Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows

Neha Mishra[*]

ABSTRACT

The regulation of internet data flows touches upon various distinct disciplines including internet governance and international trade law. In internet governance, three fundamental principles, namely, internet openness, internet security, and internet privacy apply to regulation of internet data flows. This Article argues that internet privacy and security, when implemented in a reasoned and transparent manner by different stakeholders, enable internet openness—thus, challenging the dominant perspective that cybersecurity and privacy requirements constrain the free flow of data. Further, this Article introduces a unique perspective by arguing that these three principles (notwithstanding their nonbinding nature) play an important role in applying trade law to data restrictive measures, particularly by facilitating a sound framework that balances domestic internet regulation and liberalised data flows, thus contributing to balancing of trade and non-trade policy goals. Given this important relationship between trade and internet governance, this Article suggests that different options must be explored to enhance dialogue and coordination between these two policy communities so as to build a sound, balanced, and holistic regulatory environment for cross-border data flows.

---

[*] I acknowledge the support of the Australian Government Research Training Program Scholarship. I thank Tania Voon, Andrew Mitchell, Margaret Young, Jurgen Kurtz, Mia Mikic, Luís Paulo Bogliolo, and Robi Rado for comments on earlier drafts/presentations of this Article. I also thank the editorial team of Vanderbilt Journal of Transnational Law for their helpful comments and diligent editing. A preliminary draft containing certain parts of the paper was made available as a working paper in the ArtNet Working Paper Series. MPP (NUS); LLM (LSE); BA LLB (Hons) (NLSIU); PhD Candidate, Melbourne Law School, University of Melbourne and Visiting Research Fellow, Max Planck Institute, Luxembourg. Email: <mishra.neha@gmail.com>.

TABLE OF CONTENTS

I. INTRODUCTION

At first sight, international trade law appears disconnected from internet governance due to the stark divergence in the legal and institutional structures of the two regimes. While international trade law governs relationships amongst countries, internet governance is considered to be a largely multistakeholder process aimed at policymaking for a universal and global internet, unconstrained by national borders.[1] International trade law comprises rules developed by countries through negotiated agreements at the World Trade Organization (WTO)[2] and other mechanisms such as preferential trade agreements (PTAs).[3] Several provisions, including obligations on nondiscrimination and market access, within international trade agreements are binding and enforceable, such that government measures that constitute barriers to trade may be actionable in international trade law. In contrast, different aspects of internet policymaking are dispersed across government departments,[4] multistakeholder bodies,[5] multilateral institutions (e.g., the

1. CTR. FOR INT'L GOVERNANCE INNOVATION & THE ROYAL INSTITUTE FOR INT'L AFFAIRS, GLOBAL COMMISSION ON INTERNET GOVERNANCE: ONE INTERNET 9–10 (2016), https://www.cigionline.org/sites/default/files/gcig_final_report_-_with_cover.pdf [https://perma.cc/2VU6-PRP9] (archived Jan. 15, 2019) [hereinafter GCIG ONE INTERNET].

2. *Understanding the WTO*, WORLD TRADE ORG., https://www.wto.org/english/thewto_e/whatis_e/tif_e/tif_e.htm (last visited Jan. 15, 2019) [https://perma.cc/VP9E-2EXR] (archived Jan 15, 2019).

3. PTAs cover all international trade agreements outside of the WTO such as regional trade agreements, bilateral trade agreements, or megaregional trade agreements.

4. For example, the governmental trade agency is likely to deal with e-commerce-related issues, the ministry of telecommunications would deal with issues of internet connectivity and broadband supply, the law enforcement authorities would investigate cybercrime issues, while increasingly, the homeland security department would deal with cybersecurity issues.

5. The key multistakeholder institutions in the internet governance community are the Internet Governance Forum (IGF), Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), World Wide Web Consortium (W3C), and the Internet Society (ISOC). *See generally* CTR. FOR INT'L GOVERNANCE INNOVATION & THE ROYAL INSTITUTE FOR INT'L AFFAIRS, GLOBAL COMMISSION ON INTERNET GOVERNANCE: WHO RUNS THE INTERNET? (2016),

International Telecommunications Union (ITU)[6] and other specialised agencies of the United Nations (UN)),[7] and regional organisations.[8] Further, civil society organisations[9] and technology companies[10] play an instrumental role in internet governance. Principles of internet governance can be derived from multiple sources: declarations and resolutions of multilateral and multistakeholder bodies, standards and recommendations of multistakeholder bodies such as the Internet

---

https://www.cigionline.org/sites/default/files/documents/GCIG%20Volume%202%20WEB.pdf [https://perma.cc/G9KR-PKPA] (archived Mar. 13, 2019).

6. Since the 2012 proceedings of the World Conference on International Communications (WCIT-12), concerns have been raised regarding the increasing role of the ITU in internet governance. *See generally, e.g.*, RICHARD BENNETT, THE INFO. TECH. & INNOVATION FOUND., THE GATHERING STORM: WCIT AND THE GLOBAL REGULATION OF THE INTERNET (2012), http://www2.itif.org/2012-gathering-storm-wcit-regulations.pdf [https://perma.cc/Q7BE-L9SV] (archived Jan. 15, 2019); David P. Fidler, *Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations*, 17 INSIGHTS 6 (Feb. 7, 2013), https://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision [https://perma.cc/LJF4-STM5] (archived Jan. 15, 2019); Jemima Kiss, *ITU and Google faceoff at Dubai conference over future of the internet*, THE GUARDIAN (Dec. 3, 2012), https://www.theguardian.com/technology/2012/dec/03/telecoms-unitednations [https://perma.cc/L93M-KT9W] (archived on Jan. 15, 2019). However, other experts have argued that the International Telecommunication Regulations adopted at WCIT-12 did not deal with internet governance issues at all. *See, e.g.*, RICHARD HILL, THE NEW INTERNATIONAL TELECOMMUNICATION REGULATIONS AND THE INTERNET 35–68 (2014). Nonetheless, the ITU has been active in dealing with issues in cybersecurity and privacy through its recommendations, reports, as well as the annual Global Cybersecurity Index. *See, e.g.*, INT'L TELECOMM. UNION, PRIVACY IN CLOUD COMPUTING: ITU TECH. WATCH REP. (2012); INT'L TELECOMM. UNION, SERIES X: DATA NETWORKS, OPEN SYSTEM COMM. & SECURITY RECOMMENDATION ITU-T X.1205 (2008).

7. The U.N. General Assembly has adopted several resolutions on internet privacy and cybersecurity issues. *See, e.g.*, The Right to Privacy in the Digital Age, Seventy-First Session, U.N. Doc. A/C.3/71/L.39/Rev.1 (Nov. 16, 2016); The Right to Privacy in the Digital Age, Sixty-Ninth Session, U.N. Doc. A/C.3/69/L.26/Rev.1 (Nov. 19, 2014); G.A. Res. 68/16, The Right to Privacy in the Digital Age (Dec. 18, 2013); G.A. Res. 64/21, Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures (Mar. 17, 2010); G.A. Res. 58/199, Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures (Dec. 23, 2003); G.A. Res. 56/12, Combating the Criminal Misuse of Information Technologies (Jan. 23, 2002); G.A. Res. 55/63, Combating the Criminal Misuse of Information Technologies (Dec. 4, 2000).

8. Regional organizations including the Organisation for Economic Co-operation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC) have been involved in different aspects of internet policymaking. *See, e.g.*, Asia-Pacific Econ. Coop. [APEC], *APEC Privacy Framework* (Nov. 2004), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx [https://perma.cc/LQS2-PQT7] (archived Jan. 15, 2019); Org. for Econ. Coop. & Dev. [OECD], *OECD Principles for Internet Policy Making* (2014), https://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf [https://perma.cc/BB4Y-VXYS] (archived Jan. 15, 2019) [hereinafter OECD *Principles*].

9. *See* Madeline Carr, *Power Plays in Global Internet Governance*, 43 MILLENNIUM: J. INT'L STUD. 640, 656–58 (2015); Lauren Movius, *The Influence of Global Civil Society on Internet Governance Negotiations*, 43 FLA. COMM. J. 1, 1 (2015).

10. Carr, *supra* note 9.

Engineering Task Force (IETF)[11] and the Internet Governance Forum (IGF), and voluntary standards developed by civil society or private bodies.[12]

Despite these obvious differences between international trade law and internet governance, it would be imprudent to dismiss their linkage as a matter of mere theoretical interest. Several scholars have already studied the importance of cross-border data flows to boost the growth of trade in a digitalised world.[13] Good governance of the internet (such as a high degree of openness, efficiency, and stability)

---

11. The IETF circulates memos called Request for Comment (RFCs) which "contain technical and organizational notes about the Internet." *RFCs*, INTERNET ENG'G TASK FORCE, https://www.ietf.org/standards/rfcs/ (last visited Mar. 13, 2019) [https://perma.cc/S8AR-XTKK] (archived Feb. 5, 2019) [hereinafter *IETF RFCs*]. These memos touch upon different aspects of internet governance, particularly in relation to technical issues, but may also reflect opinions on policy and user issues. *See, e.g.*, Memorandum from S. Hambridge on Netiquette Guidelines (Oct. 1995), https://www.rfc-editor.org/rfc/pdfrfc/rfc1855.txt.pdf [https://perma.cc/V29R-AJ2X] (archived Jan. 15, 2019); Memorandum from the Internet Activities Board on Ethics and the Internet (Jan. 1989), https://tools.ietf.org/pdf/rfc1087.pdf [https://perma.cc/FM7A-NLS4] (archived Jan. 15, 2019); Memorandum from T. Dierks & C. Allen on The TLS Protocol (Jan. 1999), https://www.rfc-editor.org/rfc/pdfrfc/rfc2246.txt.pdf [https://perma.cc/V7ZQ-4DLZ] (archived Jan. 15, 2019).

12. *See, e.g.*, ELECTRONIC FRONTIER FOUND., MANILA PRINCIPLES ON INTERMEDIARY LIABILITY (2015), https://www.eff.org/files/2015/10/31/manila_principles_1.0.pdf [https://perma.cc/3G85-34A9] (archived Jan. 15, 2019); ELECTRONIC FRONTIER FOUND., INTERNATIONAL PRINCIPLES ON THE APPLICATION OF HUMAN RIGHTS TO COMMUNICATIONS SURVEILLANCE (2013), https://www.eff.org/files/necessaryandproportionatefinal.pdf [https://perma.cc/4PGP-47W5] (archived Jan. 15, 2019); GLOB. NETWORK INITIATIVE, PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY (2009), https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf [https://perma.cc/5MCR-3Y9E] (archived Jan. 15, 2019) (setting forth principles aimed at advancing freedom of expression and privacy in the Information and Communications Technology industry); INT'L STANDARDS ORG., CODE OF PRACTICE FOR PROTECTION OF PERSONALLY IDENTIFIABLE INFO. (PII) IN PUBLIC CLOUDS ACTING AS PII PROCESSORS (2008), https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en [https://perma.cc/YZ7S-9JJX] (archived Jan. 15, 2019).

13. *See, e.g.*, U.N. Conference on Trade and Development, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, U.N. Doc. UNCTAD/WEB/DTL/STICT/2016/1/iPub (2016); U.S. INT'L TRADE COMM'N, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES: PART 2 at 65 (2014), https://www.usitc.gov/publications/332/pub4485.pdf [https://perma.cc/G3AE-PHMY] (archived Jan. 15, 2019); Susan Stone et al., Org. for Econ. Coop. & Dev. [OECD], *Emerging Policy Issues: Localisation Barriers to Trade*, OECD Trade Policy Papers No. 180 (2015); Joshua Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, ISSUES IN TECH. INNOVATION, Feb. 2013, at 1, https://www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf [https://perma.cc/6538-AFW7] (archived Jan. 16, 2019); James Manyika et al., *Digital globalization: The new era of global flows*, MCKINSEY GLOBAL INST. (Mar. 2016), http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows [https://perma.cc/Q2XS-M7M5] (archived Jan. 15, 2019).

facilitates the use of the internet for trade.[14] With the rapid expansion of the global market for digital services, measures that obstruct the internet (e.g., restrictions on data flows or imposition of proprietary or indigenous technical standards) also constitute barriers to trade and, therefore, may be subject to scrutiny under international trade law.

The relationship between international trade law and internet governance is increasingly being explored and evaluated.[15] For instance, in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP),[16] the parties acknowledged the importance of internet-related policy issues to digital trade and thereby introduced binding provisions on cross-border flows of information and data localisation and other disciplines on personal data protection, spam, online consumer protection, and cybersecurity cooperation.[17] Further, stakeholders in the internet governance community also recognise the significance of international trade agreements in supporting "a free and open [i]nternet, which is just, fair, and development oriented and furthers the interoperability of [i]nternet information services" and its positive ramifications on "social and economic development."[18] However, others have noted the possible discord between trade rules and internet governance as trade agreements are used by powerful stakeholders in a secretive manner to impose internet openness,[19] without due regard to the regulatory

---

14. *See* HARSHA VARDHAN SINGH ET AL., GOVERNANCE OF INTERNATIONAL TRADE AND THE INTERNET: EXISTING AND EVOLVING REGULATORY SYSTEMS 2 (2016), https://www.cigionline.org/sites/default/files/gcig_no32web.pdf [https://perma.cc/6CP4-RBHB] (archived Jan. 16, 2019).

15. *See generally, e.g.*, Mira Burri, *The World Trade Organization as an Actor in Global Internet Governance*, *in* THE INSTITUTIONS OF GLOBAL INTERNET GOVERNANCE (William J. Drake & Mira Burri eds., 2016); Susan Aaronson, *Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security*, 14 WORLD TRADE REV. 676 (2015); Luca Belli & Marilia Marcel, *The Quiet Rapprochement of Internet Governance and Trade Policy*, DIPLO (Oct. 14, 2016), https://www.diplomacy.edu/blog/quiet-rapprochement-internet-governance-and-trade-policy [https://perma.cc/Z66G-TBBY] (archived Jan. 15, 2019).

16. Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Mar. 8, 2018, https://www.mfat.govt.nz/assets/CPTPP/Comprehensive-and-Progressive-Agreement-for-Trans-Pacific-Partnership-CPTPP-English.pdf [https://perma.cc/5CDR-V8K6] (archived Feb. 26, 2019) [hereinafter CPTPP].

17. For discussion of these provisions, see 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. 30, 36–55 (2017).

18. U.N. Internet Governance Forum Dynamic Coalition on Trade & the Internet, *Resolution on Transparency*, ELECTRONIC FRONTIER FOUND. (Dec. 19, 2017), https://www.eff.org/files/2017/12/19/igf_dc_trade_resolution_on_transparency.pdf [https://perma.cc/LPL2-LVS2] (archived Jan. 17, 2019).

19. In Tae Yoo, *New Wine into Old Wineskins? Regime Diffusion by the Powerful from International Trade into Cyberspace*, 32 PAC. FOCUS 375, 376 (2017).

autonomy necessary for domestic regulation of cyberspace.[20] To date, trade tribunals have not comprehensively investigated the conflict between trade and internet policy.[21] Therefore, to understand better how these two fields interface, greater clarity is required regarding how existing (and future) trade rules can be applied and interpreted in trade disputes concerning internet and internet-enabled services.

When applying international trade agreements such as the General Agreement on Trade in Services (GATS)[22] to measures restricting data flows, a delicate balance needs to be struck between liberalising trade in digital services and preserving domestic policy goals, including regulating online content in the public interest, protecting privacy of citizens, and reducing cybercrimes.[23] Although such measures are implemented domestically, they have a direct impact on a globally interconnected network. For example, data localisation laws may affect how data is routed through the network as well as the efficiency of cross-border data flows.[24] When examining such measures under GATS, the assessment will often involve fundamental issues related to internet governance. For instance, under GATS Article XIV, a trade tribunal may need to determine the necessity of a data localisation measure to achieve privacy or cybersecurity.[25] Therefore, even applying international trade law

---

20. JANE KELSEY & BURCU KILLIC, BRIEFING ON US TISA PROPOSAL ON E-COMMERCE, TECHNOLOGY TRANSFER, CROSS-BORDER DATA FLOWS AND NET NEUTRALITY 15–16 (2014), http://www.world-psi.org/sites/default/files/documents/research/briefing_on_tisa_e-commerce_final.pdf [https://perma.cc/B3BV-QSBV] (archived Jan. 15, 2019); *see also* Svetlana Yakovleva & Kristiana Irion, *The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection?*, 2 EUR. DATA PROTECTION L. REV. 191, 202–07 (2016) (describing potential conflicts between the European Union's regulation of data protection and its obligations under international trade agreements).

21. In *US—Gambling*, the World Trade Organization Appellate Body did not dismiss the United States' argument that they could regulate online services on public morals, but rather rejected the measure because it was arbitrary and discriminatory in nature. *See* Appellate Body Report, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WTO Doc. WT/DS285/AB/R (adopted Apr. 20, 2005) [hereinafter *US—Gambling*]. In *China—Publications and Audiovisual Services*, the AB skirted any discussion on China's role in internet censorship. *See* Appellate Body Report, *China—Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WTO Doc. WT/DS363/AB/R (adopted Jan. 19, 2010).

22. General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1867 U.N.T.S. 154 [hereinafter Marrakesh Agreement].

23. *See* Andrew Mitchell & Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 YALE J.L. & TECH. 182, 201–05 (2017).

24. *See infra* Part II.B.

25. *See* DANIEL CROSBY, ANALYSIS OF DATA LOCALIZATION MEASURES UNDER WTO SERVICES TRADE RULES AND COMMITMENTS (2016), http://e15initiative.org/wp-content/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf [https://perma.cc/9UTK-

requires clarity regarding the fundamental principles governing data flows.

This Article argues that three principles of internet governance are most pertinent to internet data flows: *internet openness*, *internet security*, and *internet privacy*. Though these terms are frequently used in internet governance literature, different stakeholders attribute different meanings to these terms. This Article has defined and explained each of these principles by distilling and assimilating important and relevant values and ideas from different soft law instruments, policy documents, and scholarship in internet governance. Since the internet is a "multilayered framework" governed by several institutions, data transfers through the internet require coordination among different stakeholders, and interoperability of policies and technical protocols across different layers.[26] The principles of internet openness, security, and privacy provide important guiding tools to different stakeholders operating in different layers to ensure the interoperability and security of data flows. This Article further explores how these three principles are relevant to international trade law, particularly if it can contribute to or facilitate achieving these principles. However, as international trade law is not the appropriate platform to resolve issues related to human rights, this Article does not directly evaluate the political connotations of the principles of internet openness, security, and privacy. For example, measures restricting data flows cannot be challenged before trade tribunals because they violate human rights recognised in domestic or international non-trade instruments (e.g., the freedom of expression).[27]

Part 0 explains how measures restricting cross-border data flows operate in practice as well as the different types of data restrictive measures with a trade-restrictive effect. Part 0 focuses on three key principles in internet governance instrumental to data flows—internet openness, security, and privacy—arguing that these principles are complementary in nature. Part 0 evaluates the extent to which these three principles align with rules in international trade law, as well as how they can be used in context of applying, interpreting, and

---

HJUJ] (archived Jan. 16, 2019); Susannah Hodson, *Applying WTO and FTA Disciplines to Data Localization Measures*, WORLD TRADE REV. 1–29 (2018); Carla L. Reyes, *WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive*, 12 MELBOURNE J. INT'L L. 1, 24–25 (2011).

26. JOHN PALFREY & URS GASSER, INTEROP: THE PROMISE AND PERILS OF HIGHLY INTERCONNECTED SYSTEMS 5–6 (2012); ROLF H. WEBER, LEGAL INTEROPERABILITY AS A TOOL FOR COMBATTING FRAGMENTATION (2014), https://www.cigionline.org/sites/default/files/gcig_paper_no4.pdf [https://perma.cc/PPF8-Z8UK] (archived Jan. 20, 2019).

27. Marrakesh Agreement, *supra* note 22, Annex 2, art. 7.1,; *see also* Joost Pauwelyn, *Squaring Free Trade in Culture with Chinese Censorship: The WTO Appellate Body Report on China—Audiovisuals*, 11 MELBOURNE J. INT'L L. 119, 132–33 (2008) (describing how the WTO Appellate Body found China's censorship policies did not violate GATT without even mentioning the possibility that China was violating the right to free speech).

reforming international trade law. Part V discusses the possibility of bringing together the multilateral approach of international trade law with the multistakeholder approach in internet governance with regard to regulating cross-border data flows. The Article concludes that given the growing importance of digital trade, international trade law should not be isolated from internet governance. Understanding the linkages between the two fields is timely and crucial to: (i) ensure a more meaningful role for trade disciplines in addressing digital trade issues such as cross-border data flows; and (ii) build a comprehensive and balanced approach to govern cross-border data flows at the global level.

II. UNDERSTANDING MEASURES RESTRICTING CROSS-BORDER DATA FLOWS

The internet is a multilayered technology consisting of a physical layer containing the physical infrastructure-carrying data packets; the network layer consisting of routing protocols that determine the path of data packets; the transport layer consisting of protocols that ensure sequencing and delivery of data packets (e.g., the Transmission Control Protocol (TCP)); and finally, the applications layer consisting of the programmes that users see while using the internet.[28] These different layers should be interoperable to enable data flows through the internet.[29] This Part addresses what constitutes "data" and "cross-border data flows" along with explaining the different types of measures restricting data flows.

A. *The "Restrictive" Element of "Cross-Border Data Flows"*

1. Types of Data

Data flows are intrinsic to all digital services. For example, using an electronic commerce platform can involve a "complex web of data flows" between servers of different services (e.g., e-payment services,

---

28. WILLIAM J. DRAKE ET AL., INTERNET FRAGMENTATION: AN OVERVIEW 13 (2016); *see also* YOCHAI BENKLER, THE WEALTH OF NETWORKS 396, 412–13, 439 (2006); Jose MA. Emmanuel A. Caral, *Lessons from ICANN: Is Self-Regulation of the Internet Fundamentally Flawed?*, 12 INT'L J.L. & TECH. 1, 1, 9–13 (2012); Memorandum from Internet Architecture Board on Technical Considerations for Internet Service Blocking and Filtering 12 (Mar. 2016), https://tools.ietf.org/pdf/rfc7754.pdf [https://perma.cc/KSX4-4Q46] (archived Feb. 5, 2019); Memorandum from R. Braden on Requirements for Internet Hosts—Communication Layers 8–9 (Oct. 1989), https://tools.ietf.org/pdf/rfc1122.pdf [https://perma.cc/LS8P-HYEB] (archived Feb. 5, 2019).

29. PALFREY & GASSER, *supra* note 26, at 5.

the e-commerce portal) and the customer's computer or digital device.[30] Here, "data" (contained in data packets transferred through the internet) refers to both the digitised content in the service as well as the data generated when users access or use digital services, applications, and websites. Thus, "data flows," as used in this Article, refers to both the provision of the digital service itself (as it is encoded in bits and bytes) and the data flows generated while using a service, such as business data or user-generated data.[31]

Some scholars compartmentalise data into different categories, and, further, suggest that different categories necessitate differentiated treatment. For example, Nivedita Sen classifies data into personal data, referring to data related to individuals; company data, referring to data flowing between corporations; business data, referring to digitised content such as software and audiovisual content; and social data, referring to behavioural patterns determined using personal data.[32] Susan Ariel Aaronson and Patrick Leblond categorise data into personal data, public data, confidential business data, machine-to-machine data, and metadata, although they do not specifically define each of these terms.[33] Usually, personal data and confidential business data are protected more strongly in most domestic laws than anonymised and day-to-day business data.[34]

In practice, varied legal treatment of data categories is difficult to implement due to the overlapping nature of data categories. First, personal data and other types of data (non-personal data) cannot always be neatly distinguished in practice; for example, big data technologies can help identify individuals in anonymised datasets.[35] Similarly, metadata combined with geolocation technologies can be

---

30. Nivedita Sen, *Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path,* 21 J. INT'L ECON. L. 323, 323–24 (2018).

31. W. KUAN HON, DATA LOCALIZATION LAWS AND POLICY 72 (2017); AMY PORGES & ALICE ENDERS, DATA MOVING ACROSS BORDERS: THE FUTURE OF DIGITAL TRADE POLICY 1 (2016), http://e15initiative.org/wp-content/uploads/2015/09/E15-Digital-Economy-Porges-and-Enders-Final.pdf [https://perma.cc/M78G-B9ZN] (archived Jan. 16, 2019).

32. Sen, *supra* note 30, at 22.

33. Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO*, 2 J. INT'L ECON. L. 1, 5–6 (2018).

34. For example, in a proposed regulatory framework for cross-border flows of non-personal data, the European Commission established a fairly liberal system of self-regulation combined with a principles-based approach for non-personal data flows in the Digital Single Market while continuing to have very stringent standards for personal data processing. *See Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-Personal Data in the European Union*, pmbl., art. 7, COM (2017) 495 final (Sept. 13, 2017).

35. Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74, 78 (2013).

used to identify intimate details of an individual's life.[36] Further, personal data may be a component of business or company data—for example, employee records. Second, personal data does not only have social value but also business value, as it is traded via various digital services and drives the digital economy.[37] In fact, 75 percent of digital data today is generated by internet users, and largely falls within the scope of personal data.[38] Thus, limiting data flows to non-personal data will not be meaningful or sufficient for enabling digital services. Finally, certain policy concerns are common to both categories of data; for example, data security concerns affect both personal and non-personal data.

2. Cross-Border versus Domestic Data Flows

The global, interconnected, and instantaneous nature of data flows through the internet obfuscates the distinction between cross-border and domestic data flows. Data flows are driven by protocols that determine the most efficient path for internet traffic without consideration of geographical boundaries.[39] In cloud computing, typically, data packets are broken down into smaller chunks, which are stored and routed through multiple servers to ensure data security (this process is called sharding).[40] Further, even if data is finally stored in one server, data usually transits through multiple servers across countries during routine processing.[41] Thus, regulating data flows based on territorial boundaries (for example, data should be stored, processed, and routed through one's borders) is both counterintuitive and inefficient.

However, when applying international trade to measures that regulate cross-border data flows, the physical locations of the data, the

---

36. Article 29 Data Protection Working Party, *Opinion 2/2017 on Data Processing at Work*, at 10 (June 8, 2017), http://ec.europa.eu/newsroom/document.cfm?doc_id=45631 [https://perma.cc/46D2-NECA] (archived Jan. 16, 2019).

37. *See* Svetlana Yakovleva, *Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*, 17 WORLD TRADE REV. 477, 478 (2018) (recognizing that personal data can be viewed as both "a trade commodity and as an asset with societal value").

38. TIM COOPER & RYAN LASALLE, GUARDING AND GROWING PERSONAL DATA VALUE 10 (2016), https://www.accenture.com/_acnmedia/PDF-4/Accenture-Guarding-and-Growing-Personal-Data-Value-POV-Low-Res.pdf [https://perma.cc/4TBR-MKNU] (archived Jan. 16, 2019).

39. Rus Schuler, *How Does the Internet Work?*, STANFORD (2002), https://web.stanford.edu/class/msande91si/wwwspr04/readings/week1/InternetWhitepaper.htm [https://perma.cc/492G-YUP4] (archived Jan. 16, 2019).

40. Jeeyoung Kim, *How Sharding Works*, MEDIUM (Dec. 6, 2014), https://medium.com/@jeeyoungk/how-sharding-works-b4dec46b3f6 [https://perma.cc/N4YV-8ZH7] (archived Jan. 16, 2019).

41. KUAN HON, *supra* note 31, at 74–76.

supplier, and the internet user are relevant to determine if there is cross-border trade involved.[42] Thus, any data generated within a specific country and flowing outside its borders, data generated abroad flowing into the domestic network of another country, or a combination of the two, falls within the scope of cross-border data flows. This in turn implies that majority of data flows pertaining to digital services are cross-border in nature (at least during some stage of data processing) and could potentially be subject to members' obligations contained in different international trade agreements such as GATS.

B. *Types of Data Restrictive Measures*

Measures restricting data flows can affect different layers of the internet. Certain measures directly affect the physical or transport layer of the internet. For example, the Chinese government reportedly exercises enormous control over the physical infrastructure through which internet traffic is exchanged (or Internet Exchange Points) to prevent circulation of banned or offensive online content in Chinese cyberspace.[43] Similarly, a data localisation measure requiring local routing would interfere with transfer protocols that route internet traffic based on efficiency rather than geographic location. Other restrictive measures do not directly interfere with the technical or physical infrastructure of the network, but impose specific requirements on digital service providers, for instance, by imposing conditional requirements related to privacy or cybersecurity that might affect how these digital services are offered.[44]

Cross-border data flows can be restricted in various ways from blocking data flows through internet outages or deliberate attacks on the Domain Name System[45] to more specific measures such as data

---

42. Cross-border supply of digital services occurs through four modes: Mode 1 ("from the territory of one Member into the territory of any other Member"), Mode 2 ("in the territory of one Member to the service consumer of any other Member"), Mode 3 ("by a service supplier of one Member, through commercial presence in the territory of any other Member" and Mode 4 ("by a service supplier of one Member, through presence of natural persons of a Member in the territory of any other Member"). *See* Marrakesh Agreement, *supra* note 22, art. I(2).

43. Nikhil Sonnad & Keith Collins, *How Countries like China and Russia are Able to Control the Internet*, QUARTZ: CHOKE POINTS (Oct. 5, 2016), https://qz.com/780675/how-do-internet-censorship-and-surveillance-actually-work/ [https://perma.cc/8S7K-FCWZ] (archived Jan. 16, 2019).

44. For example, the GDPR only allows transfer of data to those countries which have met an adequacy requirement or where the service providers provide other additional undertakings regarding data transfers such as the use of Binding Corporate Rules and Standard Contractual Clauses.

45. The Domain Name System or DNS is "a database that stores all of the domain names and corresponding IP numbers for a particular top-level domain (TLD) such as .com or .net. *See What is DNS (Domain Name System)?*, VERISIGN, https://www.verisign.com/en_US/website-presence/online/domain-name-system/index.xhtml (last visited Jan. 20, 2019) [https://perma.cc/TZ9G-2N93] (archived

localisation. Additionally, service providers can use tools such as geo-blocking to limit their services to specific countries. Martina Ferracane classifies restrictions on cross-border data flows into two categories: "strict" and "conditional."[46] Strict restrictions on cross-border data flows include local storage requirements,[47] local storage and processing requirements,[48] and bans on data transfer[49] (i.e., local storage, local processing, and local access requirements).[50] Such measures are typically termed as data localisation measures.[51] Conditional restrictions consist of measures where data flows are allowed subject to conditions imposed on the recipient country or the data controller/processor.[52] In practice, a measure may incorporate both strict and conditional restrictions. For example, the Russian data localisation law requires local storing and processing,[53] but also allows

---

Jan. 16, 2019). The DNS identifies and locates computer systems and resources on the Internet. *See id.*

46. Martina F. Ferracane, *Restrictions on Cross-border Data Flows: A Taxonomy* 4 (European Ctr. for Int'l. Pol. Econ. Working Paper 1/2017, 2017), https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf [https://perma.cc/R5QP-7WW7] (archived Jan. 16, 2019).

47. *See, e.g.*, Federal'nyi Zakon o Vnesenii Izmenenii V Otdel;nyye Zakonodatel'nyye Akty Rossiiskoy Federatsii V Chasti Utochneniya Poryadka Obrabotki Personal'nykh Dannykh V Informatsionno-Telekommunikatisonnykh Setyakh [Federal Law on Amending Some Legislative Acts of the Russian Federation in as much as it Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunications Networks], FEDERAL'NYI ZAKON [FZ] [Federal Law] 2014, No. 242-FZ, art. 2 (Rus.).

48. The EU defines data processing to include data storage. *See* W. Kuan Hon et al., *Policy, Legal and Regulatory Implications of a Europe-only Cloud*, 24 INT'L J.L. & INFO. TECH. 251, 259 (2016).

49. *See, e.g.*, Law on Payment and Security Settlement Systems, Payment Services and Electronic Money Institutions, Turkish Civil Code, Law No.: 6493 art. 23 [R.G.], 20 June 2013; Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, s 30.1 (Can.); Personal Information International Disclosure Protection Act, N.S. 2006, s 5 (Can.).

50. Ferracane, *supra* note 46, at 4.

51. However, Chander and Le define data localisation more broadly to include any measure "that specifically encumber(s) the transfer of data across national borders," thus including both de jure and de facto measures. Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 680 (2015); *see also* Mitchell & Hepburn, *supra* note 23, at 188–95.

52. Ferracane, *supra* note 46, at 5.

53. Federal'nyi Zakon o Vnesenii Izmenenii V Otdel;nyye Zakonodatel'nyye Akty Rossiiskoy Federatsii V Chasti Utochneniya Poryadka Obrabotki Personal'nykh Dannykh V Informatsionno-Telekommunikatisonnykh Setyakh [Federal Law on Amending Some Legislative Acts of the Russian Federation in as much as it Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunications Networks], FEDERAL'NYI ZAKON [FZ] [Federal Law] 2014, No. 242-FZ, art. 2 (Rus.).

conditional data transfer to countries that meet certain international standards.[54]

Measures restricting data flows can also be examined in light of the nature of the measure and its underlying objective. Certain measures restrict data flows based on the nature or content of the digital service and underlying data flows—for example, preventing supply of digital services that contain politically or culturally sensitive or banned content.[55] Another tool used by China to ensure a clean internet environment in the country is restricting the supply of Virtual Private Network (VPN) services domestically.[56] Similarly, South Korea bans cross-border transfer of mapping data, which in turn reduces business opportunities for applications such as Google Maps that use geolocation and mapping data.[57] Additionally, it is possible that a government may ban digital services that contain infringing content in line with its domestic intellectual property rights law.

In contrast, certain measures may not be targeted at the nature or content of data but the way it is stored, transferred, processed, and/or secured from unauthorised intrusion such as data localization measures.[58] Here, the primary policy rationale behind the data-restrictive measure is to protect the privacy of individuals or the security of data or the network. One example of the same is the General Data Protection Regulation (GDPR) of the European Union, which imposes various conditions on data controllers and processors in course of processing and transferring personal data of EU residents.[59] In order to achieve compliance with this regulation, several foreign service

---

54. Federal'nyi Zakon o Zashchite Personal'nykh Dannykh [Federal Law on Data Protection, FEDERAL'NYI ZAKON [FZ] [Federal Law] 2006, No. 152-FZ, arts. 3.1, 12.

55. *See, e.g.*, Singapore Internet Code of Practice, art. 4, Nov. 1, 1997, https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/content-and-standards-classification/video-games/policiesandcontentguidelines_internet_internecodeofpractice.pdf?la=en [https://perma.cc/64ZU-PXWE] (archived Feb. 5, 2019); *see also* Computer Information Network and Internet Security, Protection and Management (promulgated by Ministry Pub. Sec., Dec. 30, 1997), arts. 4–6, http://www.lehmanlaw.com/resource-centre/laws-and-regulations/ information-technology/computer-information-network-and-internet-security-protection-and-management-regulations-1997.html (China) [https://perma.cc/K7T8-QBCC] (archived Jan. 16, 2019).

56. MIIT Notice on Cleaning Up and Regulating the Internet Access Service Market (issued by Ministry of Indus. & Info. Tech., Jan. 17, 2017), http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c5471946/content.html [https://perma.cc/9YSC-NFAX] (archived Feb. 5, 2019) (China).

57. *See* Julia Yoon, *South Korean Data Localization: Shaped by Conflict*, UNIV. WASH, HENRY M. JACKSON SCH. INT'L STUD. (Feb. 28, 2018), https://jsis.washington.edu/news/south-korean-data-localization-shaped-conflict/ [https://perma.cc/3WF6-GRD8] (archived Jan. 16, 2019).

58. *See* Chander & Le, *supra* note 51 (defining data localization measures).

59. *See generally* Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the 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), 2016 O.J. (L 119) [hereinafter EU Data Protection Regulation].

providers have had to relocate or build new data centers in the EU.[60] Another example is the Russian data localization law, which, as per experts, will result in a significant increase in compliance costs for foreign cloud suppliers while providing a major boost to the domestic cloud industry.[61] Thus, in practice, measures restricting data flows can have more than one policy rationale, including a hidden protectionist intent.[62] This Part explored the various types of data restrictive measures and the multiple policy rationales informing them. Given the complexity of data restrictive measures, and the ambiguity in the regulatory framework governing data flows, significant challenges exist in identifying protectionist or excessive data restrictions from legitimate ones. The next part of the Article builds further on this debate by identifying and explaining the principles of internet governance that can be applied to regulation of data flows.

III. INTERNET GOVERNANCE PRINCIPLES UNDERLYING DATA FLOWS

This Part identifies the source and content of the fundamental principles in internet governance that apply to data flows. This Article terms these three fundamental principles as *internet openness*, *internet security*, and *internet privacy*. These three principles are presented as informative and aspirational tools rather than fixed thresholds, thus acknowledging that openness and security of the internet network are matters of degree.[63] Examples are also provided of how different

---

60. *See, e.g.*, Maria Korolov, *It's Cool, It's Well Wired, and It's Staying in the EU*, DATA CTR. KNOWLEDGE (Feb. 6, 2018), https://www.datacenterknowledge.com/europe/it-s-cool-it-s-well-wired-and-it-s-staying-eu [https://perma.cc/PDB5-6YSF] (archived Jan. 16, 2019).

61. Leonid Ragozin & Michael Riley, *Putin Is Building Great Russian Firewall*, BLOOMBERG BUSINESSWEEK (Aug. 26, 2016, 8:00 PM), https://www.bloomberg.com/news/articles/2016-08-26/putin-is-building-a-great-russian-firewall [https://perma.cc/X9AY-8YUN] (archived Jan. 16, 2019); Jason Verge, *Firms Rethink Russian Data Center Strategy, as Data Sovereignty Law Nears Activation*, DATA CTR. KNOWLEDGE (July 21, 2015), http://www.datacenterknowledge.com/archives/2015/07/21/russian-data-localization-law-spurs-data-center-strategy-changes [https://perma.cc/5C5E-X6A3] (archived Jan. 16, 2019).

62. Jonah Force Hill, *A Balkanized Internet? The Uncertain Future of Global Internet Standards*, GEO. J. INT'L AFF., 49, 49 (2012).

63. Org. for Econ. Coop. & Dev. [OECD], Comm. on Dig. Econ. Policy, *Economic and Social Benefits of Internet Openness*, at 15, DSTI/ICCP (2015)17/FINAL (June 2, 2016) https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2015)17/FINAL&docLanguage=En [https://perma.cc/M9FT-U3LH] (archived Jan. 16, 2019) [hereinafter OECD *Internet Openness*]; *see also* DRAKE, *supra* note 28, at 10; INTERNET SOC'Y, UNDERSTANDING SECURITY AND RESILIENCE OF THE INTERNET 3 (2013), https://www.internetsociety.org/wp-content/uploads/2017/08/bp-securityandresilience-20130711.pdf [https://perma.cc/RL4J-7PZD] (archived Jan. 16, 2019) [hereinafter INTERNET SOC'Y].

stakeholders implement these principles in practice. Finally, this Part argues that the principles of internet openness, security, and privacy operate as complementary and interdependent principles. In other words, these three principles need to be implemented simultaneously to achieve balance, coherence, and predictability in the regulation of data flows. Principles of internet openness, security, and privacy often have strong human rights and political connotations. For example, internet openness is often considered synonymous with freedom of expression in an online context;[64] internet security is linked to national security and prevention of cyberwarfare;[65] and internet privacy is linked to observance of due process and human rights.[66]

The discussion below alludes to the global and multistakeholder nature of the internet. However, individual governments implement laws and regulations on the internet and cross-border data flows based on their domestic policy objectives, which may or may not align with principles of internet openness, security, and privacy. Where this conflict exists, the global framework for data flows becomes fragmented, causing disruption to different kinds of economic and social activities conducted through the internet.

A. *The Principle of Internet Openness*

1. Internet Openness Requires Free Flow of Data

The essence of the principle of internet openness is the "global free flow of data across the network" without unnecessary disruptions or controls.[67] In other words, the higher the degree of openness of the internet, the more easily and efficiently data packets are exchanged by devices connected to the network. The principle of internet openness can be linked to the fundamental nature of the internet (i.e., an open

---

64. Laura DeNardis, *One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation*, *in* GLOBAL COMMISSION ON INTERNET GOVERNANCE 4–5 (Ctr. for Int'l Governance Innovation & Chatham House, Paper Ser. No. 37, July 2016), https://www.cigionline.org/sites/default/files/gcig_no.38_web.pdf [https://perma.cc/GB7E-H9H5] (archived Jan. 16, 2019).

65. *See, e.g.*, Permanent Reps. of China, the Russian Federation, Tajikistan, and Uzbekistan, Letter dated Sept. 12, 2011 from the Permanent Reps. of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/66/359 (Sept. 14, 2011).

66. U.N. Internet Governance Forum, 8th Internet Governance Forum, Focus Session: Internet Governance Principles (Oct. 23, 2013) http://www.intgovforum.org/multilingual/content/focus-session-internet-governance-principles [https://perma.cc/X9W2-MD4J] (archived Feb. 24, 2019).

67. Sarah Box, *Internet Openness and Fragmentation: Toward Measuring the Economic Effects*, *in* GLOBAL COMMISSION ON INTERNET GOVERNANCE 1 (Ctr. for Int'l Governance Innovation & Chatham House, Paper Ser. No. 36, May 2016), https://www.cigionline.org/sites/default/files/gcig_no.36_web.pdf [https://perma.cc/ZVS6-3D9H] (archived Jan. 16, 2019); *see also* OECD *Internet Openness*, *supra* note 63, at 12.

and global network working on the architectural principles of "efficiency" and "non-discrimination").[68] Engineers refer to this architecture as the end-to-end principle in which "information pushed into one end of the internet should come out the other without modification," thus ensuring seamless connectivity.[69] In other words, the internet transfers information through the most efficient route, but the routing protocols do not "know" anything about the content of the data packets, and hence "cannot by architecture . . . discriminate or differentiate traffic generated by different applications."[70] Put differently, the internet is nothing but a "big, fat, dumb, digital pipe,"[71] with the applications residing at the ends of the network possessing the intelligence to process the content of the data packets.[72] The two primary consequences of this end-to-end architecture are "protection of innovation" and "provision of reliability and robustness."[73]

The principle of internet openness is often confused with the concept of *net neutrality*.[74] Since the open architecture of the internet is based on an end-to-end design, the concepts of internet openness and net neutrality are interlinked but not identical. Net neutrality is related to competition conditions within domestic markets such as preventing broadband providers from blocking specific services or devices, slowing down the speed of specific types of internet traffic (throttling), or favouring certain types of internet traffic such as those belonging to their affiliates or for money (paid prioritisation).[75] Net neutrality contributes to internet openness as it prevents arbitrary and

---

68. GCIG ONE INTERNET, *supra* note 1, at vi.

69. Simson Garfinkel, *The End of End-to-End?*, MIT TECH. REV. (July 1, 2003), https://www.technologyreview.com/s/401966/the-end-of-end-to-end/ [https://perma.cc/CHN5-L8QH] (archived Jan. 16, 2019); *see also* Memorandum from Brian Carpenter on Architectural Principles of the Internet 2 (June 1996), https://tools.ietf.org/pdf/rfc1958.pdf [https://perma.cc/GC3J-SWUM] (archived Feb. 5, 2019); Memorandum from J. Kempf & R. Austein on The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture (Mar. 2004), https://tools.ietf.org/pdf/rfc3724.pdf [https://perma.cc/GHH9-WG4G] (archived Feb. 5, 2019) [hereinafter Memorandum from J. Kempf]. *But see* Anthony Rutkowski, *Weaponizing the Internet Using the "End-to-end Principle" Myth*, CIRCLEID *(*Nov. 12, 2017), http://www.circleid.com/posts/20171112_weaponizing_the_internet_using_the_end_to_end_principle_myth/ [https://perma.cc/P4UR-5YWU] (archived Jan. 16, 2019).

70. Lawrence B. Solum, *Models of Internet Governance*, *in* INTERNET GOVERNANCE: INFRASTRUCTURE AND INSTITUTIONS 48, 63–64 (2009).

71. Garfinkel, *supra* note 69.

72. Solum, *supra* note 70, at 58.

73. DAVID D. CLARK ET AL., TUSSLE IN CYBERSPACE: DEFINING TOMORROW'S INTERNET 8 (2002); Memorandum from J. Kempf, *supra* note 69, at 8.

74. *See, e.g.*, Restoring Internet Freedom, FED. COMMC'N COMM'N, https://www.fcc.gov/restoring-internet-freedom (last visited Mar. 13, 2019) [https://perma.cc/CN6S-MNQX] (archived Feb. 24, 2019); *see also* TIM WU, A PROPOSAL FOR NET NEUTRALITY (2002).

75. Restoring Internet Freedom, *supra* note 74.

discriminatory blocking of digital services.[76] Conversely, an open internet enables internet users to "make their own choices about applications and services to use and which lawful content they want to access, create, or share with others,"[77] in turn supporting net neutrality. However, the concept of internet openness is much broader than net neutrality as it relates to openness of the global rather than the domestic network.

The Organisation for Economic Co-operation and Development (OECD) refers to two additional facets of internet openness: economic openness and social openness.[78] Economic openness refers to the "ability of the users to get online and to use the internet to enhance their economic opportunities and put them to productive uses."[79] Economic openness is determined by several factors such as the degree of competition and the availability and pricing of internet services in particular markets.[80] Governments often protect their domestic digital sectors by placing restrictions on internet services through various means such as data localisation, the imposition of indigenous technical standards, geo-restrictions, or foreign internet services bans.[81] Social openness refers to the nonpecuniary opportunities arising out of internet openness, including keeping in touch with people, accessing information, and expressing ideas on topics of interest.[82]

2. Free Flow of Information Is Recognised Internationally

Several declarations and soft law instruments recognise the importance of the free flow of information.[83] "Free flow of information" is the core idea of internet openness—data should be able to flow across

76. OECD *Internet Openness*, *supra* note 63, at 24.

77. Susan Ariel Aaronson & Rob Maxim, *Trade and the Internet: Policies in the US, the EU and Canada*, *in* HANDBOOK OF THE INTERNATIONAL POLITICAL ECONOMY OF TRADE 550, 551 (2014).

78. *See* OECD *Internet Openness*, *supra* note 63, at 24.

79. *Id.*

80. *Id.*

81. GCIG ONE INTERNET, *supra* note 1, at 52.

82. OECD *Internet Openness*, *supra* note 63, at 16.

83. World Summit on Info. Soc'y, *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6(Rev. 1)-E (Nov. 18, 2005), http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html [https://perma.cc/GR24-4NVG] (archived Jan. 16, 2019) [hereinafter *Tunis Agenda*]; World Summit on Info. Soc'y, *Declaration of Principles – Building the Information Society: A Global Challenge in the New Millennium*, WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003) http://www.itu.int/net/wsis/docs/480ecogn/official/dop.html [https://perma.cc/5TEW-MXJA] (archived Jan. 16, 2019). Free flow of information is recognised as a human right in many treaties. *See* G.A. Res. 2200A (XXI), art. 19, International Covenant on Civil and Political Rights (Mar. 23, 1976) (only binding on signatories); G.A. Res. 217, art. 19, Universal Declaration of Human Rights (Dec. 10, 1948) (not binding, but some scholars recognise it as customary international law); *see also* Lisa J Damon, *Freedom of Information versus National Sovereignty: The Need for a New Global Forum for the Resolution of Transborder Data Flow Problems*, 10 FORDHAM INT'L L.J. 262, 268–71 (1986).

the network without unnecessary or unreasonable disruptions.[84] However, a completely open and free internet, as discussed below, is neither desirable nor technically feasible. The Internet Society refers to different aspects of internet openness as "internet invariants" (or fundamental, unchanging features of the internet): (i)"the global reach and integrity" of the internet that is preserved through "end-to-end architecture" of the internet network; (ii) "universal accessibility"; (iii) "permission-less innovation," enabling digital entrepreneurship and unhindered innovation on the internet; and (iv) "inter-networking" via "open standards, enabling transparency in standard-setting."[85]

Several intergovernmental bodies have recognised internet openness in different declarations and policy recommendations. In 2011, the G8 group of countries adopted the Deauville Declaration, which supports "openness, transparency and freedom of the [i]nternet" and "non-discrimination and fair competition" on the internet.[86] The OECD recognises that "promot[ing] and protect[ing] the global free flow of information," "promot[ing] the open, distributed and interconnected nature of the [i]nternet," and "promot[ing] and enabl[ing] the cross-border delivery of services" are fundamental principles of internet policymaking.[87] The OECD reaffirmed these principles in the 2016 Cancun Declaration.[88] One of the founding principles of internet governance in the NETMundial Multistakeholder Statement was the free flow of information, acknowledging that internet users have the "right to access, share, create and distribute information on the internet, consistent with the rights of authors and creators."[89] Various bilateral statements have also expressed support for the principle of internet openness.[90]

---

84. Box, *supra* note 67.

85. *Internet Invariants: What Really Matters*, INTERNET SOC'Y (Feb. 3, 2012), https://www.internetsociety.org/internet-invariants-what-really-matters/ [https://perma.cc/B5MG-GRF3] (archived Jan. 20, 2019); *see also* DRAKE, *supra* note 28, at 12, 20.

86. G8 Declaration, *Renewed Commitment for Freedom and Democracy*, art. 2, ¶ 9 (May 26–27, 2011), https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2011_05/20110926_110526-G8-Summit-Deauville.pdf [https://perma.cc/TPJ2-NBJG] (archived Jan. 19, 2019).

87. OECD *Principles*, *supra* note 8, at 5–8.

88. Org. for Econ. Coop. & Dev. [OECD], *Ministerial Declaration on the Digital Economy* (June 21–23, 2016), https://www.oecd.org/internet/Digital-Economy-Ministerial-Declaration-2016.pdf [https://perma.cc/3TXR-RKS2] (archived Jan. 19, 2019) [hereinafter Cancún Declaration].

89. *NETmundial Multistakeholder Statement*, NETMUNDIAL (Apr. 24, 2014), http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf [https://perma.cc/2FKX-54NM] (archived Jan. 19, 2019).

90. *See, e.g.*, Japan-United States Trade Principles for Information and Communication Technology Services, Japan-U.S., Jan. 27, 2012, http://www.soumu.go.jp/main_content/000143845.pdf [https://perma.cc/4R6Q-QTM9] (archived Jan. 19, 2019); European Union-United States Trade Principles for

However, not all countries support internet openness with the same level of enthusiasm. For instance, countries such as Russia and China have repeatedly asserted sovereign control over the free flow of information to block or filter information that could be harmful to the cultural or moral ethos of the country or for purposes of national security.[91] This idea of national sovereignty in cyberspace (or *cyber sovereignty*) entails governments regulating the internet and the multistakeholder community playing only a secondary role.

3. Implementing Principle of Internet Openness

The flow of data packets requires openness and interoperability across different layers of the internet.[92] For example, technical protocols and standards (such as routing protocols) and application software should be interoperable with each other to facilitate internet openness. An integrated and universal IP address system (Domain Name System or DNS) is essential for accuracy, transparency, and efficiency in data flows through the internet.[93] Further, in order to facilitate internet openness, commercial digital services should be built on transparent and interoperable standards to ensure that customers can access and use different digital services.[94] To the contrary, the use of closed or proprietary standards or platforms reduces internet

---

Information and Communication Technology Services, E.U.-U.S., Apr. 4, 2011, http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147780.pdf [https://perma.cc/7TUH-5WCC] (archived Jan. 19, 2019).

91. Paul R. Burgman, *Securing Cyberspace: China Leading the Way in Cyber Sovereignty*, THE DIPLOMAT (May 18, 2016), https://thediplomat.com/2016/05/securing-cyberspace-china-leading-the-way-in-cyber-sovereignty/ [https://perma.cc/PW4U-YS35] (archived Jan. 19, 2019); *China internet: Xi Jinping calls for 'cyber sovereignty'*, BBC (Dec. 16, 2015), https://www.bbc.com/news/world-asia-china-35109453 [https://perma.cc/SDP6-GS87] (archived Jan. 19, 2019); Alexander Gabuev, *How China and Russia see the internet*, WORLD ECON. FORUM (Dec. 16, 2015), https://www.weforum.org/agenda/2015/12/how-china-and-russia-see-the-internet/ [https://perma.cc/CB4H-GUQX] (archived Jan. 19, 2019); Bruce Sterling, *Respecting Chinese and Russian Cyber-Sovereignty in the Formerly Global Internet*, WIRED (Dec. 22, 2015, 8:06 AM), https://www.wired.com/beyond-the-beyond/2015/12/respecting-chinese-and-russian-cyber-sovereignty-in-the-formerly-global-internet/ [https://perma.cc/HJ3E-PQ25] (archived Jan. 19, 2019); Zhu Yuan, *No absolute free flow of information*, CHINA DAILY (Jan. 26, 2010), http://www.chinadaily.com.cn/opinion/2010-01/26/content_9380067.htm [https://perma.cc/U8LF-AVF5] (archived Jan. 19, 2019).

92. *See* DeNardis, *supra* note 64, at 4–5; PALFREY & GASSER, *supra* note 26 (interoperability refers to "the ability to transfer and render useful data and other information across systems, applications, or components"); *see also* Rolf W. Weber, *Legal Interoperability as a Tool for Combatting Fragmentation, in* GLOBAL COMMISSION ON INTERNET GOVERNANCE (Ctr. for Int'l Governance Innovation & Chatham House, Paper Ser. No. 37, July 2016).

93. OECD *Internet Openness*, *supra* note 63, at 1,

94. *See, e.g.*, GRACE A. LEWIS, THE ROLE OF STANDARDS IN CLOUD-COMPUTING INTEROPERABILITY 18–19 (2012).

openness.[95] For example, certain digital services may not function on closed platforms because their technical codes are incompatible with those of the platform.

Although internet openness is desirable, a completely open internet is considered suboptimal for various reasons.[96] First, the variations in culture, language, and censorship as well as access to internet infrastructure across countries make it infeasible to construct a completely unified internet.[97] Second, a certain degree of fragmentation may be necessary for greater security or setting up business operations such as firewalls and VPN services.[98] Nonetheless, a majority of the vulnerabilities and flaws arising from the open architecture are better addressed by technical solutions including end-to-end encryption rather than closing off the network.[99]

Internet openness also relates to transparency, both at a technical and regulatory level; thus, the necessity of measures restricting internet openness and their underlying rationale should be properly assessed by governments, the internet technical community, and technology companies. The IETF has recommended a separate code "to provide transparency in circumstances where issues of law or public policy affect server operations."[100] This transparency is important as measures affecting internet openness often interfere with the seamless architecture of the internet; for example, an internet censorship measure could harm the integrity of the DNS.[101] Dennis Broeders terms the main protocols and infrastructure, including the DNS, as the "public core of the internet."[102] When imposing restrictions on internet

---

95. DeNardis, *supra* note 64, at 9; OECD *Internet Openness*, *supra* note 63, at 5.

96. ORG. FOR ECON. COOP. & DEV. [OECD], OECD DIGITAL ECONOMY OUTLOOK 2015 73–74 (2015), https://ec.europa.eu/eurostat/documents/42577/3222224/Digital+economy+ outlook+2015/dbdec3c6-ca38-432c-82f2-1e330d9d6a24 [https://perma.cc/P7RX-3TRV] (archived Feb. 6, 2019) [hereinafter OECD DIGITAL ECONOMY]; Christopher S. Yoo, *When Are Two Networks Better Than One? Toward a Theory of Optimal Fragmentation*, *in* GLOBAL COMMISSION ON INTERNET GOVERNANCE 1 (Ctr. for Int'l Governance Innovation & Chatham House, Paper Ser. No. 36, June 2016); Box, *supra* note 67; Wolfgang Kerber & Heike Schweitzer, *Interoperability in the Digital Age*, 8 J. INTELL. PROP., INFO. TECH. & ELECTRONIC COM. L., 39, 42 (2017).

97. Laura DeNardis, *Five Destabilizing Trends in Internet Governance*, 12 I/S: A J.L. & POL'Y INFO. SOC'Y 133, 127 (2015) [hereinafter DeNardis *Destabilizing*].

98. DeNardis, *supra* note 64, at 9.

99. CLARK, *supra* note 73, at 8.

100. Memorandum from Tim Bray on An HTTP Status Code to Report Legal Obstacles (Feb. 2016), https://tools.ietf.org/pdf/rfc7725.pdf [https://perma.cc/4HEP-AQ6V] (archived Feb. 5, 2019).

101. Joanna Kulesza & Rolf H. Weber, *Protecting the Public Core of the Internet*, *in* GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE 77 (The Hague Ctr. for Strategic Studies, GCSC Issue Brief No. 1, Nov. 2017).

102. DENNIS BROEDERS, THE PUBLIC CORE OF THE INTERNET: AN INTERNATIONAL AGENDA FOR INTERNET GOVERNANCE 13 (2016).

openness, governments or the private sector should remain cautious when the said measure affects this core architecture of the network.

Finally, internet openness does not imply that governments cannot regulate digital services on legitimate public policy grounds—for example, to prevent circulation of racist content or child pornography.[103] However, internet users should be clearly made aware of the specific reasons for being denied access to a specific digital service. Similarly, governments should be transparent and objective in implementing their laws and regulations such that private sectors can have legal certainty regarding how domestic laws apply to political or sociocultural online content. Thus, as Laura DeNardis argues, facilitating internet openness is not just an engineering function but also a "constan[t] navigat[ion]" between "diverging social values and interests" that "vary by region."[104]

B. *Principle of Internet Security*

1. Internet Security Means Both Network and Application Security

Internet security is typically defined as encompassing all "measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means."[105] Broadly speaking, the implementation of this principle requires protecting the security of the internet network and all applications and websites supplied through this network, thereby preventing "unintended or unauthorized access, change or destruction" of data transferred through the network.[106] As new threats and vulnerabilities emerge every day, no network can be fully secure.[107] Therefore, ensuring internet security often refers to a higher degree of security within the network than a completely secure network. In other words, the implementation of this principle should be aimed at preserving the fundamental integrity and stability of the network to the greatest extent possible.[108] Additionally, the principle of internet security also refers to security of the applications layer; for example,

---

103. DANIEL CASTRO & ROBERT ATKINSON, BEYOND INTERNET UNIVERSALISM: A FRAMEWORK FOR ADDRESSING CROSS-BORDER INTERNET POLICY 8 (2014), http://www2.itif.org/2014-crossborder-internet-policy.pdf [https://perma.cc/MLM2-JSJR] (archived Feb. 5, 2019).

104. DeNardis, *supra* note 64, at 3.

105. AUSTL. DEP'T OF FOREIGN AFFAIRS & TRADE, AUSTRALIA'S INTERNATIONAL CYBER ENGAGEMENT STRATEGY 23 (2017) (examining various sources to define cybersecurity); *see also* Convention on Cybercrime, pmbl., Nov. 23, 2011, E.T.S. 185 (offering a similar definition based on confidentiality, integrity, and availability of data).

106. *Introduction to Cyber Security*, UNIV. MD., UNIV. COLLEGE, https://www.umuc.edu/academic-programs/cyber-security/about.cfm [https://perma.cc/TFP6-DJ8P] (archived Feb. 5, 2019).

107. INTERNET SOC'Y, *supra* note 63, at 3.

108. *Id.*

technical designs of digital services should be secure from foreign intrusion and/or data theft.[109] Thus, internet security is achieved through a combination of network and data security, enabling "trust among networks, between websites and browsers, and in common technical standards and systems of routing and addressing."[110] Different terms are used to refer to internet security in internet governance scholarship: cybersecurity, digital security, and information security.[111]

2. Increasing Recognition of Internet Security in Various International Platforms

Several international declarations have emphasised the importance of internet security. The Tunis Agenda, adopted in phase two of the World Summit on the Information Society, recognised internet security as one of the fundamental principles of internet governance:

> [W]e commit ourselves to the stability and security of the [i]nternet as a global facility and to ensuring the requisite legitimacy of its governance, based on the full participation of all stakeholders, from both developed and developing countries, within their respective roles and responsibilities.[112]

Similar declarations, recommendations, and guidelines on internet security have been issued by regional bodies such as the OECD,[113] the

---

109. *See* Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 431 (2016); Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARV. INT'L L.J. 373, 380 (2011).

110. Laura DeNardis, *The Future of Global Cyber Trust: Fragmentation v. Universality Tradeoffs* 3 (Colum. Sch. of Int'l & Pub. Aff., Working Paper, 2017) [hereinafter DeNardis *Future*].

111. *See, e.g.*, OECD *Internet Openness*, *supra* note 63, at 28; Org. for Econ. Coop. & Dev. [OECD], *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document* 19, 20 (Sept. 17, 2015), https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf [https://perma.cc/8Q42-KK7T] (archived Feb. 5, 2019) [hereinafter OECD *Risk Management*].

112. *Tunis Agenda*, *supra* note 83, at ¶31.

113. *See* OECD *Risk Management*, *supra* note 111; Org. for Econ. Coop. & Dev. [OECD], *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures*, C(2008)35 (June 2008), https://www.oecd.org/sti/40825404.pdf [https://perma.cc/GWV2-TBY2] (archived Feb. 5, 2019); Org. for Econ. Coop. & Dev. [OECD], *Recommendation of the Council Concerning Guidelines for Cryptography Policy*, C(97)62/FINAL (Mar. 27, 1997), http://www.oecd.org/officialdocuments/publicdisplay documentpdf/?cote=C(97)62/FINAL&docLanguage=En [https://perma.cc/SR2Q-8X3P] (archived Feb. 5, 2019).

African Union,[114] the G7,[115] the Asia-Pacific Economic Cooperation (APEC),[116] and in the NETMundial Principles.[117] Many countries are also working in bilateral arrangements to achieve cooperation on issues related to internet security.[118] The IGF has also engaged deeply with issues of internet security since its inception in 2005.[119] The UN General Assembly adopted several resolutions on promoting global cooperation on cybersecurity issues, protection of critical infrastructure, and prevention of cyber-related crimes.[120] Further, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, a UN intergovernmental working group, was actively contributing to the development of international law on global cybersecurity until its end in 2017.

3. Implementing Principle of Internet Security

Different stakeholders in the internet governance regime are interested in varied facets of internet security and thus have differing rationales for focusing on internet security.[121] Nonetheless, a consensus exists among stakeholders that internet security is of

---

114. African Union Convention on Cyber Security and Personal Data Protection, art. 8, June 27, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf [https://perma.cc/Z7NZ-M7C3] (archived Feb. 5, 2019).

115. *See* G7 Declaration on Responsible States Behavior in Cyberspace, Apr. 11, 2017.

116. *See, e.g.*, Asia-Pacific Econ. Cooperation [APEC], *APEC Cyber-security Strategy*, Doc. No. telwg26/BFSG/22 (Aug. 2002), http://mddb.apec.org/Documents/2002/TEL/TEL26-PLEN/02_tel26_plen_summary.pdf [https://perma.cc/EWB3-YCD2] (Feb. 25, 2019).

117. *NETmundial*, *supra* note 89.

118. *See, e.g.*, Franz-Stefan Gady, *Japan and the United States to Deepen Cybersecurity Cooperation*, THE DIPLOMAT (June 2, 2015), https://thediplomat.com/2015/06/japan-and-the-united-states-to-deepen-cybersecurity-cooperation/ [https://perma.cc/ZD7B-M8LZ] (archived Jan. 20, 2019); Scott W. Harold, *The U.S.-China Cyber Agreement: A Good First Step*, THE RAND BLOG (Aug. 1, 2016), https://www.rand.org/blog/2016/08/the-us-china-cyber-agreement-a-good-first-step.html [https://perma.cc/F3FH-F9HH] (archived Jan. 20, 2019); Yuxi Wei, *China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty*, UNIV. WASH. (June 21, 2016), https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/ [https://perma.cc/4RXA-ZJTZ] (archived Jan. 20, 2019); *see also* Finnemore & Hollis, *supra* note 109, at 442.

119. *See* ALEJANDRO PISANTY, *Security, the Key to Trust and Growth of the Internet*, *in* INTERNET GOVERNANCE: CREATING OPPORTUNITIES FOR ALL 46, 46–54 (2009).

120. G.S. Res. 2010, *supra* note 7; G.A. Res. 2004, *supra* note 7; G.A. Res. 2002, *supra* note 7; G.A. Res. 2001, *supra* note 7.

121. Press Release, Internet Soc'y, Internet Society Approach to Cyber Security Policy (Jan. 22, 2015), https://www.internetsociety.org/news/press-releases/2015/internet-society-approach-to-cyber-security-policy/ [https://perma.cc/879X-ZBAN] (archived Jan. 20, 2019).

paramount importance.[122] Governments largely implement cybersecurity laws to address concerns regarding protection of critical infrastructure from cyberattacks (often conflating national security and internet security in this process).[123] Further, internet security is also included in the digital economy strategy of different countries.[124] However, the appetite for risk varies among governments. The Global Cybersecurity Index, developed by the ITU, illustrates the variation in the levels of engagement and preparedness of countries on cybersecurity.[125] Further, certain countries use cybersecurity or information security strategies to disguise other political or economic interests including monitoring information regarding citizens and protecting local companies.[126] Technology companies are concerned about internet security to protect their intellectual property as well as personal data of their customers such as credit card or personal identification details (including the use of end-to-end encryption).[127]

Finally, the internet technical community is also concerned about incorporating security features in internet protocols. For example, in 1997, the IETF decided that all requests for comment (RFCs)[128] should contain a dedicated section on "security considerations of the protocol or procedures."[129] But the role of the IETF does not extend to devising

---

122. JOANNA KULESZA, INTERNATIONAL INTERNET LAW 67 (2012).

123. *See* BROEDERS, *supra* note 102, at 13; LAURA DENARDIS ET AL., THE RISING GEOPOLITICS OF INTERNET GOVERNANCE: CYBER SOVEREIGNTY V. DISTRIBUTED GOVERNANCE 16–17 (2016).

124. *See* Org. for Econ. Coop. & Dev. [OECD], *Cybersecurity Policy Making at a Turning Point* (2012), https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf [https://perma.cc/Q64S-9U52] (archived Feb. 5, 2019); OECD DIGITAL ECONOMY OUTLOOK 2015, *supra* note 96, at 30.

125. *Global Cybersecurity Index*, INT'L TELECOMM. UNION (2017), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf [https://perma.cc/LL6N-7333] (archived Feb. 5, 2019).

126. Adam Segal, *Chinese Cyber Diplomacy in a New Era of Uncertainty* 3–5, 16 (Hoover Inst., Aegis Paper Ser. No. 1703), https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf [https://perma.cc/UVA5-PHT2] (archived Feb. 3, 2019); Bethany Allen-Ebrahimian, *The 'Chilling Effect' of China's New Cybersecurity Regime*, FOREIGN POLICY, (July 10, 2015, 3:27 PM), https://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/ [https://perma.cc/D3TW-8N3N] (archived Jan. 20, 2019); Janus Kopfstein, *Washington's cybersecurity is about surveillance, not security*, AL JAZEERA AM. (Mar. 10, 2015, 2:00 AM), http://america.aljazeera.com/opinions/2015/3/washingtons-cybersecurity-is-about-surveillance-not-security.html [https://perma.cc/47TM-JQLN] (archived Jan. 20, 2019).

127. Finnemore & Hollis, *supra* note 109, at 453; *see also* Josephine Wolff, *What We Talk About When We Talk About Cybersecurity: Security in Internet Governance Debates*, INTERNET POL'Y REV. 1–4 (Sept. 30, 2016); OECD *Risk Management*, *supra* note 111, at 19–20.

128. *See* Memorandum from S. Hambridge on Netiquette Guidelines, *supra* note 11.

129. Memorandum from John Postel & J. Reynolds on Instructions to RFC Authors (Oct. 1997), https://tools.ietf.org/pdf/rfc2223.pdf [https://perma.cc/PSJ5-JWM7] (archived Feb. 5, 2019); *see also* Memorandum from E. Rescorla on Guidelines for Writing

technical protocols based on domestic laws of individual countries.[130] The IETF has also designed a new set of technical standards known as the Domain Name System Security Extensions (DNNSEC), which can help assess the authenticity of websites (through cryptography), and prevent malicious attacks.[131] While some of the above policy objectives can be achieved harmoniously (e.g., the protection of personal information also reduces online consumer fraud and surveillance, network integrity helps prevents coordinated cyberattacks on a country's critical infrastructure and other digital services), others may be in conflict (e.g., government measures requiring access to encryption keys or a source code so as to authenticate its security can compromise personal data and trade secrets of companies).

The development of protocols or standards on cybersecurity increasingly requires collaboration between different stakeholders and a shared understanding regarding their individual roles in the management of security risks.[132] The majority of standard-setting on internet security is not managed by state or intergovernmental bodies, but rather through informal trust-based relationships among private bodies such as internet service providers, computer security incident response teams within companies, domain name registrars, hosting companies, IT departments, and some private security services.[133] The same holds true for management of spam, since most internet service providers rely on spam blocking lists maintained by private entities.[134] However, achieving collaboration between various stakeholders on internet security issues is difficult in practice. For example, governments often want to exercise control over encryption software for easier data access while the private sector supports innovation in internet security standards.

RFC Text on Security Considerations (July 2003), https://tools.ietf.org/pdf/rfc3552.pdf [https://perma.cc/7N2J-PQZY] (archived Feb. 5, 2019).

130. Memorandum from IAB & IESG on IETF Policy on Wiretapping (May 2000), https://tools.ietf.org/pdf/rfc2804.pdf [https://perma.cc/U5A9-ZH7Q] (archived Feb. 5, 2019).

131. *See* GCIG ONE INTERNET, *supra* note 1, at 82.

132. *See* MILTON L. MUELLER, NETWORKS AND STATES—THE GLOBAL POLITICS OF INTERNET GOVERNANCE 159–60 (2010); SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, AND RELATIONS IN SEARCH OF CYBER PEACE 3–4 (2014).

133. *See* MUELLER, *supra* note 132, at 163; Louise Marie Hurel & Louisa Cruz Lobato, *Unpacking Cyber Norms: Private Companies as Norms Entrepreneurs*, 3 J. CYBER POL'Y (2018).

134. For example, Spamhaus, ARM Research Labs, Spamcop are private companies providing DNS blacklists to control spam.

C. *Principle of Internet Privacy*

1. Internet Privacy: A User-Centric Approach

Internet privacy refers to protecting the privacy of internet users. Privacy is closely linked to data protection and often used interchangeably.[135] Data protection is an "expression of right to privacy" and privacy is at "the core of data protection."[136] Given the increased use of digital technologies and big data processing (discussed further below), the principle of internet privacy refers to the protection of privacy of individual users in the process of managing their personal data include gathering, storing, using, and transferring such data,[137] as well as protecting it from unwanted surveillance.[138] In this Article, internet privacy excludes data security (i.e., user information is stored and transferred securely) because it falls within the scope of internet security, as discussed previously.[139] This distinction is important as even when data is fully secure from unauthorised access, service providers can use data in violation of users' privacy—for example, selling personal data to third-party advertisers without the express consent of users.[140]

The key high-level principles of internet privacy are well summarised by Lee Bygrave:

> Personal data should be collected by fair and lawful means (principle of fair and lawful processing); the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data is gathered and further processed (principle of minimality); personal data should be collected for specified, legitimate purposes, and not used in ways that are incompatible with those purposes (principle of purpose limitation); personal data should be

---

135. Juliane Kokott & Christoph Sobotta, *The Distinction Between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 INT'L DATA PRIVACY L. 222, 228 (2013).

136. *See id.* at 222–23. Some distinguish between the economic rationale behind privacy (i.e., building consumer trust) from the human rights rationale (i.e., protecting privacy rights of an individual), and argue that the latter is weaker than the former. *See, e.g.*, Yakovleva, *supra* note 37, at 478.

137. *See* LEE A. BYGRAVE, DATA PRIVACY LAW 1 (2014).

138. *See* Steve Henn, *If There's Privacy in the Digital Age, It Has a New Definition*, NPR (Mar. 3, 2014, 4:00 PM), https://www.npr.org/sections/alltechconsidered/2014/03/03/285334820/if-theres-privacy-in-the-digital-age-it-has-a-new-definition [https://perma.cc/A7M4-QZPZ] (archived Jan. 20, 2019).

139. *See* BYGRAVE, *supra* note 137, at 2.

140. *See* Alex Hern, *Social networks may have to reveal how they target users with ads*, THE GUARDIAN (Mar. 6, 2018, 1:16 PM), https://www.theguardian.com/technology/2018/mar/06/social-networks-reveal-how-they-target-users-with-political-ads [https://perma.cc/6Y5A-NN5X] (archived Jan. 20, 2019); Kurt Wagner, *This is how Facebook uses your data for ad targeting*, RECODE (Apr. 11, 2018, 6:00 AM), https://www.recode.net/2018/4/11/17177842/facebook-advertising-ads-explained-mark-zuckerberg [https://perma.cc/G3KG-RH29] (archived Jan. 20, 2019).

> relevant, accurate, and complete in relation to the purposes for which it is processed (principle of data quality); personal data should be protected against unauthorized attempts to disclose, delete, change, or exploit it (principle of data security); and processing of personal data should be transparent to, and capable of being influenced by, the data subject (principle of data subject influence).[141]

The above principles are well recognised in existing data protection laws;[142] however, the norm of privacy is culture specific and can vary across countries. For example, in certain countries, an individual's privacy is considered secondary to other interests such as national security or maintenance of public order or even commercial interests.[143] Even in countries with developed privacy regimes, a conflict could exist regarding the proper approach for achieving internet privacy. In particular, scholars have discussed the clash between the European Union (EU)-type model and the US-type model of privacy and data protection in great detail.[144] While the EU-type model is prescriptive and adopts a comprehensive framework on privacy and data protection, the United States adopts a more market-oriented approach, largely depending on self-regulation on privacy issues, barring a few sensitive issues.[145] Further, certain scholars argue that a US-type approach aimed at ensuring privacy to facilitate consumer trust is weaker than an EU-type approach premised on protecting a fundamental right.[146] In practice, however, this argument is inconclusive as the means or tools used to enforce privacy ultimately determine their effectiveness. For example, a certain country can severely restrict cross-border data flows out of its borders through prescriptive data transfer requirements without achieving significant increase in privacy protection. Conversely, a country may allow cross-border data flows but impose strict requirements on all service suppliers to comply with its privacy laws.

The development of big data analytics has triggered significant concerns regarding protection of privacy of internet users.[147] In recent

---

141. BYGRAVE, *supra* note 137, at 1–2. As discussed earlier, I cover data security under internet security rather than internet privacy.

142. About 57 percent of countries worldwide have a data protection law. *See* U.N. Conference on Trade and Development, *Data Protection and Privacy Legislation Worldwide*, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx [https://perma.cc/3PMS-SG7A] (archived Jan. 20, 2019).

143. The concept of information security embedded in its domestic cybersecurity laws refers to national or public security rather than individual's right to privacy. *See* Jyh-An Lee, *Hacking Into China's Cybersecurity Law*, 53 WAKE FOREST L. REV. 57, 89–94 (2018).

144. *See* Catherine L. Mann, *International Internet Governance—Oh What a Tangled Web We Could Have*, 2 GEO. J. INT'L AFF. 79, 81 (2001).

145. *See id.*

146. *See* Yakovleva, *supra* note 37, at 7–8.

147. *See, e.g.*, Press Release, Internet Soc'y, Majority (52%) Says They're More Concerned About Online Privacy Than They Were a Year Ago (May 17, 2018), https://www.cigionline.org/sites/default/files/documents/CIGI-2018-Factum.pdf

years, concerned users have brought actions against technology companies for invading their privacy—for instance, the legal challenge against Facebook by an Austrian activist, Maximillian Schrems, in 2013.[148] Commercial surveillance is common in many free services such as email, social networking sites, and messenger applications. For example, the providers of these services collect enormous amounts of customer data, which is used for targeted advertising or sold to third parties, often without informed user consent.[149] Even in paid services such as cloud computing, significant uncertainty exists for users regarding where their data is stored, how it can be used or transferred, and the extent to which company officials or third parties have access to it.[150] Similarly, internet privacy is eroded by online surveillance programs carried out by government intelligence agencies.[151] Several governments demand that digital service providers provide information such as their source code and encryption keys in order to offer services in that country, potentially endangering user privacy.[152] Thus, internet privacy is a central concern in internet governance, and is a key requirement for ensuring secure and free data flows.

2. Growing Recognition of Internet Privacy

Within the internet governance regime, privacy and data protection are unanimously recognised as fundamental issues. The UN General Assembly has noted that the increasing "capacity of governments, companies and individuals to undertake surveillance, interception and data collection" can threaten the privacy of individuals, and that states need to take necessary action in this regard.[153] Several international human rights treaties also recognise

---

[https://perma.cc/K7GM-YUBV] (archived Jan. 20, 2019) [hereinafter Internet Soc'y Press Release].

148. Schrems v. Data Prot. Comm'r, Case C-363/14, E.C.L.I:C:2015:650 (2015); *see also* Derek Scally, *Max Schrems files first cases under GDPR against Facebook and Google*, THE IRISH TIMES (May 25, 2018, 6:15 PM), https://www.irishtimes.com/business/technology/max-schrems-files-first-cases-under-gdpr-against-facebook-and-google-1.3508177 [https://perma.cc/Z3LV-8VDL] (archived Jan. 20, 2019).

149. *See id.*

150. *See id.*

151. Certain civil society groups are attempting to build consensus around principles that should apply to governments engaging in surveillance. *See, e.g.*, *International Principles on the Application of Human Rights to Communications Surveillance*, NECESSARY & PROPORTIONATE (2014), https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf [https://perma.cc/F48Z-STK5] (archived Jan. 20, 2019).

152. *See* MARTINA F. FERRACANE ET AL., DIGITAL TRADE RESTRICTIVENESS INDEX 33–35 (2018), http://globalgovernanceprogramme.eui.eu/wp-content/uploads/2018/09/DTRI-final.pdf [https://perma.cc/9HGD-Z7GF] (archived Feb. 5, 2019).

153. G.A. Res. 71/199 (Dec. 19, 2016); *see also* G.A. Res. 45/95, (Dec. 14, 1990).

the right to privacy of individuals,[154] although these treaties only refer to domestic violations of privacy rights, not cross-territorial conduct such as online commercial and governmental surveillance.[155] Several international declarations also recognise the importance of privacy.[156] In the Tunis Agenda, the multistakeholder community expressed its commitment to "strengthe[n] the trust framework," including enhancing international cooperation on data protection and privacy issues.[157] However, to date, no international consensus exists regarding regulation of both commercial and governmental surveillance, or definitions of privacy or data protection.

Among regional organisations, the OECD recognises the importance of "consistency and effectiveness in privacy protection at a global level" as "good practice" in internet governance.[158] The OECD has adopted the OECD Privacy Framework, which contains implementation guidelines for member countries including development of a national privacy strategy alongside adoption of privacy laws and enforcement mechanisms.[159] One of the key concerns in the OECD framework was to ensure that privacy laws did not become a tool for disguised protectionism.[160] Closely related to the OECD framework, APEC countries have adopted a voluntary privacy framework which "recogniz[es] the importance of the development of effective privacy protections that avoid barriers to information flows, ensure continued trade, and economic growth in the APEC region."[161] Amongst domestic regulations, the GDPR of the EU is the most comprehensive and detailed framework on data protection.

3. Implementing Principle of Internet Privacy

Although certain values related to internet privacy are recognised globally, governments enforce privacy and data protection laws in

---

154. G.A. Res. 217, art. 12, Universal Declaration of Human Rights (Dec. 10, 1948); G.A. Res. 2200A (XXI), art. 17, International Covenant on Civil and Political Rights (Mar. 23, 1976); European Convention on Human Rights, art. 8 (Nov. 4, 1950).

155. *See* Frederic Gilles Sourgens, *The Privacy Principle*, 42 YALE J. INT'L L. 345, 355–57 (2017) (noting that "global or extraterritorial conduct is not within the scope of the ICCPR").

156. *See* Paul De Hert & Valeis Papakonstantinou, *Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?*, 9 I/S: A J.L. & POL'Y INFO. SOC'Y 271, 293–300 (2013).

157. *See Tunis Agenda*, *supra* note 83, at ¶ 39.

158. *See* Org. for Econ. Coop. & Dev. [OECD], *The OECD Privacy Framework* (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/J7MD-7CVH] (archived Jan. 20, 2019).

159. *See id.* at 19.

160. BYGRAVE, *supra* note 137, at 44.

161. *See* APEC, *supra* note 8, at foreword; *see also* BYGRAVE, *supra* note 137, at 77.

different ways, based on their political and cultural perspectives.[162] Governments impose various checks on data collectors and processors in their domestic laws so as to ensure more transparency in the process of data collection, such as imposing consumer consent requirements for collecting, transferring, or using personal data.[163] Since these regulatory practices and laws are not always uniform across countries, they create legal uncertainty for digital service providers operating on a cross-border basis, including significant increases in compliance costs.

In order to implement internet privacy, companies managing internet infrastructure (such as internet intermediaries and network operators) and those offering digital services incorporate necessary privacy features in their services, for example, through end-to-end encryption and transparent practices in data processing.[164] Further, in order to address the "trust gap" of internet users in countries with extensive mass surveillance programmes, leading technology companies are now providing annual transparency reports including government requests for user data.[165]

The internet technical community also recognises internet privacy as one of the fundamental considerations in devising protocols and architectural designs.[166] However, organisations such as the IETF also acknowledge that the legal and political aspects of surveillance or

---

162. *See* Joanna Kulesza, *International Law Challenges to Location Privacy Protection*, 3 INT'L DATA PRIVACY L. 158, 161 (2013).

163. *See, e.g.*, EU Data Protection Regulation, *supra* note 59, arts. 4, 6, 7, 49.

164. Amnesty International, *How Private Are Your Favourite Messaging Apps?*, AMNESTY INT'L (Oct. 21, 2016), https://www.amnesty.org/en/latest/campaigns/2016/10/which-messaging-apps-best-protect-your-privacy/?date=2016-12-24&imageIndex=12&matchday=2&id=20518228265&view=zertifikate&i=6&facelift=true&addUrlParams=true [https://perma.cc/8VM9-Q642] (archived Jan. 20, 2019).

165. *See, e.g.*, *Google Transparency Report*, GOOGLE, https://transparencyreport.google.com/?hl=en (last visited Mar. 13, 2019) [https://perma.cc/3BDD-UNNH] (archived Jan. 20, 2019).

166. *See* Memorandum from A. Cooper et al. on Privacy Considerations for Internet Protocols (July 2013), https://tools.ietf.org/pdf/rfc6973.pdf [https://perma.cc/DJ3R-RV9N] (archived Feb. 6, 2019) (providing a catalogue for assessment of the privacy level of technical protocols); Memorandum from IAB & IESG, IAB and IESG Statement on Cryptographic Technology and the Internet (Aug. 1996), https://tools.ietf.org/pdf/rfc1984.pdf [https://perma.cc/ZF58-K9K3] (archived Feb. 5, 2019) (one of the earliest RFCs to recognise "the need for increased protection of international commercial transactions on the Internet, and by the need to offer all Internet users an adequate degree of privacy," particularly focusing on the importance of public key cryptography to ensure internet trust and security); Memorandum from Stephen Farrell, Pervasive Monitoring is an Attack (May 2014), https://tools.ietf.org/pdf/rfc7258.pdf [https://perma.cc/VXF4-GG2E] (archived Feb. 6, 2019) (outlining the various considerations in preventing surveillance); N. ten Oever, Guidelines for Human Rights Protocol Considerations (Mar. 20, 2018) (draft) (expired on Sept. 21, 2018), https://tools.ietf.org/id/draft-irtf-hrpc-guidelines-00.html [https://perma.cc/CG4Z-5528] (archived Feb. 6, 2019).

pervasive monitoring are outside the scope of their competence.[167] In fact, privacy-related concerns were noted since the early days of the IETF.[168] Engineers in organisations such as the IETF and the World Wide Web Consortium (W3C) as well as within private companies develop protocols and architectural designs that enforce internet privacy in the underlying logical layer and the applications layer.[169] They also consider prevailing privacy risks and existing privacy models in making several technical recommendations.[170]

Given the complexities associated with implementing internet privacy, experts have advocated the need for greater collaboration between governments, the private sector, and the internet technical community.[171] Insufficient coordination between various stakeholders on internet privacy often results in highly restrictive measures such as data localisation that are harmful for both commercial and technical reasons. However, internet privacy is as such not a barrier to digital flows; in fact, implementing internet privacy enables users to trust the network and digital services, thus facilitating its use for commercial and other purposes.[172] In order to enable higher levels of internet privacy, certain governments have entered into arrangements to enable data transfers without compromising on privacy; for example, the EU and the United States have entered into the Privacy Shield, and the APEC countries have a voluntary certification system to facilitate data flows.[173] Certain governments adopt deeper provisions that not only impose principles for data protection, but also require service suppliers to hardwire privacy in their technical designs. For example, the EU sets a requirement in the GDPR for data protection by design and default.[174]

---

167. *See, e.g.*, Adamantia Rachovitsa, *Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue*, 24 INT'L J.L. & INFO. TECH. 374, 376 (2016); Memorandum from A. Cooper, *supra* note 166; Memorandum from Stephen Farrell, *supra* note 166; Memorandum from J. Kempf, *supra* note 69.

168. Lee A. Bygrave, *Hardwiring Privacy*, *in* THE OXFORD HANDBOOK OF LAW, REGULATION AND TECHNOLOGY 755, 766 (Roger Brownsword et al. eds., 2017).

169. *See IETF RFCs*, *supra* note 11; *see also W3C Mission*, W3C (2017), https://www.w3.org/Consortium/mission [https://perma.cc/R4MU-KPFS] (archived Jan. 20, 2019).

170. *See* Memorandum from Stephen Farrell, *supra* note 166, at 3–4.

171. *See* ORG. FOR ECON. COOP. & DEV. [OECD], THIRTY YEARS AFTER: THE OECD PRIVACY GUIDELINES 13 (2011), http://www.oecd.org/sti/ieconomy/49710223.pdf [https://perma.cc/B9AJ-U2HE] (archived Feb. 6, 2019) (acknowledging "encouraging signs of a broad multi-stakeholder commitment on the part of privacy advocates, the technical community, businesses and governments to protecting privacy"); DeNardis *Future*, *supra* note 110.

172. DeNardis *Future*, *supra* note 110.

173. *About CBPRS*, CROSS BORDER PRIVACY RULES SYSTEM, http://cbprs.org/about-cbprs/ (last visited Feb. 6, 2019) [https://perma.cc/G7FB-5WSG] (archived Jan. 19, 2019).

174. EU Data Protection Regulation, *supra* note 59, art. 25.

D. *Complementarity of Internet Openness, Security, and Privacy*

At first sight, internet openness appears to be an isolated principle, and arguably in conflict with the principles of internet security and privacy, as security and privacy measures can directly or indirectly interfere with the unrestricted flow of data through the internet. In practice, however, openness in data flows is realistically only possible in a network in which privacy and security features are embedded into the network.[175] Questions related to internet openness "cross-cu[t] specific issues such as . . . accessibility, security, and privacy."[176] Simply put, the more efficiently and safely data can be transferred across borders, the easier it is for digital service providers to sell across the world. This subpart demonstrates how these three principles are mutually supportive and complementary and should be applied collectively in regulating data flows.

Internet security and internet openness are often seen as being opposing principles, as internet openness can facilitate cybercrime such as cyberespionage, theft of personal information, and attacks on critical infrastructure of a country.[177] The typical argument is that internet openness opens the door to various kinds of malicious and criminal activities; thus, to improve the security of the network, certain checks are necessary to minimise these threats.[178] Governments and other stakeholders can justifiably impose restrictions on internet openness in order to safeguard security of the network and user data.[179] As the internet transformed from a research-based network to a commercial platform, certain levels of restrictions on the openness of the network have arguably become necessary to ensure greater security.[180] Nonetheless, internet security needs to be balanced with other objectives such as the free flow of information, as is also recognised in the Convention on Cybercrime.[181]

Further, the openness of the internet itself is not the cause of malicious or illegal activity, provided that security and privacy features are incorporated into available digital services and devices.[182]

---

175. INTERNET SOC'Y, *supra* note 63, at 3; OECD DIGITAL ECONOMY, *supra* note 96, at 19; Jeremy West, *A Framework for Understanding Internet Openness, in* GLOBAL COMMISSION ON INTERNET GOVERNANCE 2016 at 5 (Ctr. for Int'l Governance Innovation & Chatham House, Paper Ser. No. 35, 2016), https://www.cigionline.org/sites/default/files/gcig_no.35_web.pdf [https://perma.cc/2Z9L-MEEW] (archived Jan. 19, 2019).

176. GCIG ONE INTERNET, *supra* note 1, at 2.

177. OECD *Internet Openness*, *supra* note 63, at 10.

178. *Id*. at 6.

179. Hill, *supra* note 62, at 53–54.

180. Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1977–78 (2006).

181. Convention on Cybercrime, *supra* note 105.

182. INTERNET SOC'Y, *supra* note 63, at 3; OECD DIGITAL ECONOMY, *supra* note 96, at 19; West, *supra* note 175, at 5.

In fact, internet openness is enhanced when adequate and necessary standards of internet security and privacy are incorporated in both the logical and transport layers of the network and the applications that run on the network. In other words, these tools facilitate the flow of information.[183] Similarly, internet users are likely to place greater trust in open networks, rather than closed networks (often run by specific companies or mandated by certain governments), because surveillance can be easily conducted in closed networks, resulting in breach of user privacy.[184] Internet openness also stimulates more innovation in ensuring higher standards of security and privacy as it becomes necessary for increasing economic activity.[185]

Conversely, lack of internet privacy or security can reduce internet openness, as many users either stop using certain services or "tur[n] to closed, proprietary solutions."[186] Further, blocking data flows does not counter all security risks, because intelligent users, particularly cybercriminals, can often work around firewalls or other filtering tools.[187] Even data restrictive measures arguably designed to ensure internet security and privacy can backfire because the concentration of data in specific local servers makes it more vulnerable to cyberattacks and external surveillance, particularly in jurisdictions with poor cybersecurity laws.[188] Thus, rather than being contradictory, internet openness is enhanced by internet security, and vice versa. Finally, open technical standards and protocols are more secure than closed and proprietary standards, as the security and privacy features of the latter remain unknown to users.[189] Therefore, interfering with the openness of the internet not only disturbs flows of data, but also affects the "security, flexibility, and stability" of the network.[190]

Internet privacy and internet security are also interrelated principles. As Christopher Kuner argues:

> Privacy depends absolutely on security. No obligation to provide privacy, whether entered into voluntarily or compelled by law, will be meaningful if the data to be protected are accessed or stolen by unauthorized third parties. As a result, all modern data protection principles include an obligation to protect security as well. Data privacy and cybersecurity are often advanced by common tools, such as encryption, data minimization, and limits on collecting, retaining,

183. West, *supra* note 175, at 7; *see also* DeNardis *Future*, *supra* note 110.
184. Internet Soc'y Press Release, *supra* note 147.
185. SINGH, *supra* note 14, at 2.
186. GCIG ONE INTERNET, *supra* note 1, at vii.
187. *See infra* Section 0.A3.
188. Anupam Chander & Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet*, *in* U.C. DAVIS LEGAL STUDIES RESEARCH PAPER SERIES 30 (U.C. Davis, Research Paper No. 378, 2014).
189. DeNardis *Destabilizing*, *supra* note 97, at 130.
190. OECD *Internet Openness*, *supra* note 63, at 8.

> and transferring personal data. In short, what is good for privacy is often good for security as well.[191]

However, implementing internet security can sometimes be detrimental to personal privacy, for example, "by requiring identity verification, reducing online anonymity, and sharing potentially personal information about cyberattacks."[192]

The interplay between the principles of internet openness, security, and privacy provides a useful guide in achieving balance and coherence in the regulation of data flows.[193] In fact, this complementarity is the foundation of an open and trusted internet.[194] Measures related to internet security and privacy act as building blocks, rather than impediments to data flows. Thus, these three principles are neither contrary to each other, nor do they operate in isolation of each other—rather, they are complementary.

A clash between internet openness and security or privacy laws or standards is a clash between multistakeholder norms and choices relevant to sovereignty, such as protecting social, political, or economic goals.[195] In practice, many of these conflicts can be minimised if these principles are understood from a transnational point of view and in a collective manner. However, certain challenges remain, particularly due to lack of global standards on internet privacy and security. For example, diverging privacy laws or conflicting security standards in different countries make it difficult for service providers to transfer data freely across countries via the internet, hampering internet openness in the process. One such challenge addressed in the next Part discusses both the relevance and challenges involved in operationalising these three principles in the context of application, interpretation, and, potentially, the reform of international trade law.

---

191. Christopher Kuner et al., *The Rise of Cybersecurity and its Impact on Data Protection*, 7 INT'L DATA PRIVACY L. 73, 73–74 (2017); *see also* Rachovitsa, *supra* note 167, at 386.

192. Kuner, *supra* note 191, at 74.

193. In the words of Kleinwachter, "everything is connected to everything." *See* Wolfgang Kleinwächter, *Internet Governance Outlook 2017: Nationalistic Hierarchies vs. Multistakeholder Networks?*, CIRCLEID (Jan. 6, 2017, 9:50 AM), http://www.circleid.com/posts/20160106_internet_outlook_2017_nationalistic_hierarchies_multistakeholder/ [https://perma.cc/38CL-8S25] (archived Jan. 19, 2019).

194. INTERNET SOC'Y, A POLICY FRAMEWORK FOR AN OPEN AND TRUSTED INTERNET 3 (2017), https://www.internetsociety.org/wp-content/uploads/2017/08/bp-Trust-20170314 -en.pdf [https://perma.cc/Z22K-LU56] (archived Jan. 19, 2019); *see also* INTERNET SOC'Y, GLOBAL INTERNET REPORT 2016 at 22 (2016), https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf [https://perma.cc/RH2F-PF4D] (archived Feb. 6, 2019); Carl Bildt & Gordon Smith, *The One and Future Internet*, 1 J. CYBER POL'Y, 142, 145 (2016).

195. DeNardis, *supra* note 64, at 3.

IV. OPERATIONALISING INTERNET OPENNESS, SECURITY, AND PRIVACY IN INTERNATIONAL TRADE LAW

The principles of internet openness, security, and privacy are not binding in international law, but rather originate from soft law instruments such as international declarations as well as several extralegal instruments such as RFCs, industry best practices, and other technical documents.[196] In practice, both domestic laws and regulations usually do not reflect an optimum balance of internet openness, security, and privacy that is necessary to ensure the security and integrity of data flows. For example, as discussed earlier, certain governments privilege internet security or privacy over internet openness, while others do not pay adequate attention to the role of internet security and privacy in facilitating internet openness.[197]

This Part argues that despite the nonbinding nature of the principles of internet openness, security, and privacy, they can be relevant in applying, interpreting, and/or reforming international trade law. At the outset, it argues that these three principles can potentially contribute to achieving different objectives of the GATS and WTO Agreement. Further, these three principles help facilitate a sound framework for digital trade. Finally, this Part argues that these principles can be helpful in (i) interpreting existing trade rules in disputes such as providing evidence on the technical aspects of certain data restrictive measures and (ii) understanding the gaps and formulating new rules on cross-border data flows in international trade law. Although this Part largely refers to provisions in WTO agreements, its arguments would also be relevant for PTAs aimed at promoting greater liberalisation in the services sector.

A. *The Principles of Internet Openness, Security, and Privacy and Objectives of GATS and WTO Agreement Are Mutually Compatible*

The principles of internet openness, security, and privacy are compatible with the underlying economic welfare objective of WTO law. The economic welfare objective is embodied in the preamble of the WTO Agreement:[198]

> Recognizing that their relations in the field of trade and economic endeavour should be conducted with a view to raising standards of living, ensuring full employment and a large and steadily growing volume of real income and effective demand, and expanding the production of and trade in goods and services, while allowing for the optimal use of the world's resources

196. *See supra* Part 0. For a discussion on soft law, see Diane Shelton, *Soft Law*, *in* ROUTLEDGE HANDBOOK OF INTERNATIONAL LAW 68, 70 (David Armstrong ed., 2012).

197. *See infra* Part IV.B.3 and IV.C.3.

198. Marrakesh Agreement, *supra* note 22, at pmbl.

> Recognizing further that there is need for positive efforts designed to ensure that developing countries, and especially the least developed among them, secure a share in the growth in international trade commensurate with the needs of their economic development.[199]

To achieve the above objectives, the WTO members agree to engage in trade liberalisation by "entering into reciprocal and mutually advantageous arrangements" for reducing tariffs and non-tariff barriers to trade as well as "eliminating discriminatory treatment in international trade relations."[200]

Similarly, the GATS Preamble also recognises the importance of trade liberalisation and balancing the interests of developing and developed countries: [201]

> Wishing to establish a multilateral framework of principles and rules for trade in services with a view to the expansion of such trade under conditions of transparency and progressive liberalization and as a means of promoting the economic growth of all trading partners and the development of developing countries;
>
> Desiring the early achievement of progressively higher levels of liberalization of trade in services through successive rounds of multilateral negotiations aimed at promoting the interests of all participants on a mutually advantageous basis and at securing an overall balance of rights and obligations, while giving due respect to national policy objectives . . .
>
> Desiring to facilitate the increasing participation of developing countries in trade in services and the expansion of their service exports including, inter alia, through the strengthening of their domestic services capacity and its efficiency and competitiveness.[202]

The principles of internet openness, security, and privacy enable a globally interconnected network, allowing for more digital innovation and new businesses, and thereby, help achieve greater economic welfare through trade liberalisation. The digital services market is the fastest growing sector in the world today and is a key driver of the global economy.[203] The entry barriers in the industry are low, and consumers have access to a range of competitive and high-quality services from across the world.[204] Further, digital platforms have also

---

199. *Id.*
200. *Id.*
201. *Id.* Annex 1B, preamble.
202. *Id.*
203. *See* Manyika, *supra* note 13.
204. *See Micro-Multinationals, Global Consumers and the WTO*, EBAY, https://www.ebaymainstreet.com/sites/default/files/Micro-Multinationals_Global-Consumers_WTO_Report_1.pdf (last visited Jan. 20, 2019) [https://perma.cc/LA2Q-G4E7] (archived Jan. 20, 2019); ORG. FOR ECON. COOP. & DEV. [OECD], SMALL AND MEDIUM-SIZED ENTERPRISES: LOCAL STRENGTH, GLOBAL REACH (June 2000),

increased access of small and medium enterprises to consumers outside their local or domestic markets.[205] Experts have argued that digital services will be critical in enabling entrepreneurs in developing countries and least developed countries to reach a wider global audience in a cost-effective manner, and help reduce income gaps between developing and developed countries.[206] These businesses also generate revenues and increase employment for the local people.[207] Thus, the increased use of the internet as a platform for trade directly helps achieve the fundamental objectives set out in the WTO Agreement and GATS.

Further, implementing the principles of internet openness, security, and privacy requires more transparent and nondiscriminatory measures in relation to cross-border data flows. For example, governments would need to clearly establish the security or privacy rationales behind data restrictive measures. In devising these measures, governments could collaborate with relevant stakeholders in the industry and civil society to find the right balance between internet openness, security, and privacy. As a result, governmental practices that diminish accessibility and trust of digital services to favour domestic companies or enable secret access to data will be minimised. Therefore, in implementing these three principles, governments can also achieve core objectives in WTO law of transparency and nondiscrimination.[208]

Finally, although the GATS was not devised to promote digital trade, the balancing of internet openness, security, and privacy can contribute to finding the desired balance between liberalising digital trade and safeguarding domestic policy objectives (relevant to the internet and cyberspace) as enshrined under GATS (particularly Article XIV).[209] The principles of internet privacy and security explicitly recognise the need for regulatory frameworks where data and network integrity and security as well as privacy of individuals are protected. However, as discussed earlier in Part III.D, when implemented in a reasoned and objective manner, these principles

---

http://www.oecd.org/cfe/leed/1918307.pdf [https://perma.cc/UM4W-VWTR] (archived Feb. 6, 2019).

205. *See, e.g.*, Huijun Jin & Fiona Hurd, *Exploring the Impact of Digital Platforms on SME Internationalization: New Zealand SMEs Use of the Alibaba Platform for Chinese Market Entry*, 19 J. ASIA-PAC. BUS. 72, 91–92 (2018).

206. *See, e.g.*, Laura Tyson & Susan Lund, *Digital Globalization and the Developing World*, PROJECT SYNDICATE (Mar. 25, 2016), https://www.project-syndicate.org/commentary/digital-globalization-opportunities-developing-countries-by-laura-tyson-and-susan-lund-2016-03 [https://perma.cc/Z2HT-A6XG] (archived Jan. 20, 2019).

207. *See Micro-Multinationals, Global Consumers and the WTO*, *supra* note 204.

208. *See* Marrakesh Agreement, *supra* note 22, Annex 1B, arts. III, II, VI, XVI, XVII.

209. *See id.* Annex 1B, art. XIV.

enable a free and open internet rather than constraining data flows.[210] By following these principles in regulating cross-border data flows, governments can achieve the necessary balance required to protect domestic policy goals without unduly interfering with internet openness (thereby, also enabling more digital trade).[211]

B. *Internet Openness, Security, and Privacy Are Beneficial for Digital Trade*

The complementarity of internet openness, security, and privacy brings a new perspective in international trade law: contrary to popular perception, internet security and privacy can promote free flow of data and trade in digital services, provided they are consistent and reasonable and promote global, interoperable standards. Thus, not just internet openness, but also internet security and privacy, are highly beneficial for digital trade. This subpart explains further how internet openness, security, and privacy, when achieved in a balanced manner, benefit the growth of digital trade.

1. Internet Openness and Digital Trade Liberalisation Go Together

Internet openness benefits digital trade for several reasons. As explained earlier, internet openness is not only about technical openness, but also has significant social and economic aspects. For instance, internet openness enhances opportunities for service providers to innovate anywhere and thereby helps them sell their products globally rather than in regional or domestic markets; internet openness also provides greater choice to consumers, in terms of both price and quality.[212] Further, the use of open and global standards and protocols enhances consumer confidence by increasing consumer choice and enhancing security of digital services.[213] Generally speaking, barriers to internet openness also constitute barriers to trade in digital services. However, certain forms of restrictions may be justified to protect the security or stability of the internet, or enhance consumer confidence. In such cases, a more reasoned approach is necessary to distinguish illegal protectionist barriers from legitimate measures allowable under the different exceptions in international trade agreements.

---

210. *See supra* Part III.D.

211. *See infra* Part IV.B.1.

212. *See* Box, *supra* note 67; DRAKE, *supra* note 28, at 36; OECD *Internet Openness*, *supra* note 63, at 9.

213. OECD *Internet Openness*, *supra* note 63, at 8; West, *supra* note 175, at 3.

2. Internet Security Supports Digital Trade

Internet users are increasingly anxious about using digital services that they deem to be less secure—for instance, those services whose databases have been hacked by criminals or foreign governments previously.[214] Consequently, internet users may also avoid using certain digital services that do not use recognised electronic payment services or are offered from countries with poor cybersecurity standards.[215] Therefore, to gain consumer trust and make competitive products for a global market, digital service providers should be able to adopt higher levels of innovation in security of their services.[216] Thus, internet security plays a critical role in supporting digital trade.

In certain cases, cybersecurity standards can also become an impediment to free digital trade. For example, China mandates the adoption of indigenous standards that are believed to be less secure and transparent than open standards.[217] Further, the Chinese government demands access to encryption keys as well as source code used in digital services,[218] thereby also increasing the risk of surveillance and trade secret theft from foreign companies. Such measures not only deter foreign service providers from entering the domestic market but also adversely affect consumers of digital services. In a similar vein, some countries block certain foreign websites or services as they do not consider their underlying technology to be secure enough.[219] This blockage may result in depriving consumers of

---

214. *See, e.g.*, Nicolas Rivero, *The Biggest Data Breaches of All Time, Ranked*, QUARTZ (Nov. 30, 2018), https://qz.com/1480809/the-biggest-data-breaches-of-all-time-ranked/ [https://perma.cc/9L6V-SKE9] (archived Jan. 20, 2019).

215. Internet Soc'y Press Release, *supra* note 147.

216. DANIEL CASTRO & ALAN MCQUINN, INFO. TECH. & INNOVATION FOUND., UNLOCKING ENCRYPTION: INFORMATION SECURITY AND THE RULE OF LAW 9, 35 (2016), http://www2.itif.org/2016-unlocking-encryption.pdf?_ga=2.32927998.1310045406.1547316400-115360438.1547316400 [https://perma.cc/HC2G-67NW] (archived Feb. 6, 2019).

217. *See* NATHANIEL AHRENS, CTR. FOR STRATEGIC & INT'L STUDIES, NATIONAL SECURITY AND CHINA'S INFORMATION SECURITY STANDARDS (2012), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/121108_Ahrens_NationalSecurityChina_web.pdf [https://perma.cc/W2EL-EFUJ] (archived Jan. 20, 2019); *see also* Hill, *supra* note 62, at 54.

218. Microsoft and International Business Machines Inc. have provided their source code to the Chinese government, in order to sell their digital products in the domestic market. *See* Theodore H. Moran, *Should US Tech Companies Share Their "Source Code" with China?*, PETERSON INST. FOR INT'L ECON.: REAL TIME ECON. ISSUES WATCH (Oct. 27, 2015, 10:45 AM), https://piie.com/blogs/realtime-economic-issues-watch/should-us-tech-companies-share-their-source-code-china [https://perma.cc/8EPE-7X3S] (archived Jan. 20, 2019).

219. *See, e.g.*, *U.K. Cybersecurity Chief Wants National Filter to Block "Bad Addresses",* CBS NEWS (Sept. 14, 2016), http://www.cbsnews.com/news/u-k-cybersecurity-chief-wants-filter-to-block-bad-addresses/ [https://perma.cc/9EQV-9QSV] (archived Jan. 20, 2019); Leonhard Weese, *What Does China's VPN Ban Really Mean?*, FORBES (Jan. 25, 2017), http://www.forbes.com/sites/leonhardweese/2017/01/25/what-

high-quality and competitively-priced digital services even when there are no security concerns.[220] However, achieving a high level of internet security implies adoption of reasonable standards that enable data flows; thus, if this principle is implemented in its spirit, such restrictive standards can be eliminated, giving way to more global and innovative cybersecurity standards.

3. Internet Privacy Is a Precondition for Digital Trade

Implementing internet privacy is increasingly recognised as one of the fundamental requirements for digital trade. Recent PTAs recognise the importance of ensuring the trust and confidence of users of electronic commerce, including a sound framework for protecting personal data.[221] Particularly after certain recent exposures involving massive privacy breaches by digital giants such as Facebook, users are more aware of privacy policies of companies and are likely to prefer those which ensure more privacy for their users.[222] Moreover, cross-border trade in digital services will only grow in an environment where individual users do not feel threatened by service providers, particularly by how they control/use their data. In that context, the EU has argued consistently that trade and data protection should go together.[223]

---

does-chinas-vpn-ban-really-mean/#6e6963c2efdc [https://perma.cc/ZQ7J-ADP7] (archived Jan. 20, 2019).

220. *See, e.g.*, Andrew Roth, *Russia blocks millions of IP addresses in battle against Telegram app*, THE GUARDIAN (Apr. 17, 2018), https://www.theguardian.com/world/2018/apr/17/russia-blocks-millions-of-ip-addresses-in-battle-against-telegram-app [https://perma.cc/ZMG8-QBZN] (archived Jan, 20, 2019).

221. *See, e.g.*, CPTPP, *supra* note 16, art. 14.8; Comprehensive Economic and Trade Agreement, Can.-E.U., art. 16.4, Oct. 30, 2016, O.J. (L 11) 23; Free Trade Agreement, China-S. Kor., art. 13.5, June 1, 2015, http://fta.mofcom.gov.cn/korea/annex/xdzw_en.pdf [https://perma.cc/5QEG-QD32] (archived Feb. 6, 2019); Agreement Establishing the ASEAN-Australia, New Zealand Free Trade Area (AANZFTA) art. 7, Feb. 27, 2009, https://dfat.gov.au/trade/agreements/in-force/aanzfta/official-documents/Pages/agreement-establishing-the-asean-australia-new-zealand-free-trade-area-aanzfta.aspx [https://perma.cc/HJK3-T2JV] (archived Jan. 20, 2019); Council Decision 2011/265, art. 7.48.2, Dec. 13, 2015, 2011 O.J. (L 127) (EU).

222. For a succinct summary of the Cambridge Analytica scandal concerning Facebook, see Michael Riley et al., *How the Facebook Cambridge Analytica Scandal Unfolded*, BLOOMBERG (Mar. 21, 2018), https://www.bloomberg.com/news/articles/2018-03-21/understanding-the-facebook-cambridge-analytica-story-quicktake [https://perma.cc/M2MP-VNWZ] (archived Jan. 20, 2019).

223. *Communication from the Commission to the European Parliament and the Council*, *Exchanging and Protecting Personal Data in a Globalised World*, sec. I.3 COM (2017) 7 final (Jan. 10, 2017).

C. *Applying and Interpreting Principles of International Trade Law*

Principles of internet governance are not binding in international law. Wolfgang Kleinwachter argues that the adoption of resolutions and recommendations by intergovernmental organisations, such as the G8 and the OECD, and individual countries, such as the EU and the United States, on issues related to internet governance such as free flow of information, privacy, and cybersecurity, marks a "policy shift" towards a soft law approach that is addressed to the internet multistakeholder community.[224] Joanna Kulesza argues that principles of internet governance found in multistakeholder declarations such as the Tunis Agenda constitute soft law.[225] She also argues that as principles of internet governance mature further, they may evolve into a "customary framework" and "general principles of international internet law."[226] However, these arguments are not universally accepted, and, at best, there is a weak case to argue that internet governance principles are soft law principles.

Nonetheless, the principles of internet openness, security, and privacy can help in applying international trade agreements such as GATS or PTAs. Under the general exceptions, a WTO panel could assess whether a GATS-inconsistent measure may be justified on various grounds such as protecting public morals or public order (GATS Article XIV(a)), or obtaining compliance with GATS-consistent domestic laws, including privacy and/or cybersecurity laws (GATS Article XIV(c)).[227] Some examples include the Chinese Firewall, which prevents data flows into China from several websites, and the GDPR, which places restrictions on how data transfers are conducted to countries outside of the EU.[228] Here, it might be useful to assess how these measures affect the balance between internet openness, security, and privacy, particularly their technical efficacy in achieving the said policy objectives. These factors could form important evidence in assessing the necessity of the measures to achieve the said objectives,

---

224. Wolfgang Kleinwachter, *Internet principle hype: how soft law is used to regulate the Internet*, AFRICANN, (July 25, 2011), https://lists.afrinic.net/pipermail/africann/2011-August/003811.html [https://perma.cc/6VXW-68K9] (archived Jan. 20, 2019).

225. KULESZA, *supra* note 122, at 136–38, 144–55.

226. *Id.*

227. Marrakesh Agreement, *supra* note 22, Annex 1B, art. XIV.

228. The term "Great Firewall of China" was coined by Barme and Ye, referring to the online censorship and surveillance tools employed by the Chinese Ministry of Public Security. *See* Geremeie R. Barme & Sang Ye, *The Great Firewall of China*, WIRED (Jan. 6, 1997, 12:00 PM), https://www.wired.com/1997/06/china-3/ [https://perma.cc/Y8AA-TXH2] (archived Jan. 20, 2019); *see also* Human Rights Watch, *How Censorship Works in China: A Brief Overview*, HUMAN RIGHTS WATCH VOL. 18, NO. 8(C), 9 (2006), https://www.hrw.org/reports/2006/china0806/china0806webwcover.pdf [https://perma.cc/9Q23-CUDE] (archived Jan. 20, 2019).

as well as exploring other less restrictive alternative measures.[229] Thus, WTO Panels will need a basic understanding of the impact of data restrictive measures on the balance between openness and security or privacy in the internet network to make an informed assessment under the GATS exceptions.[230] In doing so, the panels already have options such as examining *amicus curiae* briefs from relevant international institutions or civil society bodies that are submitted in a dispute[231] as well as inviting technical or policy experts to provide input or technical evidence on relevant issues.[232]

The assessment of a data restrictive measure under GATS Article XIV primarily entails balancing international trade obligations and domestic policy. However, in the context of cross-border data flows, another evident conflict is that between a government's understanding of how the internet should be regulated and the multistakeholder principles of internet openness, security, and privacy.[233] The latter conflict is much harder to address in WTO law as internet norms or standards are typically prepared either by private bodies or multistakeholder internet governance institutions and thus have no legal effect.[234] However, certain experts argue that since informal lawmaking through multistakeholder declarations or private standards is common in certain fields of governance (like internet governance), their relevance cannot be completely ignored in interpreting WTO agreements.[235] The existing jurisprudence in WTO law however suggests that applying such standards is very difficult in practice,[236] thus placing limits on using principles derived from international declarations and extralegal technical codes.

---

229. *See, e.g.*, DIANE DESIERTO, PUBLIC POLICY IN INTERNATIONAL ECONOMIC LAW: THE ICESCR IN TRADE, FINANCE, AND INVESTMENT 189–206 (2015); John B. Morris, Jr., *Injecting the Public Interest into Internet Standards*, *in* OPENING STANDARDS: THE GLOBAL POLITICS OF INTEROPERABILITY 11 (Laura DeNardis et al. eds., 2011).

230. *See supra* Part 0.D (discussing complementarity of internet openness, security and privacy).

231. Appellate Body Report, *United States—Import Prohibition of Certain Shrimp and Shrimp Products*, ¶¶ 105–08, WT/DS58/AB/R (Oct. 12, 1998).

232. Marrakesh Agreement, *supra* note 22, Annex 2, art. 13.2.

233. *See* Gunther Teubner & Peter Korth, *Two Kinds of Legal Pluralism: Collision of Transnational Regimes in the Double Fragmentation of World Society, in* REGIME INTERACTION IN INTERNATIONAL LAW: FACING FRAGMENTATION 23, 23–53 (2012).

234. *See, e.g.*, Memorandum from S. Hambridge on Netiquette Guidelines, *supra* note 11; *see also* Biel Company, *A Public Law Approach to Internet Standard Setting*, 7 GOETTINGEN J. INT'L L. 49, 54–61 (2016).

235. JOOST PAUWELYN, CONFLICT OF NORMS IN PUBLIC INTERNATIONAL LAW: HOW WTO LAW RELATES TO OTHER RULES OF INTERNATIONAL LAW 269 (2003); Joost Pauwelyn, *Rule-Based Trade 2.0? The Rise of Informal Rules and International Standards and How They May Outcompete WTO Treaties*, 17 J. INT'L ECON. L. 739, 748 (2014).

236. For example, both in *United States—Gambling* and *Argentina—Financial Services*, the WTO AB did not consider the standards set by Financial Task Action Force

D. *Framing New Rules on Cross-Border Data Flows and Data Localisation*

Despite their limited relevance in applying and interpreting international trade law, the principles of internet openness, security, and privacy can be highly relevant and informative in framing new rules on cross-border data flows and data localisation. Currently, these two issues are very topical at the WTO and are also being negotiated in other PTAs. For example, several of the proposals submitted by WTO members refer to the importance of the free flow of data to electronic commerce, removing data localisation barriers, and building an open, secure, and reliable regulatory environment for electronic commerce, including issues of privacy, consumer protection, and cybersecurity.[237] Similarly, recent PTAs such as the CPTPP and United States-Canada-Mexico Agreement (USMCA)[238] contain provisions on cross-border data flows and data localisation, as well as certain basic requirements for implementing a regulatory framework on data protection and undertaking cooperation on cybersecurity issues.[239]

GATS is a pre-internet era treaty and was not designed for contextualising trade in a digital world; thus, internet security and privacy were not recognised as essential preconditions for the free flow of services across borders. The only tool available under GATS is for WTO members to argue that their cybersecurity or privacy measures fall under the existing exceptions, presuming that internet security and privacy are only relevant in the domestic context but not in a global or transnational context. This deficiency however could be addressed by acknowledging the role of internet security and privacy in enhancing the free flow of data and prohibiting data localisation. Further, domestic regulations in the field of electronic commerce could be adopted that ensure an appropriate balance between internet openness, security, and privacy in the domestic regulatory framework

---

relevant for the legal analysis. *US—Gambling*, *supra* note 21; Appellate Body Report, *Argentina—Measures Relating to Trade in Goods and Services*, WTO Doc. WT/DS453/AB/R and Add.1 (adopted May 9, 2016).

237. *See, e.g.*, Work Programmed on Electronic Commerce, Communication from Canada, Chile, Colombia, Côte d'Ivoire, the European Union, the Republic of Korea, Mexico, Montenegro, Paraguay, Singapore and Turkey, *Trade Policy, the WTO and the Digital Economy*, WTO Doc. JOB/GC/116, JOB/CTG/4 JOB/SERV/248, JOB/IP/21 JOB/DEV/42 (Jan. 13, 2017); Work Programme on Electronic Commerce, *Non-Paper for the Discussions on Electronic Commerce/Digital Trade from Japan*, WTO Doc. JOB/GC/100 (July 25, 2016); Work Programme on Electronic Commerce, *Non-Paper from the United States*, WTO Doc. JOB/GC/94 (July 4, 2016).

238. Agreement Between the United States of America, the United Mexican States, and Canada, art. 19, Nov. 30, 2018, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between [https://perma.cc/87RL-JTLD] (archived Feb. 6, 2019).

239. *See* Mishra, *supra* note 17.

for digital trade. Seventy-one countries (including the EU, as a whole) are now involved in plurilateral discussions and negotiations on electronic commerce at the WTO, including on the above issues.[240] In each of these cases, the principles of internet governance can be instructive in devising balanced rules by considering the open architecture of the internet and its complex interplay with the security and privacy features.[241]

V. TYING MULTISTAKEHOLDER AND MULTILATERAL PROCESSES TO SUPPORT DIGITAL TRADE

Both international trade law and internet governance principles are directed towards forming a globally connected world. While rules in WTO law are aimed at enabling global, integrated markets, thus creating a level playing field for businesses across all member countries, the internet governance regime is directed towards forming a global, interconnected communications network that supports seamless transactions. Hence, several experts have suggested that these parallel tracks of multilateral negotiations in international trade law should be coordinated with multistakeholder processes in internet governance to achieve optimal results.[242]

The idea of collaborating across different international institutions is not entirely new to trade institutions such as the WTO. Previously, WTO members recognised that cooperation between the WTO and other international organisations such as the World Bank and the International Monetary Fund was necessary to "achiev[e] greater coherence in global economic policymaking."[243] In the Declaration on the Contribution of the World Trade Organization to Achieving Greater Coherence in Global Economic Policymaking, WTO members agreed that incoherence in the global economic system

240. World Trade Organization, Joint Statement on Electronic Commerce, WTO Doc. WT/MIN(17)/60 (Dec. 13, 2017).

241. *See* Andrew D. Mitchell & Neha Mishra, *Data at the Docks: Modernizing International Trade Law for the Digital Economy*, 20 VAND. J. ENT. & TECH. L. 1073, 1127–29 (2017).

242. *See, e.g.*, PETER F. COWHEY & JONATHAN D. AARONSON, DIGITAL DNA: DISRUPTION AND THE CHALLENGES FOR GLOBAL GOVERNANCE 233–58 (2017); William J. Drake, *Background Paper for the Workshop on Data Localization and Barriers to Transborder Data Flows* 20 (World Econ. Forum, Sept. 14–15, 2016). *But see* Steven Burnstein & Erin Hannah, *The WTO And Institutional (In)Coherence in Global Economic Governance*, *in* THE OXFORD HANDBOOK ON THE WORLD TRADE ORGANIZATION 778, 801 (Amrita Narlikar et al. eds., 2012).

243. World Trade Organization, Declaration on the Contribution of the World Trade Organization to Achieving Greater Coherence in Global Economic Policymaking ¶ 5 (Dec. 15, 1993), https://www.wto.org/english/docs_e/legal_e/32-dcohr.pdf [https://perma.cc/SA2A-KMWZ] (archived Feb. 6, 2019).

arising due to issues "outside the trade field," "cannot be redressed through measures taken in the trade field alone."[244] A similar initiative may be critical to achieve coherence in international law governing cross-border data flows.

The collaboration between trade institutions such as the WTO and multistakeholder internet governance institutions is also essential for reasons of expediency. Trade negotiations are typically slow and often do not yield concrete results. On the other hand, internet multistakeholder bodies are more experienced in dealing with the informal and dynamic nature of technical standard setting on internet policy issues. [245] For example, as soon as the engineers at IETF become aware of privacy or security risks in an internet protocol, they can immediately fix it.[246] However, if governments set these standards through trade agreements, they cannot be addressed as expeditiously.[247]

Several initiatives are now underway to increase cross-sectoral engagement between the international trade and internet communities, despite the distinct cultures of both fields.[248] The WTO Public Forum in the last three years brought together trade experts, academics, internet policy advocates, companies, and human rights institutions under one roof to openly discuss different facets of electronic commerce and how they affect various stakeholders.[249] The issue of cross-border data flows was one of the most highly debated issues.[250] Trade experts are also showing more willingness to participate in open fora such as the IGF. The last few IGFs have included dedicated sessions on trade and internet governance, which

---

244. *Id.*

245. *See* Stavros Gadinis, *Three Pathways to Global Standards: Private, Regulator and the Ministry Networks*, 109 AM. J. INT'L L. 1, 1–2 (2015).

246. John B. Morris Jr., *Injecting the Public Interest into Internet Standards*, *in* OPENING STANDARDS: THE GLOBAL POLITICS OF INTEROPERABILITY 3, 5 (2011).

247. *Id.* at 7.

248. *Id.* at 8.

249. *See, e.g.*, WTO Public Forum 2018, Session 76 Summary, *Data Localisation: Balancing Trade Disciplines and National Policy Objectives* (Oct. 4, 2018), https://www.wto.org/english/forums_e/public_forum18_e/rep_76.pdf [https://perma.cc/8EZD-L4M9] (archived Feb. 6, 2019); WTO Public Forum 2018, Session 17, *Trust, Trade and Technology: E-commerce that Works for Consumers* (Oct. 2, 2018), https://www.wto.org/english/forums_e/public_forum18_e/pf18programme_e. htm [https://perma.cc/93MC-LYLF] (archived Feb. 6, 2019); WTO Public Forum 2017, Session 83, *Could WTO E-Commerce Proposals Help Development?* (Sept. 28, 2017), https://www.wto.org/english/forums_e/public_forum17_e/pf17programme_e.htm [https://perma.cc/NZ4G-XP9Z] (archived Feb. 6, 2019); WTO Public Forum 2017, Session 35, *What Are the Potential Implications of Recent WTO Ecommerce Proposals on Digital Industrial Policy?* (Sept. 27, 2017), https://www.wto.org/english/forums_e/public_forum17_e/pf17programme_e.htm [https://perma.cc/NZ4G-XP9Z] (archived Feb. 6, 2019).

250. *See, e.g.*, WTO Public Forum 2018, Session 76 Summary, *supra* note 249; WTO Public Forum 2018, Session 17, *supra* note 249; WTO Public Forum 2017, Session 83, *supra* note 249; WTO Public Forum 2017, Session 35, *supra* note 249.

included both trade negotiators and internet policy experts, and discussed very openly as to how trade and non-trade values can be balanced in regulating cross-border data flows.[251] Even a joint study on electronic commerce issues by the WTO and relevant internet governance institutions can assist in developing a better understanding of trade and non-trade issues related to cross-border data flows.

VI. CONCLUSION

International trade law cannot be isolated from internet governance. This Article argues that trade rules are or can be compatible with the idea of a globally connected and secure internet, particularly through the principles of internet openness, security, and privacy. Further, a possibility also exists of applying the principles of internet openness, security, and privacy in evaluating data restrictive measures in international trade law, despite their nonbinding nature, particularly as technical or factual evidence. This Article also points out the importance of internet security and privacy for enabling the free flow of data. However, the majority of international trade agreements, including the multilateral framework of GATS, were designed well before the current digital economy era, and hence, do not contain relevant provisions. Recent PTAs have, however, taken a more informed, comprehensive approach in their Electronic Commerce Chapters, and there is increasing pressure to replicate such provisions in WTO agreements. In that context, the principles of internet openness, security, and privacy can be highly informative in the shaping of a balanced and appropriate regulatory framework for cross-border data flows. Therefore, despite the evident nonbinding nature of technical codes and high-level principles governing the internet, trade negotiators should pay close attention to these principles while devising new rules on data flows and data localisation and aim to bridge the existing gaps between trade rules and the global governance framework for the internet and data flows.

---

251. For notes of the author from the 2018 Internet Governance Forum sessions, see U.N. INTERNET GOVERNANCE FORUM, https://www.intgovforum.org/multilingual/ (last visited Mar. 13, 2019) [https://perma.cc/9YX8-HDJP] (archived Feb. 25, 2019).