Mishra, Neha

Working Paper

International trade, Internet governance and the shaping of the digital economy

ARTNeT Working Paper Series, No. 168

Provided in Cooperation with:
Asia-Pacific Research and Training Network on Trade (ARTNeT), Bangkok

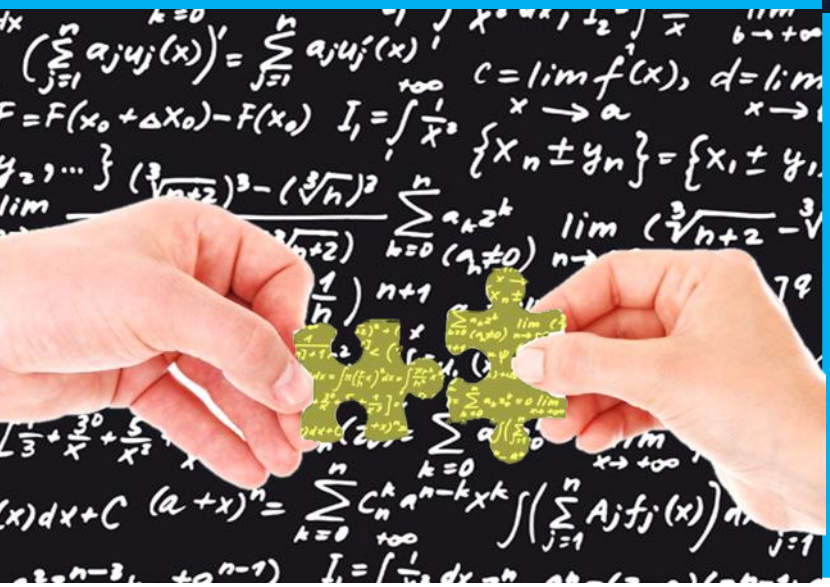
Suggested Citation: Mishra, Neha (2017) : International trade, Internet governance and the shaping of the digital economy, ARTNeT Working Paper Series, No. 168, Asia-Pacific Research and Training Network on Trade (ARTNeT), Bangkok

This Version is available at:
https://hdl.handle.net/10419/167330

ARTNeT

UNITED NATIONS ESCAP
Economic and Social Commission for Asia and the Pacific

International trade, Internet governance and the shaping of the digital economy



Neha Mishra

ASIA-PACIFIC RESEARCH AND TRAINING NETWORK ON TRADE

Working Paper

NO. 168 | 2017

The Asia-Pacific Research and Training Network on Trade (ARTNeT) is an open regional network of research and academic institutions specializing in international trade policy and facilitation issues. AFD, UNCTAD, UNDP, ESCAP and WTO, as core network partners, provide substantive and/or financial support to the network. The Trade, Investment and Innovation Division of ESCAP, the regional branch of the United Nations for Asia and the Pacific, provides the Secretariat of the network and a direct regional link to trade policymakers and other international organizations.

The ARTNeT Working Paper Series disseminates the findings of work in progress to encourage the exchange of ideas about trade issues. An objective of the series is to publish the findings quickly, even if the presentations are less than fully polished. ARTNeT Working Papers are available online at www.artnetontrade.org. All material in the Working Papers may be freely quoted or reprinted, but acknowledgment is requested, together with a copy of the publication containing the quotation or reprint. The use of the Working Papers for any commercial purpose, including resale, is prohibited.

Disclaimer:

The designations employed and the presentation of the material in this Working Paper do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. Where the designation “country or area” appears, it covers countries, territories, cities or areas. Bibliographical and other references have, wherever possible, been verified. The United Nations bears no responsibility for the availability or functioning of URLs. The views expressed in this publication are those of the author(s) and do not necessarily reflect the views of the United Nations. The opinions, figures and estimates set forth in this publication are the responsibility of the author(s), and should not necessarily be considered as reflecting the views or carrying the endorsement of the United Nations. Any errors are the responsibility of the author(s). The mention of firm names and commercial products does not imply the endorsement of the United Nations.

ASIA-PACIFIC RESEARCH AND TRAINING NETWORK ON TRADE

WORKING PAPER

International trade, Internet governance and the shaping of the digital economy[†]

Neha Mishra[*]

Please cite this paper as: Neha Mishra (2017), "International trade, Internet governance and the shaping of the digital economy", ARTNeT Working Paper Series, No. 168, June 2017, Bangkok, ESCAP.

Available at: http://artnet.unescap.org

[†] This working paper is derived from ongoing research of the author related to her doctoral thesis on studying the interface between international trade law and Internet governance. Any comments and inputs on the working paper are welcome, and can be directly sent to the author at nmishra@student.unimelb.edu.au.

[*]PhD Candidate, Melbourne Law School, MPP (NUS), LLM (LSE), B.A. LL.B. Hons (NLSIU). The author gratefully acknowledges the support of the Australian Government Research Training Program Scholarship. She would like to thank Mia Mikic, Tania Voon and Andrew Mitchell for their very helpful comments and insights on earlier drafts. All errors and omissions in this are her own.

Abstract

The interface between trade and Internet governance is one of the most complex policy challenges in the current-day digital economy. This working paper highlights the following observations and findings on the delicate and complex relationship between international trade and the Internet:

- Recent preferential trade agreements (PTAs) such as the *Trans-Pacific Partnership Agreement* (TPP) and the *Japan – Mongolia Economic Partnership Agreement* (Japan – Mongolia FTA) contain legal provisions on cybersecurity, data protection, data localisation, consumer protection, net neutrality, spam control, and protection of online intellectual property, intended to facilitate electronic commerce and enable cross-border data flows. However, these provisions will also have a lasting impact on important aspects of Internet regulation. Similar provisions are likely to appear in other ongoing trade deals such as the *Trade in Services Agreement* (TISA) and the renegotiation of *North American Free Trade Agreement* (NAFTA)
- International trade law does not contain adequate tools to address all aspects of Internet data flows because: (a) Internet is not just an important platform for trade, but also a site for political, cultural and social engagement – the latter aspects largely relate to the domestic regulatory space of countries and fall outside the scope of international trade law; (b) trade lawyers and policy-makers have insufficient knowledge of the technical and policy aspects of the Internet; and (c) the ideological divide between countries on issues including online censorship and surveillance, cybersecurity and privacy (which deeply impact cross-border data flows) cannot be resolved through international trade agreements. Yet, many issues related to Internet policy are also central to trade in digital economy, and thereby, not entirely avoidable in international trade law.

- Internet openness, security and trust are fundamental to the governance of Internet data flows. Measures designed to enforce Internet security and Internet trust, when implemented in a well-reasoned and proportionate manner, do not act as impediments to Internet openness— to the contrary, these measures play an essential role in facilitating efficient and secure data flows through the Internet. Thus, issues of cybersecurity, privacy and data protection can not only act as barriers to electronic commerce, but also facilitate electronic commerce – this perspective necessitates a reorientation of legal provisions in trade agreements.
- International trade institutions should explore both formal and informal means to engage with the Internet policy community in course of dialogues and/or trade negotiations within the World Trade Organization (WTO) as well as bilateral and plurilateral trade agreements, and in multistakeholder platforms such as the Internet Governance Forum. Further, international trade tribunals can rely on the technical and policy expertise of the Internet community to resolve certain complex trade disputes in international trade law.

Key words: International trade agreements, Internet governance, cross-border data flows, Internet openness, Internet security, Internet trust

JEL codes: K33, K39

Table of contents

1. Introduction

The transformation of the Internet from a research network to a platform for online commerce and trade presents new challenges for international trade law. The multilateral framework of the World Trade Organization (WTO) was developed more than two decades ago – as a result, most WTO agreements, including *General Agreement on Trade in Services* (GATS)[1] and the *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS),[2] are inadequate in dealing with complex issues of the current-day digital economy. One of such complex issues is the interface between international trade law and the governance of the Internet visible in different areas such as regulation of cross-border flows of data, cybersecurity, privacy and data protection, online consumer protection, protection of online intellectual property rights, and net neutrality. Although the fields of international trade and Internet governance appear to be disconnected (Weber, 2014a, p. 32), the growing significance of the Internet as a platform for international trade (Meltzer, 2016) is creating an intricate and delicate relationship between these fields (Aaronson, 2015; Burri, 2016; Belli and Marcel, 2016). This paper examines various facets of this relationship, in the specific context of cross-border data flows, and related issues of privacy, cybersecurity and online consumer protection, and reflects on policy approaches that may address the growing conflict between liberalisation in the digital economy and protecting important policy goals in cyberspace.

A complex, two-way interaction exists between governance of the Internet and international trade, which in turn has deep repercussions on the development of the digital economy. In recent years, several countries have imposed measures restricting cross-border data flows on several grounds including enforcement of domestic privacy and cybersecurity regulations or standards, protection of national security, protection of public order or public morals, and less obviously, to boost their domestic digital sector (DeNardis, 2009). As several studies have already established, such measures have a

[1] *Marrakesh Agreement Establishing the World Trade Organization*, opened for signature 15 April 1994, 1867 UNTS 3 (entered into force 1 January 1995), annex IB (*General Agreement on Trade in Services*) (GATS).
[2] *Marrakesh Agreement Establishing the World Trade Organization*, opened for signature 15 April 1994, 1869 UNTS 299 (entered into force 1 January 1995) annex 1C (*Agreement on Trade-Related Aspects of Intellectual Property Rights*) (TRIPS Agreement).

detrimental impact on trade flows not only in relation to the ICT sector or services, but also the manufacturing sector (Manyika et al., 2016; Meltzer, 2015 and2016; Stone et al., 2015; UNCTAD, 2016). Similarly, the European Union standards on data protection (particularly after the *Schrems* case)[3] have had a deep impact on cross-border data flows, particularly between the United States and European Union, and despite the adoption of the Privacy Shield, United States companies which store data of citizens in the European Union outside of its borders continue to face business uncertainty.

To minimise such restrictive measures, countries are now using international trade agreements to adopt binding legal provisions preventing governments from interfering with digital data flows. For example, the Electronic Commerce Chapter of the T*rans-Pacific Partnership Agreement*[4] contains provisions that obligate countries to allow free cross-border data flows and bans data localisation. These provisions are accompanied by other legal requirements on cybersecurity, data protection, consumer protection, net neutrality, spam control, and protection of online intellectual property. Similar provisions are also being proposed in other ongoing international/plurilateral trade negotiations including the *Transatlantic Trade and Investment Partnership* (TTIP),[5] *Trade in Services Agreement* (TISA).[6] *Regional Comprehensive Economic Partnership* (RCEP)[7] and most recently, the renegotiation of the *North American Free Trade Agreement* (NAFTA).[8] While the main purpose of these provisions is to facilitate cross-border data flows necessary for electronic commerce, they also have a deep impact on processes of Internet governance.[9] Thus, the question arises as to how to best balance competing considerations in international trade and Internet governance to enable the development of an open as well as stable and secure digital economy.

---

[3] *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, [2015] ECLI:EU:C:2015:650 (European Court of Justice, Grand Chamber, 6 October 2015).
[4] *Trans Pacific Partnership Agreement*, text released following legal review 26 January 2016 (signed 4 February 2016, not yet in force) ('TPP').
[5] EU Textual Proposal for TTIP Electronic Commerce Chapter, July 2015 (publicly released 31 July 2015), <http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf > 47-50.
[6] The latest draft of the Annex on Electronic Commerce was leaked on 25 May 2016 by Wikileaks. See Wikileaks, TISA Annex on Electronic Commerce <https://wikileaks.org>.
[7] RCEP Working Group on Electronic Commerce, 'Terms of Reference', February 2015 <http://www.bilaterals.org>.
[8] *North American Free Trade Agreement*, signed 17 December 1992, [1994] CTS 2 (entered into force 1 January 1994) ('NAFTA').
[9] Whether this impact is intended or unintended is not as easy to determine at this stage.

This working paper is divided into three sections. Section 2 provides a broad overview of how international trade agreements influence governance of the Internet, referring to specific examples in context of the GATS and more recent preferential trade agreements (PTAs). Section 3 focuses on the regulation of data flows and related issues of security and trust, arguing why and how principles of Internet governance are critical in the development of new disciplines on electronic commerce in relation to cross-border data flows. In making this argument, this section argues that openness, security and trust in the Internet are mutually reinforcing principles, and international trade law needs to align with these principles in order to facilitate to a secure, predictable and open digital economy. Section 4 concludes by highlighting policy approaches that may be helpful in accommodating competing considerations in international trade law and Internet governance in relation to regulation of cross-border data flows.

2. How international trade agreements influence governance of the Internet

The application of international trade law to measures restricting Internet or Internet-related services often entails dealing with policy issues directly related to the governance of the Internet. For example, a country may restrict data flows out of a country to protect privacy or ensure data security. Hypothetically, in a WTO dispute, a panel may find that the measure violates WTO law as it is unrelated to data security or online privacy, or is disproportionate or arbitrarily implemented in achieving these objectives.[10] Conversely, if the panel accepts the legitimacy of the policy objective and the effectiveness of the measure, it might find no violation even if the measure constrains access to the market for foreign companies. In either of these scenarios, the WTO tribunal has to conduct an extensive legal exercise to balance the objectives of international trade law with policy considerations fundamental to the Internet such as cybersecurity and data protection. This analysis is particularly difficult for two reasons: (a) Trade experts lack expertise in technical and policy aspects of Internet regulation on

[10] See, for example, while conducting a legal analysis under GATS art XIV.

issues such as cybersecurity and data protection; and (b) A deep ideological divide exists between countries regarding the extent of regulatory control that should be exercised over the Internet. For example, countries such as China, Vietnam and Russia advocate strong government control over all layers of the Internet network. The European Union considers trade interests secondary to fundamental rights of Internet users, while several other members of the Organisation for Economic Cooperation and Development (OECD) and Asia-Pacific Economic Cooperation (APEC) tend to be more focused on innovation and economic growth (Jamart, 2014, p. 63). The above scenario also presents us with another complicated question – to what extent are issues related to privacy, consumer protection or cybersecurity relevant in international trade law? Should international trade law facilitate free cross-border flows of data? Should cross-border data transfer and related issues of privacy and cybersecurity be addressed through disciplines in international trade law (i.e. are they trade-related)? Or do such issues fit exclusively into the Internet policy and governance domain, although they may affect trade?

Some of the recently concluded PTAs contain provisions on electronic commerce that impact the governance of the Internet. For example, in the Electronic Commerce Chapter of the TPP, some of the provisions directly relate to the regulation of the Internet include:

- TPP art(icle) 14.11 mandates cross-border flows of data and TPP art 14.13 prohibits data localisation, although both these provisions are subject to a broadly worded exception;
- TPP art 14.8 sets out a legal requirement for countries to adopt a legal framework for the protection of personal information;
- TPP art 14.7 requires all member countries to 'adopt or maintain' consumer protection laws for electronic commerce transactions;
- TPP art 14.10 vaguely recognises the principle of net neutrality;
- TPP art 14.17 prohibits its members from mandating sharing of proprietary secrets such as source code, as a condition of market access in its territory for foreign service providers;

- TPP art 14.16 sets out a provision on cybersecurity cooperation among member countries;
- TPP art 14.14.1 requires all TPP parties to "adopt or maintain measures regarding unsolicited commercial electronic messages".

Another recent PTA which contains similarly worded provisions on many of the above areas in its Electronic Commerce Chapter is the *Japan – Mongolia Economic Partnership Agreement* (Japan – Mongolia FTA). [11]

Additionally, certain important PTAs currently under negotiation are also likely to contain disciplines on some of the above areas, although the outcomes of these negotiations are less certain due to strong countervailing factors. For example, the presence of the European Union in the TTIP, and the presence of China in the Regional Comprehensive Economic partnership (RCEP) may make it harder to adopt binding provisions on cross-border data flows, and data localisation. On the issue of data protection and privacy, a sharp divergence exists between the market-centric approach of the United States and some other APEC economies and the highly regulatory approach of the European Union (Mann, 2001, p. 81). The renegotiation of the NAFTA has created another opportunity for the digital lobbies in the United States to push for TPP-type digital trade provisions, which is increasingly finding support in the Office of the United State Trade Representative (USTR) (Intellectual Property Watch, 2017). Similarly, in case of TISA, many of the TPP parties are recommending provisions which adhere to the legal standards prescribed in the Electronic Commerce Chapter of the TPP. Interestingly, Australia, Canada, , the Republic of Korea, Hong Kong, China and Switzerland all have recommended stronger obligations on data protection and privacy, and Internet security, compared to the provisions in the TPP.[12] Finally, in case of the RCEP which is emerging as one of the most important trade agreements in the Pacific-Rim (post the United States' withdrawal of the TPP), many of the TPP issues such as cross-border data flows, privacy and cybersecurity cooperation

[11] *Japan – Mongolia Economic Partnership Agreement*, signed 10 February 2015, entered into force 7 June 2016 ('Japan – Mongolia FTA'). See Japan-Mongolia FTA, art 9.6 dealing with online consumer protection, art 9.7 dealing with spam, art 9.10 dealing with prohibition on data localisation, art 9.11 dealing with involuntary disclosure of source code, and art 9.12 dealing with cooperation on cyber security issues.
[12] Wikileaks, TISA Annex on Electronic Commerce <https://wikileaks.org/tisa/document/20151001_Annex-on-Electronic-Commerce/20151001_Annex-on-Electronic-Commerce.pdf>.

were laid out in the terms of reference.[13] However, given the reticent attitude of China, India, Indonesia and other South-East Asian countries on many of these issues, it is possible that the RCEP might not lay down strong legal obligations on electronic commerce similar to that of the TPP.

The incorporation of Internet policy issues in international trade agreements is a response to the need for greater amount of regulatory coordination or cooperation between countries on areas that impact trade between countries (e.g., privacy, net neutrality, consumer protection, Internet intermediary liability, etc.) as well as removing barriers to Internet data flows (e.g., data localisation). As Internet governance is dispersed across various stakeholders and largely occurs through informal, collaborative mechanisms, international trade law is now being used to fill the gaps through binding rules in many recent PTAs. Many civil society advocates object to this approach for various reasons including the non-transparency of trade negotiations, the lack of expertise within trade institutions to deal with Internet-related issues, the failure to consider social, political and human rights aspects of Internet governance, and the long-term detrimental impact on the organic growth of the Internet (Kaminiski, 2015). While a high level of support exists in the international trade law community to achieve regulatory harmonization/regulatory cooperation and minimise regulatory barriers to trade (Chander, 2012, p.18; Meltzer, 2015), a lack of shared understanding among countries on how to regulate key aspects of the Internet, including data protection, government surveillance and regulation of digital innovation, makes it difficult to achieve this goal in practice.

Further, the inclusion of legal provisions related to Internet-related policy issues may have negligible benefits because these provisions are based on bare minimum standards (see, for example, TPP art 14.8.2 does not refer to any internationally recognised standard of privacy/data protection), subject to broad exceptions whose interpretation remains uncertain (eg, art 14.11.2 and 14.13.2 refers to “legitimate public policy objective”) and often dependant on the political will of participating countries because of the non-binding nature of many provisions (for example, net neutrality or

[13] RCEP Working Group on Electronic Commerce, ‘Terms of Reference’ (February 2015).

cooperation on cybersecurity in the TPP). Despite aiming to establish greater amount of harmonization and coordination in the regulations governing digital economy, these provisions effectively pave a path for weak standards on cybersecurity, data protection etc. (Mishra, 2017). Further, Internet governance experts would argue that most appropriate platform to deliberate on such issues should remain open and transparent such as the Internet Governance Forum or the Internet Society, so as to fulfil the basic requirements of due process, political participation, freedom of expression, and rule of law.[14]

The application of international trade law should be aligned with basic values of Internet governance, to strike a reasoned balance between promoting the Internet as a platform for trade, protecting rights of Internet users, and continuing to enable innovation. In the specific context of digital data flows and related policy issues, the next section outlines how and why principles of Internet governance will play an important role in the development and application of international trade law.

3. Regulation of digital data flows in international trade law: Why principles of Internet governance matter?

Most international trade agreements do not directly regulate data flows.[15] However, when international trade law is applied to measures that restrict or obstruct data flows, international trade law effectively determines the legitimacy of certain categories of data flows, as described earlier. However, the Internet is a complex phenomenon and is driven not only by economic factors (such as promoting trade flows or promoting opportunities for economic innovation) but also important considerations related to political and social engagement, technical efficiency and even, cultural and moral considerations. As a result, international trade law, by itself, does not necessarily provide sufficient tools to a tribunal to decide how a particular measure restricting digital data flows affects the larger governance framework of the Internet.

[14] See, for example, the Brussels Declaration on Trade and the Internet, 22 February 2016, <http://www.ifla.org/files/assets/clm/brussels_declaration.pdf>.
[15] However, see TPP art 14.11 and art 14.13.

Internet governance and regulation of data flows

The Internet governance regime encompasses rules, principles and institutions governing technical or policy aspects of the Internet (Kulesza, 2012, pp.61, 136-8, 144-55). The norms and principles of Internet governance are contained in various declarations, resolutions, memos and recommendations of international organisations, as well as day-to-day practices and shared understandings between various stakeholders dealing with the policy and technical administration of the Internet.[16] With regard to regulation of data flows, Internet governance aims to marry the technical features of the Internet network (based on an open, end-to-end design) with other important policy considerations to ensure trust and safety of users. So what are these key principles in Internet governance that apply to information flows via the Internet? This section focuses on *Internet openness, Internet security* and *Internet trust* as being fundamental to the governance of Internet data flows. Given the amorphous nature of Internet regulation, *Internet openness, Internet security* and *Internet trust* should be viewed as aspirational tools rather than fixed or binding benchmarks, which facilitate achieving a higher degree of openness, stability, interoperability, security and trust in the network (Drake et al, 2016, p. 10; ISOC, 2013; OECD, 2016, p.15).

Internet openness refers to the "global free flow of data across the network" without unnecessary disruptions or controls (Box, 2016, p. 1). In other words, Internet openness refers to the easy transfer and exchange of data packets as a result of the open, end-to-end architecture of the Internet (Global Commission on Internet Governance, 2016, p. vi; Garfinkel, 2003; Solum, 2009, pp. 63-4). [17] Several

[16] See, eg, the United Nations ('UN')-sponsored World Summit on Information Society ('WSIS') adopted *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6(Rev. 1)-E, 18 November 2005 ('Tunis Agenda'). The Internet Engineering Task Force ('IETF') circulates memos called Request for Comment ('RFC') which 'contain technical and organizational notes about the Internet'. 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, for eg, IETF, 'Netiquette Guidelines', RFC 1855 (October 1995); IETF, 'Ethics and the Internet' (January 1989); IETF, 'The TLS Protocol Version 1.0' (January 1999)). The UN General Assembly has adopted various resolutions on cybersecurity and privacy. See, eg, *GA Res 68/167: The Right to Privacy in the Digital Age*, Resolution adopted by the General Assembly on 18 December 2013, 68th session UN Doc A/RES/68/167 (21 January 2014); *GA Res 64/211: Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures*, Resolution adopted on 21 December 2009, 64th session, Agenda Item 55(c), UN Doc A/RES/64/211 (17 March 2010).

[17] Global Commission on Internet Governance, 'One Internet' (CIGI and Chatham House, 2016) vi; Simson Garfinkel, 'The End of End-to-End?' (1 July 2003) *MIT Technology Review* (online); Lawrence B Solum,

instruments recognise the importance of 'free flow of information', which is important both from a commercial and human rights point of view (Damon, 1986, pp. 268-71).[18] The idea of Internet openness aligns with the idea of free flow of information (in the context of online transactions and communications).[19] Although the virtues of Internet openness are accepted by the Internet community as whole, and by some individual governments, certain countries (e.g., China, the Russian Federation) are also opposed to surrendering sovereign power over regulating information flows (Jensen, 2015; Xinmin, 2015; Mueller, 2010, p.3). These ideological differences are also reflected in the debate amongst countries in committing to cross-border data flows and prohibiting data localisation measures in international trade agreements (DeNardis, 2016, p. 3).

Internet openness also closely aligns with the idea of liberalisation of trade flows, because Internet openness generally enhances opportunities for economic and digital innovation and thereby facilitates a global marketplace (Box, 2016, p.1; Drake et al., 2016, p. 36). Further, the use of open and global standards and protocols enhances consumer confidence by increasing consumer choice and enhancing security of digital services (OECD, 2016, p.8; West, 2016, p. 3). Barriers to Internet openness also constitute barriers to electronic commerce. However, Internet openness needs to be balanced with other requirements that complement an open network such as preserving security and trust in the system. At this juncture, *Internet security* and *Internet trust* emerge as the other important considerations in the regulation of data flows.

Internet security entails the protection of the integrity of the Internet network, thereby 'preventing unintended or unauthorized access, change or destruction of data'

'Models of Internet Governance' in Lee A. Bygrave and Jon Bing eds, *Internet Governance: Infrastructure and Institutions* (Oxford Scholarship Online, 2009) 48, 63-64; ISOC, 'Internet Invariants: What Really Matters' <https://www.internetsociety.org/internet-invariants-what-really-matters>.

[18] WSIS Declaration of Principles, [4]; Tunis Agenda [4]. Free flow of information is recognised as human right in many treaties – *Universal Declaration of Human Rights* art 19 (not binding, but some scholars recognise it as customary international law), *International Covenant on Civil and Political Rights* art 19 (only binding on signatories).

[19] See, eg, G8, *Deauville G8 Declaration – Renewed Commitment for Freedom and Democracy* (26-27 May 2011) ('*Deauville Declaration*') art II.9; OECD Principles for Internet Policy Making, Principles 1, 2, 4; OECD, *Ministerial Declaration on the Digital Economy* (2016) <https://www.oecd.org/Internet/Digital-Economy-Ministerial-Declaration-2016.pdf> ('Cancún Declaration'); *European Union — United States Trade Principles for Information and Communication Technology Services* (4 April 2011); *Japan — United States Trade Principles for Information and Communication Technology Services* (27 January 2012).

transferred through the networks.[20] The development of protocols or standards on cybersecurity, and management of security risks requires collaboration amongst different stakeholders (particularly in the private sector) (Mueller, 2010, pp. 159-60; Shackelford, 2013, pp. 3-4). As new threats and vulnerabilities emerge every day, implementation of Internet security aims at preserving the fundamental integrity and stability of the network to the greatest extent possible (ISOC, 2013). In practice, different stakeholders attribute different meanings and legal content to Internet security, depending on their political interests and policy objectives, including protecting critical infrastructure, consumers and data, preventing cyberespionage and preventing cybercrimes (ISOC, 2015; OECD, 2016, p. 28; OECD, 2015, pp. 19-20). Further, certain countries use cybersecurity or information security strategies as a disguise to promote other political or economic interests, such as for state surveillance or protecting local companies (Allen-Ebrahimian, 2015; Kopstein, 2015).

Internet security is pertinent to electronic commerce when cybersecurity standards become an impediment to provision of digital products (for example, Government of china has enforced measures in the past to provide access to encryption keys or source code to protect security) (Hill, 2012, p. 54; Moran, 2015). Measures implemented to ensure Internet security can therefore only be justified under exceptions in international trade agreements (e.g., on grounds of national security or to enable online consumer protection).[21] In general, unreasonable standards on Internet security can deter foreign companies and affect consumers of digital services. However, simultaneously, a higher degree of Internet security (e.g., robust technical standards, end-to-end encryption, protection against malware etc.) is essential to facilitate economic transactions via the Internet. Therefore, in implementing Internet security, a delicate balance needs to be struck between: (a) the various perceptions of security held by governments, companies and users; and (b) implementing Internet security harmoniously with other considerations of Internet openness and enhancing user trust (as discussed below).

[20] University of Maryland University College, Cybersecurity Primer <http://www.umuc.edu>.
[21] See GATS art XIV, art XIV bis.

Internet trust refers to the extent to which users can rely on the Internet as a network to share and access information, which is turn derived from other underlying principles relevant to user trust, such as data protection and privacy, and online consumer protection). [22] Privacy and data protection are unanimously recognised as a fundamental concern in Internet governance today, and a key component of Internet trust.[23] Further, both technology companies and governments recognise the importance of having interoperable frameworks on consumer protection, particularly as electronic commerce has enabled cross-border transactions directly between end consumers and sellers. The Internet governance framework recognises the importance of balancing Internet trust with security and openness of the Internet in several policy instruments and declarations.[24]

However, privacy and consumer protection regimes vary from country to country and can also conflict with each other, which in turn creates roadblocks to free flows of data. First, many developing countries have either no or minimal and ineffective privacy and consumer protection laws. Second, in some countries, privacy and consumer protection is considered secondary to other interests such as national security or maintenance of public order. Therefore, in such countries, privacy or protection of consumer interests can be easily compromised for other policy objectives. Finally, many countries with developed privacy regimes have very different approaches to privacy and data protection. In recent years, several countries have also imposed stringent legal checks on data collectors to ensure more transparency in the process of data collection, such as imposing consumer consent requirements before collecting, transferring or using

[22] *Report of the Working Group on Internet Governance* (June 2005), [84]; Tunis Agenda, [47], [39], [41]. Internet trust can also refer to other things, which I do not cover within this definition: (a) trust issues amongst netizens, e.g. C2C trading platforms such as eBay and Alibaba or other services such as online dating; and (b) trust in Internet governance processes, for e.g., domain name allocation by ICANN (Bradshaw, 2015; Hoffman, 2015, p.8).

[23] See, e.g., Tunis Agenda, [39]; OECD, The *OECD Privacy Framework* (2013) <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> ('*OECD Privacy Framework*').

[24] Tunis Agenda, [39]; *OECD Privacy Framework*, [19]; APEC, *APEC Privacy Framework* (November 2004) <http://www.apec.org/Groups/Committee-on-Trade-andInvestment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx> ('*APEC Privacy Framework*'). See also UDHR art 12; ICCPR art 17; *The Right to Privacy in the Digital Age*, 69th session, Third Committee, Agenda Item 68 (b), UN Doc A/C.3/69/L.26/Rev.1(19 November 2014); See also *Guiding Principles on Business and Human Rights*, endorsed by the Human Rights Council in 2011.

personal data of users.[25] Since these regulatory practices and laws are not uniform across most countries, they can often create legal uncertainty for digital service providers operating on a cross-border basis, significantly increasing their compliance costs.

Many countries are attempting to minimise these conflicts in domestic regimes through binding legal mechanisms such as bilateral agreements on data transfer (e.g., European Union-United States Privacy Shield) or by adopting enforceable legal obligations in international trade agreements. For instance, in the TPP although art 14.8.2 and art 14.7 requires all members to adopt a legal framework for protection of personal information and online consumer protection respectively, although due regard is provided to a country's 'regulatory preferences'. It remains uncertain whether such a legal framework in international trade law can enable the necessary legal framework to facilitate user trust, particularly because many of these cross-border regulatory cooperation mechanisms are based on political good will and commitment to an open digital market. Thus, in the case of regulation of data flows, Internet governance principles do not necessarily tie in with the legal obligations in international trade law.

Conclusively, it is reiterated that Internet openness, security and trust can be extremely useful and informative in bringing greater clarity and coherence to the regulation of data flows necessary for conducting various transactions via the Internet. Free data flows can only be facilitated in an environment of Internet security and trust. Conversely, Internet openness facilitates a higher level of innovation in the development of security and trust standards, as well as transparent dialogues between governments regarding the regulation of the Internet. Therefore, cybersecurity, data protection and consumer protection measures, when implemented in a well-reasoned and proportionate manner, do not act as impediments to data flows — to the contrary, these measures play an essential role in facilitating efficient and secure data flows through the Internet. Further, Internet openness is not contrary to Internet trust and security, but rather supports and complements security and trust in the network.

[25] This is mostly being implemented through extensive domestic data protection laws. For e.g., Malaysia, Singapore, Philippines, Republic of Korea and the European Union.

Internet governance and international trade law

The exact legal status of Internet governance principles is unclear in the context of public international law. Kleinwachter (2011) argues that the adoption of resolutions and recommendations by intergovernmental organisations such as the G8 and the OECD, and individual countries such as the European Union 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' which is addressed to the Internet multistakeholder community as a whole constituting of states, businesses, and the civil society. Kulesza (2012) argues that principles of Internet governance found in multistakeholder declarations such as the Tunis Agenda constitute soft law. 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'. These arguments are however not universally accepted, and at best, there is a weak case to argue that Internet governance principles are persuasive in public international law. Internet governance is still largely of a transnational or private nature, particularly in terms of technical administration and implementation of user policies – however, principles derived from these multistakeholder processes remain central to Internet governance.

Internet openness, security and trust introduce a new perspective into international trade law, regarding the role of cybersecurity, data protection and consumer protection in trade in digital services. For instance, they highlight the importance of a consistent and functional transnational legal framework on data protection, online consumer protection and cybersecurity-related issues in order to facilitate Internet data flows (Bieron and Ahmed, 2012, pp. 567-8; Weber, 2014b, p. 11-12). The recent Japan-Mongolia FTA succinctly captures the essence of these principles, and lays out the basic objective of the Electronic Commerce Chapter (Chapter 9) as the 'creation of environment of trust and confidence in the use of electronic commerce' and to 'promote' 'wider use' of electronic commerce.[26] This provision implies that openness in electronic commerce or digital trade (including free cross-border data flows) necessarily

[26] Japan – Mongolia FTA art 9.1.2.

requires trust and security of the Internet network (ISOC, 2013, p.3; West, 2016, p. 5), and thus, legal obligations on electronic commerce contained in the agreement should be interpreted in light of this objective. This approach provides a fine balance between balancing the liberalisation objectives of an international trade agreement and policy considerations fundamental to Internet governance, such as Internet security and trust.

The concepts of Internet openness, Internet security and Internet trust can also help international trade tribunals in the evaluation of complex issues related to electronic commerce such as the application of exceptions in GATS to measures restricting electronic commerce,[27] or determination of whether a data flow-restrictive measure qualifies as a 'legitimate public policy objective' under the TPP.[28] For example, is a specific measure technically efficient in enabling user trust or enhancing Internet security, or is it driven by other policy considerations set out in GATS exceptions (such as protection of public morals, public order etc.)? What is the impact of a specific measure on Internet openness? What is the rational nexus between the measure restricting data flows which is at issue and the policy objective? Is there any other mechanism by which the same policy outcome can be achieved without restricting cross-border data flows, or imposing unreasonable standards? For example, in the context of data localisation, one of the most common means of restricting data flows, a deeper investigation of the fundamental Internet policy considerations reveals that data flow restrictions rarely prevent foreign state surveillance or ensure integrity of personal data – rather they make such domestic servers more vulnerable to targeted cyber-attacks. Further, certain governments block foreign Internet services on grounds of public morals or order, or because these websites harm consumer interests (for e.g., pornography, online gambling websites) even though such content may be freely available on domestic websites, or can be easily accessed by bypassing firewalls. In such a case, a measure banning these foreign websites (and thereby, hampering Internet openness) cannot be justified both on technical and policy grounds.

In order to create a robust and predictable ecosystem for electronic commerce, achieving greater consensus amongst stakeholders on issues of Internet openness,

[27] GATS art XIV; art XIV bis.
[28] TPP art 14.11.3; art 14.13.3.

security and trust will remain critical. Many domestic regulations on the Internet are being enforced without paying due consideration to the global and universal nature of cyberspace, and its relevance for international trade. The digital economy can best develop in an environment where the Internet remains open, stable, secure and trustworthy – thus, the manner in which domestic frameworks on privacy, consumer protection and cybersecurity are developed will influence both Internet governance and international trade. In light of these factors, the inclusion of provisions on Internet-related policy issues in recent PTAs (as discussed in Section 2 above) is a step in the right direction. However, international trade institutions need to develop a more sound understanding of the processes of Internet governance to develop coherence, stability and predictability in the application and interpretation of these provisions. In particular, trade institutions need to remain aware of their limitations, and acknowledge that the international framework for regulation of Internet data flows is contingent on greater interaction and coordination between different domains of expertise including Internet governance, international human rights, and international trade (Wunsch-Vincent, 2012, p.562).

Despite the uncertainty regarding how Internet governance principles can be relevant in international trade law, a vast scope exists for trade policy-makers to learn from the Internet policy community, and adopt better legal frameworks to govern cross-border data flows. As discussed in greater detail in the final concluding section, several multistakeholder platforms and networks contribute significantly to the ongoing dialogues on trade and Internet, and open doors for multilateral institutions such as the WTO as well as regional trade institutions to exchange and share knowledge and experience with the Internet governance community. Given the slow pace of legal reform in international trade law and the important role of non-state institutions in the governance of the Internet, such ongoing policy dialogues will play an instrumental role in building new insights and experimenting with more creative ideas to regulate important issues at the confluence of international trade and the Internet, such as cross-border data flows.

4. Policy approaches: Towards a stronger and resilient digital economy

The discussions in the preceding sections indicate that international trade agreements are important tools in shaping the future of the digital economy. As cross-border data flows are indispensable to the digital economy, international trade agreements should be equipped to respond to the challenges of cyber sovereignty, frequently enforced through disproportionate and burdensome regulatory measures such as data localisation, unreasonable cybersecurity requirements, and lack of interoperability of domestic privacy and consumer protection laws. Thus, understanding the linkages and developing mechanisms to synergise international trade and Internet are not just desirable, but absolutely vital to create a robust and strong digital economy.

Negotiation of international trade agreements enables countries to gain greater understanding of common areas of interest and discord, identification of priority areas and policy rationale behind variable domestic approaches. Even though many ongoing dialogues and negotiations often do not yield concrete or comprehensive results (e.g., the long-standing Work Programme on Electronic Commerce at the WTO), they continue to improve prospects for future coordination on such issues (Hoekman and Mattoo, 2011, pp. 13-14). For example, while many PTAs contain only hortatory provisions on supporting SMEs to participate in electronic commerce,[29] these provisions are nonetheless critical because it can facilitate policy action in the short run (for example, on issues on which political good will exists) or can pave the path for binding norms in the long run. Similarly, the provision on cross-border data flows was non-binding under the KORUS FTA[30] but it laid the foundation for stronger legal obligations under the TPP. Further, trade negotiations enable countries to understand better the limitations of international trade agreements in harmonizing regulations in certain policy areas. With regard to such politically-sensitive issues, countries may be required to liaise with important non-trade institutions (for example, International Telecommunications Union (ITU) or the Internet Governance Forum (IGF)) or pay

[29] Example, TPP Chapter 24.
[30] Consolidated KORUS FTA Text (signed on 30 June 2007, entered into force 15 March 2012) <https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text> art 15.8.

greater deference to domestic values (for example, the domestic ideology on online censorship, provided it is non-discriminatory and non-arbitrary) (Castro and Atkinson, 2014, p. 8).

Internet governance institutions can provide valuable feedback in the development of new disciplines on electronic commerce. Typically, trade deals are negotiated discreetly, so as to enable countries to bargain with each other without being subject to intense public scrutiny. However, the development of the digital economy is not only dependant on rules on open trade, but also the maintenance of a stable and open Internet. Therefore, the WTO and other trade institutions should develop more mechanisms to consult and obtain feedback from Internet governance institutions such as the Internet Engineering Task Force (IETF), World Web Wide Consortium (W3C), Internet Corporation for Assigned Names and Numbers (ICANN), ITU, Internet Society 'ISOC') and IGF, in course of ongoing trade dialogues, or even during various internal meetings and discussions. Even a joint study on electronic commerce issues by the WTO and relevant Internet governance institutions can assist in developing a better understanding of the digital economy. The comprehensive work in institutions such as the OECD, UNCTAD and APEC also provide very useful inputs on developing coherent rules for the digital economy.

Further, if governments remain more open to publicly release their policy stand on electronic commerce issues in a timely manner, it will enable the Internet governance community to provide transparent and meaningful feedback in context of both domestic and international law. The European Union has taken an important step in this direction by releasing its negotiating position on various issues in ongoing trade negotiations. However, such initiatives are generally lacking amongst most developed and developing countries. The online leaks of different chapters of trade agreements can enable greater academic and civil society engagement – however, the very same leaks also indicate lack of transparency, accountability and participation in trade negotiations.

Several initiatives are now underway to increase cross-sectoral engagement between the international trade and Internet community. The WTO Public Forum in 2016 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 it affects various stakeholders. Trade experts are also showing more willingness to participate in open fora such as the IGF. The last IGF included dedicated sessions on trade and Internet governance, which included both trade negotiators and Internet policy experts, and discussed very openly as to how trade and non-trade values can be balanced in the current-day digital economy. Of course, the level of representation from developing countries in many of these platforms will be a critical factor in the development of balanced rules on electronic commerce, given the sharp divide between developing and developed countries on Internet regulation.

Finally, Internet governance principles can inform the interpretation and application of international trade law, albeit to a limited extent. For example, when measures restricting data flows are brought before trade tribunals, the technical and policy ramifications of the measure(s) at issue can be investigated by engaging with external expertise, e.g., *amicus curiae* briefs from relevant international institutions or civil society bodies, or inviting technical/policy experts to provide inputs or technical evidence on relevant issues. Such external expertise can assist the tribunals in balancing trade and non-trade values while investigating measures restricting data flows. International trade law cannot and should not become a site for Internet governance – however, ongoing collaboration between the trade and Internet community is essential to ensure that international trade agreements do not directly or indirectly interfere with or hamper important processes in Internet governance. Thus, efforts should be continued both within the Internet and the trade community to bridge gaps and develop synergies between these two disciplines.

References

Aaronson, S., 2015 “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, no. 4 *World Trade Review* 671-700.

Allen-Ebrahimian, B., (2015). “The ‘Chilling Effect’ of China’s New Cybersecurity Regime”, *Foreign Policy* (online). <http://foreignpolicy.com/2015/07/10/china-new-cybersecurity-law-internet-security/>.

Belli, L., and Marcel, M. “The Quiet Rapprochement of Internet Governance and Trade Policy” on *Diplo* (14 October 2016) <https://www.diplomacy.edu/blog/quiet-rapprochement-internet-governance-and-trade-policy>.

Bieron, B., and Ahmed, U., (2012). “Regulating E-commerce through International Policy: Understanding the International Trade Law Issues of E-commerce”, 46, no. 3 *Journal of World Trade* 545-70.

Box, S., (2016). “Internet Openness and Fragmentation: Toward Measuring the Economic Effects”. Centre for International Governance Innovation and Chatham House, Paper Series No.36.

Bradshaw, S. (2015). “Rethinking Trust in Internet Governance”. Paper presented at 10th Annual GigaNet Symposium, Joao Pessoa (Unpublished)

Burri, M. (2016). “The World Trade Organization as an Actor in Global Internet Governance” in W.J. Drake and M. Burri (eds), *The Institutions of Global Internet Governance.* Cambridge: Cambridge University Press.

Castro, D. and Atkinson, R., (2014). “Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy”. <http://www2.itif.org/2014-crossborder-internet-policy.pdf> .

Chander, A., (2012). “Trade 2.0” in Mira Burri and Thomas Cottier eds, *Trade Governance in the Digital Age.* Cambridge: Cambridge University Press.

Damon, L.J., (1986).”Freedom of Information versus National Sovereignty: The Need for a New Global Forum for the Resolution of Transborder Data Flow Problems”, 10, no. 2 *Fordham International Law Journal* 262-287.

DeNardis, L. (2016). “One Internet: An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation”. Centre for International Governance Innovation and Chatham House, Paper Series No. 38.

DeNardis, L., (2009). *Protocol Politics: The Globalization of Internet Governance* (Washington: The MIT Press).

Drake, W.J., et al, (2016). “Internet Fragmentation: An Overview”. *Future of the Internet Initiative White Paper*, World Economic Forum.

Garfinkel, S., (2003). “The End of End-to-End?” *MIT Technology Review* (online).

Global Commission on Internet Governance (2016). “One Internet”. CIGI and Chatham House.

Hill, J.F., (2012). “A Balkanized Internet? The Uncertain Future of Global Internet Standards?”. *Georgetown Journal of International Affair*s. International Engagement on Cyber 2012: Establishing Norms and Improving Security (online).

Hoekman, B., and Mattoo, A., (2011). “Services Trade Liberalization and Regulatory Reform: Re-Invigorating International Cooperation”. Policy Research Working Paper 5517, The World Bank Poverty Reduction and Economic Management Network International Trade Department & Development Research Group Trade and Integration Team. l

Hoffman, J. (2015). “Constellations of Trust and Distrust in Internet Governance”, Working Paper, Alexander von Humboldt Institute for Internet and Society.

Intellectual Property Watch (2017). “US Renegotiation of NAFTA to Include IP Rights, Digital Trade”, <https://www.ip-watch.org/2017/05/18/us-renegotiation-nafta-include-ip-rights-digital-trade/>.

ISOC (2013). ‘”Understanding Security and Resilience of the Internet”. <https://www.internetsociety.org/sites/default/files/bp-securityandresilience-20130711.pdf>.

ISOC (2015). “Internet Society Approach to Cybersecurity Policy”. <https://www.internetsociety.org/news/internet-society-approach-cyber-security-policy>

Jamart, A., (2014). “Internet Freedom and the Constitutionalization of Internet Governance” in R. Radu et al eds, *The Evolution of Global Internet Governance.* Springer Online.

Jensen, E.T., (2015). “Cyber Sovereignty: The Way Ahead” 50, no. 2 *Texas International Law Journal* 274-302.

Kaminiski, M., (2015). “Why trade is not the place for EU to negotiate privacy”. <http://www.slate.com/articles/technology/future_tense/2015/06/trade_in_services_agreement_could_change_the_global_internet.html>.

Kleinwachter, W. (2011). “Internet Principle Hype: How Soft Law is Used to Regulate the Internet”, <https://lists.afrinic.net/pipermail/africann/2011-August/003811.html>.

Kopstein, J., (2015). “Washington’s Cybersecurity is About Surveillance, Not Security”.*Al Jazeera* (online).

Kulesza, J. (2012). *International Internet Law.* Oxon*:* Routledge.

Mann, C.L.., (2001). “International Internet Governance: Oh What A Tangled Web We Weave”, 2, no. 2 *Georgetown Journal of International Affairs* 79-86.

Manyika, J., et al. (2016) “Digital Globalization: The New Era of Global Flows”, McKinsey Global Institute.

Meltzer, J.P. (2015). “A New Digital Trade Agenda”, E15 Initiative. *Overview Paper*. <http://e15initiative.org/publications/a-new-digital-trade-agenda/>.

Meltzer, J.P., (2016). “Maximizing the Opportunities of the Internet for Digital Trade”. *Policy Options Paper* (January 2016), http://e15initiative.org/publications/maximizing-opportunities-internet-international-trade/

Mishra, N., (2017). “The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?”, 20, no. 1 *Journal of International Economic Law* 31 -60.

Moran, T.H., (2015). “Should US Tech Companies Share Their “Source Code” with China?”, *Real Time Economic Issues Watch* <https://piie.com>.

Mueller, M., (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press Online.

OECD (2015). *Digital Security Risk Management for Economic and Social Prosperity*. OECD Recommendation and Companion Document.

OECD (2016). *Economic and Social Benefits of Internet Openness*, DSTI/ICCP(2015)17/FINAL.

Shackelford, S.J., (2013). *Managing Cyber Attacks in International Law, Business, and Relations In Search of Cyber Peace*. Cambridge: Cambridge University Press.

Solum, LB., (2009). “Models of Internet Governance” in L.A. Bygrave and J. Bing eds, *Internet Governance: Infrastructure and Institutions.* Oxford Scholarship Online.

Stone, S., et al (2012). “Emerging Policy Issues: Localisation Barriers to Trade”, *OECD Trade Policy Papers*, No 180.OECD Publishing.

UNCTAD (2016). “Data protection regulations and international data flows: Implications for trade and development”, United Nations.

Weber, R.H., (2014a). *Realizing a New Global Cyberspace Framework: Normative Foundations and Guiding Principles.* Berlin: Springer English/International Ebooks.

Weber, R.H. (2014b). “Legal Interoperability as a Tool for Combatting Fragmentation”. Paper Series no 4, Global Commission on Internet Governance.

West, J. (2016). “A Framework for Understanding Internet Openness”, Centre for International Governance Innovation and Chatham House, Paper Series no 35.

Wunsch-Vincent, S., (2012). “Trade rules for the digital age’ in M. Burri and T. Cottier eds, *Trade Governance in the Digital Age : World Trade Forum*. Cambridge: Cambridge University Press.

Xinmin, M.A. (2015). “What Kind of Internet Order do we Need?”, 14, no. 2 *Chinese Journal of International Law* 399-403.

The Asia-Pacific Research and Training Network on Trade – ARTNeT – is an open network of research and academic institutions and think-tanks in the Asia-Pacific region, supported by core partners AFD, ESCAP, UNCTAD, UNDP and WTO. ARTNeT aims to increase the amount of high quality, topical and applied research in the region by harnessing existent research capacity and developing new capacities. ARTNeT also focuses on communicating these research outputs for policymaking in the region including through the ARTNeT Working Paper Series which provide new and policy–relevant research on topics related to trade, investment and development. The views expressed in this publication are those of the authors and do not necessarily reflect the views of the United Nations and ARTNeT secretariat or ARTNeT members.

This and other ARTNeT publications are available from
artnet.unescap.org

ARTNeTontrade

@ARTNeTontrade

ARTNeT Group

artnetontrade@un.org

ARTNeT Secretariat, United Nations ESCAP
Rajadamnern Nok Avenue
Bangkok 10200, Thailand
Tel: +66(0) 22881410
Fax: +66(0) 22881027