., with specific companies, in specific sectors, or specific applications of digital technologies), to determine appropriate checks and balances, including whether certain decision-making processes should not be solely driven by data-driven technologies so as to avoid undesirable policy outcomes.[289] Sandboxes can be important in achieving legitimate public policy objectives, so they will most likely be consistent with international trade law.

B. *Trade Secret Protection Versus Public Interest*

The lack of trust in algorithms of data-driven services has increased the pressure on governments to acquire better access to proprietary technical and business information to verify the security of software and prevent algorithmic bias, especially in AI/ML technologies.[290] Expectedly, technology companies are likely to be guarded about sharing their source codes, algorithms, and other critical trade secrets with governments, especially given the chances of economic or political espionage. Protecting companies' proprietary software and trade secrets while also ensuring governments' ability to regulate the digital sector to promote ethical data practices entails a delicate balance.

Although international trade agreements contain provisions that prohibit unauthorized or involuntary disclosure of source code or algorithms, they also contain exceptions al-

289. McGregor et al., s*upra* note 74, at 314. **R**

290. *See, e.g.*, Algorithmic Accountability Act, S.1108, 116th Cong. (2019) (demanding greater algorithmic accountability in the US); *A Governance Framework for Algorithmic Accountability and Transparency*, at 71–74, European Parliamentary Research Service, PE 624.262 (Apr. 2019) https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf [https://perma.cc/FDQ2-6QQW] (demanding algorithmic impact assessments in the EU for both public and private decision-making in AI-driven services); GOV'T N.Z., ALGORITHM CHARTER FOR AOTERAROA NEW ZEALAND (July 2020) https://data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020_Final-English-1.pdf [https://perma.cc/SY2V-F8N7] (committing to algorithmic transparency in public decisions, including explaining the decision-making logic of algorithms).

lowing governments to access to source code or algorithms when needed for public policy reasons.[291] Given that establishing commercial espionage or trade secret theft is very challenging due to the covert nature of the activity,[292] technology companies could instead seek protection for their proprietary software and algorithms under IP laws, especially trade secret laws. However, very broad exceptions can reduce this protection. Ultimately, IP protection may adversely impact innovation,[293] but the secrecy of algorithms can also obstruct algorithmic accountability.[294]

In order to strike a balance between the public and commercial interests in data-driven systems, provisions on source code or algorithmic disclosure and trade secret protection in international trade agreements can and should be interpreted in a manner that promotes higher standards of data ethics. Certain recent PTAs have balanced protecting public interest and promoting digital innovation by including broad carve outs for critical infrastructure services and exceptions that cover a range of legitimate public policy objectives.[295] However, governments must use these exceptions in good faith and not impose unnecessary restrictions. Further, overly broad exceptions must be avoided in international trade agreements to prevent malicious state actors.

Accountability structures at the domestic level will be essential to ensure compliance with the principles of data ethics. Algorithms can be verified using technological mechanisms, like verifying that the software meets certain specifications, as well as through laws and regulations such as those holding companies liable for the malfunctioning of data-driven tech-

---

291. *See* discussion *supra* Section IV(E).

292. David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets Through Cyber Technologies,* 17 ASIL INSIGHTS (Mar. 20, 2013), https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving [https://perma.cc/W5FP-4PYT].

293. Protection of trade secrets generally has positive knock-on effects on digital innovation. *See generally* Katherine Linton, *The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research,* J. INT'L. COM. & ECON., Sept. 2016, at 10–13 (discussing the impact of trade secret protection on innovation, trade, and investment).

294. Sonia K. Katyal, *The Paradox of Source Code Secrecy,* 104 CORNELL L. REV. 1184, 1186–88 (2019).

295. *See* discussion *supra* Section IV(E).

nologies. Deven Desai and Joshua A. Kroll term the former "technical accountability" and the latter "legal-political accountability."[296] They argue that technical accountability such as verification through computer science methods is a "necessary step" to achieving legal-political accountability.[297] For example, a legal framework can recognize voluntary certification mechanisms developed by engineers that check whether a specific software or algorithm complies with relevant standards of data ethics compliance.[298] However, domestic laws and regulations typically do not sufficiently acknowledge the role of technical accountability, often leading to weaker regulatory choices.[299]

International trade agreements can incentivize countries to develop technical accountability alongside legal-political accountability to ensure stronger compliance with data ethics principles. For example, DEPA requires all parties to endeavor to promote AI governance frameworks compatible with internationally recognized standards. Although not legally binding, such provisions can encourage countries to develop mutually compatible frameworks on data-driven technologies as well as address problems of technical and politico-legal accountability in a complementary manner. For instance, through the regulatory cooperation mechanisms available and encouraged in international trade agreements, countries could agree to mutually recognize a multistakeholder body of highly qualified engineers and other technical experts that monitors and reviews data-driven technologies for compliance with the key principles of data ethics.[300] Such bodies could also be designed to incorporate sufficient (inter)governmental oversight. In the long run, such mechanisms may also facilitate the multilateral-

296. Desai & Kroll, *supra* note 55, at 11. R

297. *Id.*

298. *See* GDPR, *supra* note 64, art. 42 (allowing for development of privacy seals and trust marks in the European Union). R

299. The development of XAI may make this requirement more relevant in the future.

300. *See* Fjeld et al., *supra* note 15, at 32 (exploring the possibility of a monitoring body to regulate AI and the different, transnational visions for what such a body would be like); *see also* SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE, *supra* note 58, at 128 (suggesting collaboration between The Centre for Data Ethics and Innovation (a government body), the Alan Turing Institute, the Institute of Electrical and Electronics Engineers, the British Standards Institute, and other expert bodies). R

ization of an ethical data framework, thereby reducing instances of regulatory conflict and promoting ethical data regulation practices transnationally.

C. *International Cooperation for Data-Driven Innovation and Technical Standards*

The international community has repeatedly recognized the significance of multistakeholder models in resolving difficult policy challenges in data governance, such as promoting data ethics.[301] Achieving compliance with data ethics principles will thus necessarily require meaningful collaboration between governments, technology companies, and relevant multistakeholder and transnational organizations dealing with data governance. The current predominant approach of imposing highly prescriptive Data Ethics Measures is likely to be ineffective in achieving balanced data-driven innovation. For instance, several unilateral trade policies in the digital sector are resulting in tit-for-tat strategies, including significant decoupling in the technology sector between leading digital powers, thereby reducing competitiveness and sustainability in digital innovation.[302] Similarly, standard-setting competition between digital powers, especially in AI, is leading to unproductive outcomes.[303] In contrast, if leading digital powers worked towards bridging the gaps between their domestic policies, multilateral trade rules, and transnational norms and best

---

301. *See generally* U.N. Secretary General's High-Level Panel on Digital Cooperation, The Age of Digital Interdependence (2019), https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf [https://perma.cc/U4Y4-8ADJ] (describing the importance of digital cooperation in the age of digital interdependence).

302. For a discussion of technological decoupling in digital trade, see Cheng Ting-Fang & Lauly Li, *The Great US-China Tech Decoupling: Where Are We Now?*, NIKKEI ASIAN REV. (Dec. 30, 2019), https://asia.nikkei.com/Economy/Trade-war/The-great-US-China-tech-decoupling-Where-are-we-now [https://perma.cc/GGR3-PW3F]; Rana Foroohar, *China Wants to Decouple from US Tech, Too*, FIN. TIMES (Sept. 6, 2020), https://www.ft.com/content/371e139e-df4d-4ef8-9ed9-a92b97543af6 [https://perma.cc/Q9DW-TDM4].

303. Jeffrey Ding et al., *Chinese Interests Take a Big Seat at the AI Governance Table*, NEW AM. (June 20, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/ [https://perma.cc/WP92-SG9T]; Lorand Laskai & Helen Toner, *Can China Grow Its Own Tech Base?*, *in* AI POLICY AND CHINA 5–6 (Graham Webster ed., 2019).

practices in data governance, data-driven innovation would advance rapidly.

An important component of bridging this gap is ensuring recognition of globally competitive technical standards on data-driven services and technologies in international trade agreements. Standards play an important role in ensuring trust and interoperability.[304] The first intergovernmental standard on AI was adopted by the OECD Council on May 22, 2019.[305] However, the digital industry is predominantly dependent on private standards developed by multistakeholder or private bodies such as the IEEE, the International Organization for Standardization (ISO) and the IETF. Yet rules on trade in services in international trade agreements, such as the GATS, do not provide sufficient scope to consider these private or multistakeholder standards. For example, while assessing if domestic technical standards are consistent with international standards, trade tribunals are likely to only refer to multilateral standards due to the restrictive wording of "international organization" in Article VI of the GATS.[306]

Another WTO treaty, the Agreement on Technical Barriers to Trade (TBT Agreement), indirectly addresses the problem of transnational or private standards, allowing consideration of a broader range of standards by different international institutions provided certain basic factors, such as transparency, openness, impartiality, consensus, effectiveness, relevance and coherence, are met.[307] Further, some scholars ar-

304. MICHEL GIRARD, CTR. FOR INT'L GOVERNANCE INNOVATION, BIG DATA ANALYTICS NEED STANDARDS TO THRIVE: WHAT STANDARDS ARE AND WHY THEY MATTER, 2–3 (2019); Gasser & Almeida, *supra* note 25, at 60. R

305. OECD, *supra* note 23. R

306. *See* discussion *supra* Section IV(B).

307. Agreement on Technical Barriers to Trade, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, 1868 U.N.T.S. 120. *See* Appellate Body Report, *United States—Measures Concerning the Importation, Marketing and Sale of Tuna and Tuna Products*, ¶ 384, WTO Doc. WT/DS381/AB/R (adopted June 13, 2012) (stating that "an international standardizing body must not privilege any particular interests in the development of international standard."). Further, the TBT Committee of the WTO has developed guidelines for members in developing international standards, including transparency of procedures, openness of standard-setting bodies, following non-discrimination principles, impartiality, competitiveness and relevance of standards, coherence and consistency of international standards, and consideration developing country concerns. *Principles*

gue that disputes such as *Tuna Dolphin II* opened the doors for consideration of private transnational standards in WTO law.[308] Given the increasingly significant role of private and self-regulatory standards in data-driven services, trade rules applicable to data-driven technologies should recognize relevant industry standards and global best practices in data-driven sectors. Even the most recent PTAs containing an electronic commerce/digital trade chapter fail to address this deficiency and only include non-binding provisions encouraging countries to cooperate on technical standard-setting issues.[309]

Moving forward, TBT-like disciplines could be developed for data-driven services, where industry-driven or multistakeholder standards are usually more predominant.[310] However, such disciplines should be cautious to avoid industry capture, especially considering the extensive competition between countries in developing data-driven technologies and the highly political nature of technical standard-setting in the digital sector.[311] Developing countries and LDCs are especially vulnerable to coercion by leading digital powers, particularly given the conflicting digital "sectors of influence" of the United States and China and, to a lesser extent, the European Union.[312] In the WTO, countries may also consider developing new rules or reinterpreting existing rules to permit an expansive understanding of terms such as "international standards of relevant international organizations"[313] so as to pay greater attention to multistakeholder standards in data-driven sectors. Such reforms cannot address *ad hoc* processes set up in

---

for the Development of International Standards, Guides and Recommendations, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm [https://perma.cc/X73U-PMDK] (last visited Nov. 11, 2020).

308. Glinski, *supra* note 219, at 148. **R**

309. Andrew D. Mitchell & Neha Mishra, *Data at the Docks: Modernizing International Trade Law for the Digital Economy*, 20 VAND. J. ENT. & TECH. L. 1073, 1101–02 (2018).

310. A similar suggestion was made in the context of regulating cross-border data flows under WTO law. Andrew D. Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22 J. INT'L ECON. L.389, 413 (2019).

311. Cath & Floridi, *supra* note 29, at 449, 453. **R**

312. Anthea Roberts et al., *Toward a Geoeconomic Order in International Trade and Investment*, 22 J. INT'L ECON. L. 655, 673–75 (2019).

313. GATS, *supra* note 21, art. VI:5.

response to specific technological requirements[314] or standards developed by open sourcing on platforms such as Github.[315] However, domestic governments could recognize such standards provided they are compliant with the key principles of data ethics.

A related issue in international trade law is the reasonableness, efficiency, and objectivity of authorization and certification processes for data-driven technologies. Many of these mechanisms are currently being developed domestically in highly developed countries, leading to regulatory fragmentation and reduction in their market appeal.[316] The majority of developing countries in Africa, South and Central America, and Central Asia do not have a framework in place for data-driven technologies such as AI/ML.[317] Therefore, even if certain monitoring mechanisms appear to be technologically and economically efficient, they may not be relevant to countries without sufficient capacity and resources to monitor or implement them. These factors should be considered in evaluating the laws and regulations of developing countries under international trade law.

To play a more proactive role in promoting globally competitive, transparent, and interoperable technical standards and best practices in digital trade, international trade institutions should look beyond traditional cooperation mechanisms with other international organizations. For instance, in addition to aligning with the International Telecommunications Union, one of the key multilateral institutions involved in technical standard-setting,[318] the WTO and other regional trade institutions can form collaborative partnerships with internet technical bodies such as the IETF and private standard-setting institutions such as the ISO and the IEEE. However,

---

314. *See* Girard, *supra* note 304, at 12 (pointing out how standards consortia are more sensitive to technological advancement than traditional standards development organizations and thus have shorter lifespans). R

315. *Id.*

316. *See White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, at 10, COM (2020) 65 final (Feb. 19, 2020) (showing the potential regulatory fragmentation within the European Union).

317. Jobin et al, *supra* note 15, at 396.

318. *ITU-T Recommendations and Other Publications*, ITU, https://www.itu.int/en/ITU-T/publications/Pages/default.aspx [https://perma.cc/M9EZ-PQJH] (last visited Nov. 11, 2020).

the existing rules, including in the most recent PTAs, do not allow for such formal cooperation, despite the increasing recognition of the importance of multistakeholder approaches in internet and data governance.[319] Yet informal cooperation is nevertheless possible. For instance, these expert institutions could be invited to present to the relevant committees in international trade institutions dealing with electronic commerce matters. Similarly, technical experts can play a meaningful role in resolving disputes on data-related measures. However, whether trade bodies will engage in such multistakeholder partnerships in the coming years remains uncertain.

A reasonable degree of transparency in the negotiation of digital trade rules can facilitate the meaningful participation of all interest groups, especially relevant expert multistakeholder bodies, allowing them to provide inputs on best practices and data ethics standards. Given the expanding agenda on electronic commerce in international trade agreements and the increasing intersection between trade rules and data governance, this form of engagement is especially necessary. Further, at domestic and regional levels, certain governments such as the United States and even the European Union are developing stronger coordination mechanisms with the private sector. These coordination mechanisms could eventually grow transnationally, especially between groups of like-minded countries, facilitating greater regulatory cooperation on data ethics-related issues. International trade institutions should rely upon the outputs of these coordination mechanisms (e.g., standards and best practices for data transfer or processing), in applying domestic regulation rules in Article VI of the GATS. By adopting such a broad-based and open approach, international trade institutions can play a more meaningful role in global data governance and unlock the economic and social benefits that arise from global cooperation in growing sectors such as AI.[320]

---

319. *See* U.N. Secretary General's High-Level Panel on Digital Cooperation, *supra* note 301 (noting the importance of multistakeholder solutions to resolve global policy problems in the digital space). R

320. JOSHUA P MELTZER ET AL., BROOKINGS INST. SUBMISSION TO THE EC WHITE PAPER ON ARTIFICIAL INTELLIGENCE 4 (2020).

VI. Conclusion

Countries increasingly adopt Data Ethics Measures to ensure a human rights-centric approach to data governance and increase digital trust and security. However, some of these measures are highly prescriptive and may even pose a barrier to digital trade, especially if they restrict data flows or impose burdensome compliance requirements on technology companies. Data Ethics Measures that are trade-restrictive can conflict with various obligations contained in international trade agreements, but governments can justify such measures under the general exceptions in WTO law (necessary for protecting public morals, maintaining public order, or achieving compliance with domestic laws), and the legitimate public policy exception in the Electronic Commerce Chapters of recent PTAs. Similarly, although international trade agreements contain certain obligations on protecting trade secrets, including restricting forced disclosure of source code, these provisions also contain exceptions that can meaningfully balance the commercial interests of technology companies with legitimate public interests.

In the absence of internationally binding standards and best practices for data-driven technologies, considerable legal uncertainty is likely to exist regarding how trade obligations apply to certain Data Ethics Measures. Further, in applying exceptions to justify such measures, trade tribunals can err if they read the exceptions too narrowly (i.e. constraining the regulatory space necessary for AI and data regulation) or too broadly (i.e. permitting countries to abuse the exception to adopt protectionist measures). Referring to norms and best practices set out in international treaties and multistakeholder declarations, in addition to local policy preferences, could be helpful in determining a balanced interpretation and application of the exceptions. Further, trade tribunals must examine the necessity of Data Ethics Measures holistically, taking into account available legal and technical evidence, including the evolution of business and technological practices on algorithmic accountability and ethical design. Stronger recognition of private and multistakeholder standards and best practices in data-driven sectors is desirable in international trade law, especially in the context of digital services. The Code of Good Practice under the TBT Agreement is an important

benchmark in this regard. Greater transnational regulatory coordination among countries engaging in data-driven trade can further the achievement of this goal. Finally, sound and reasonable accountability structures at the domestic level are crucial to balance commercial and public interests.

In the current environment of increasing trade tensions and the decline of public trust in trade negotiations, the proposals presented in this article may appear challenging and ambitious. However, the proposed reforms to international trade agreements can contribute to balancing the diverging regulatory preferences on data governance and promote ethical data-driven technologies. Eventually, such reforms will also ensure that international trade institutions play a more concrete and relevant role in the regulation of data-driven trade. However, to achieve this goal, it is imperative that international trade institutions enhance their willingness and capacity to understand and, when necessary, adapt their rules and processes to evolving norms in data governance.