Background Paper
Dynamic Coalition on Trade & the Internet

LIST OF ABBREVIATIONS

APEC	Asia-Pacific Economic Cooperation
EU	European Union
FTAs	free trade agreements
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDP	gross domestic product
ICANN	Internet Corporation for Assigned Names and Numbers
IP	Internet Protocol
IPRs	intellectual property rights
ISPs	Internet service providers

IT	**information technology**
ITA	**Information Technology Agreement**
MNEs	**multinational enterprises**
OECD	**Organisation for Economic Co-operation and Development**
PCs	**personal computers**
RCEP	**Regional Comprehensive Economic Partnership**
SMEs	**small and medium enterprises**
TBT	**Technical Barriers to Trade**
TiSA	**Trade in Services Agreement**
TRIPS	**Trade Related Intellectual Property Rights**
TPP	**Trans Pacific Partnership**
TTIP	**Transatlantic Trade and Investment Partnership**
UNCITRAL	**United Nations Commission on International Trade Law**
UPICC	**Uniform Principles of International Commercial Contracts**
US	**United States**
WIPO	**World Intellectual Property Organization**
WTO	**World Trade Organization**

1. Preface

Proliferation of digital technologies and cross-border flow of information has created social, economic and cultural growth. Nations now face the challenge of ensuring that the opportunities and benefits driven by Internet and communications technologies (ICT) are shared by all. With the development of national standards and the emergence of digital players transforming production processes and industries, there is increased push for centrally controlled regulatory environment for the Internet and Internet related services. This is driven by both economic and strategic interests.

The pace of ICT adoption and its impact on national economies has raised concerns about the legitimacy of control and civic participation. Issues that were considered purely technical have transformed into areas for strategic governance and tools for foreign policy.

While the Internet was conceived as a technology that would defy national borders, the historical imbalance of the United States' domination of ICTs and growing fears of surveillance has created the political momentum for increased state control on regulatory aspects of the Internet.

The evolution of the Internet from a research network to a platform for commerce presents challenges for trade law. The World Trade Organization (WTO) agreements were developed more than two decades ago and are inadequate in dealing with complex issues of present day digital economy. While the role of nation states in regulating physical goods and services has been established in global trade order, the role of nation states with respect to cross-border flow of information is less understood.

This is partly due to the novelty of digital technologies and the associated unorthodox processes that have evolved in the context of its governance. Existing Internet governance (IG) frameworks—many of which are still evolving—are led by multistakeholder decision-making where state and non-state actors address issues through open and transparent arrangements of rulemaking. This is in contrast to conventional regulatory domains which feature state-led processes for the development of global norms and treaties.

In the absence of global binding norms on Internet related issues, and in light of fears of rising 'digital protectionism', states are are seeking to draw up rules and frameworks for regulation of the digital economy through conventional mechanisms for international cooperation such as trade agreements. Although trade and Internet governance appear to be disconnected, with the growing significance of the Internet for international trade, a tenuous and complex relationship between the fields is emerging that will have repercussions on the development of the digital economy.

Direct or indirect inclusion of contemporary issues related to the Internet are being included in plurilateral and multilateral arrangements with the aim to counter restrictive measures on data flows that hinder cross-border trade. For example, the Electronic Commerce Chapter of the Trans-Pacific Partnership Agreement (TPP) contains provisions that ban data localization. Such provisions are accompanied by other legal obligations on cybersecurity, spam and intellectual property. Similar provisions are also being proposed in other ongoing plurilateral trade negotiations including the the Transatlantic Trade and

Investment Partnership (TTIP), the Trade in Services Agreement (TISA), the Regional Comprehensive Economic Partnership (RCEP) and most recently the North American Free Trade Agreement (NAFTA).

Any framework or rules evolving out of these agreements will have a deep impact and Internet governance processes and policymaking. Regulating commercial aspects of Internet through trade agreements entails choices that will significantly influence and bear repercussions for critical aspects of the emerging digital economy. It requires coming up with global solutions that strike a balance between trade liberalization and preservation of fundamental goals of Internet governance such as openness, transparency and protection of human rights. It would also necessitate resolving differences in political and ideological stance on issues like privacy, innovation and democratic standard setting.

It is important to understand the complexities and risks involved in aligning the disciplines of trade policy and Internet governance. Despite recent initiatives, it is important to take a step back and question whether trade agreements should be concerned with setting standards for Internet technologies or on issues such as national security and privacy. Going forward policymakers and governments need to understand how the application of international trade law could be better aligned with values of Internet governance such as openness and inclusion.

With the aim of bringing in a multistakeholder approach to application of international trade civil society, private sector, technical and academic community members have come together to form the Dynamic Coalition on Trade and the Internet (DCTI). The Dynamic Coalition was formally approved by the Internet Governance Forum (IGF) Secretariat in February, 2017 and the inaugural meeting will be held in Geneva in December 2017. The Dynamic Coalition aims to serve as a liaison between representatives from trade institutions and government delegations and the broader IGF community. The Coalition been established to address the lack of transparency in international trade negotiations and domestic consultation processes and provide recommendations about how Internet public policy can be developed in a transparent and inclusive way. The Coalition will also serve as an interface for the exchange of information and best practices on Internet public policy issues.

This paper is a resource developed for the DCTI and summarizing the issues, concerns and recent developments on trade and digital rights. The paper is divided in four parts.

Part I provides a background to the evolution of trade frameworks in the context of digital trade agenda. This section will draw on history of intellectual property trade frameworks and recent attempts to introduce e-commerce related issues in the digital trade agenda.

In Part II we cover the trade negotiations that have included digital issues or are currently being negotiated. We delve into the status of negotiations including the areas where countries have reached consensus or others where negotiations face inability to pass muster and what experts have been saying on these issues.

Part III we address some of the emerging themes and issues in the context of the digital economy that are increasingly being included in trade agreements. We analyze these provisions based on the implications for Internet governance and on consumers and human rights online.

In Part IV we highlight some of the procedural inconsistencies between the multistakeholder approach that is common to Internet governance. We provide a broad-range of recommendations for introducing transparency and opening up digital trade negotiation processes by by governments for the participation by affected stakeholders and NGOs. The recommendations seek to establish a framework for participation of diverse stakeholders when developing rules through regional and mega-regional trade treaties.

2. Overview of Digital Trade Frameworks

In 2006, law professor Tim Wu stressing that the Internet is built on information flows noted that the global Internet allows anyone to become an exporter or importer of goods and services.[1] "Hence almost by accident, the WTO has put itself in an oversight position for most of the national laws and practices that regulate the Internet." (Wu 2006, 263-264). According to Wu, the WTO members would need to consider if control of the Internet is legitimate domestic regulation and how much a barrier to trade (Wu 2006, 287). It is easy to

1

conceive the WTO as the best place to set rules to govern digital trade because it covers 164 nations but in reality the WTO is not the most up-to-date framework for tackling Internet related issues. The WTO covers several agreements that cover issues affecting digital trade and they include the Information Technology Agreement (ITA), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the General Agreement on Trade in Services (GATS).

The law of the WTO is contained in multiple agreements, attached as annexes to the Marrakesh Agreement establishing the World Trade Organization.[2] The General Agreement on Tariffs and Trade (GATT), the General Agreement on Trade in Services (GATS) and the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) build the three essential pillars of the WTO law. IN addition to the three frameworks, the Information Technology Agreement contains provisions relevant to e-commerce and the digital economy.

2.1 General Agreement on Tariffs and Trade (GATT)

The General Agreement on Tariffs and Trade was the first worldwide multilateral free trade agreement.[3] It was in effect from June 30, 1948 until January 1, 1995. GATT was first discussed during the United Nations Conference on Trade and Employment and was the outcome of the failure of negotiating governments to create the International Trade Organization (ITO).

GATT had three main provisions. The most important requirement was that each member must confer most favored nation status to every other member.[4] That means all members must be treated equally when it comes to tariffs. It permitted tariffs if their removal would cause serious injury to domestic producers. Second, GATT prohibited restriction on the number of imports[5] and exports.[6] The exceptions were when a government had a surplus of agricultural products, if a country needed to protect its balance of payments[7] because its

[2] World Trade Organization, https://www.wto.org/index.htm
[3] General Agreement on Tariffs and Trade https://www.wto.org/english/tratop_e/gatt_e/gatt_e.htm
[4] Most Favored Nation Status, https://www.thebalance.com/most-favored-nation-status-3305840
[5] Imports: Definition, Examples, Effect on Economy, https://www.thebalance.com/imports-definition-examples-effect-on-economy-3305851
[6] What Are Exports? Their Effect on the Economy https://www.thebalance.com/exports-definition-examples-effect-on-economy-3305838
[7] What Is Balance of Payments? Components and Deficit

foreign exchange reserves[8] were low and developing countries that needed to protect fledgling industries. In addition, countries could restrict trade for reasons of national security, protecting patents, copyrights and public morals. The third provision was added in 1965 to promote developing countries joined GATT. Developed countries agreed to eliminate tariffs on imports of developing countries to boost their economies.

GATT was signed by 23 nations in Geneva on October 30, 1947 and took effect on January 1, 1948. It remained in effect until the the World Trade Organization (WTO)[9] was established in April 1994 as part of the final act embodying the results of the Uruguay Round of multilateral trade negotiations (1986– 1994), and building upon the GATT 1947. The WTO became operational on January 1, 1995 and is in some ways a successor to GATT, and the original GATT text is still in effect under the WTO framework, subject to the modifications of GATT 1994.

2.2 General Agreement on Trade in Services (GATS)

The creation of the General Agreement on Trade in Services (GATS) was one of the landmark achievements of the Uruguay Round, whose results entered into force in January 1995.[10] The GATS was inspired by essentially the same objectives GATT, creating a credible and reliable system of international trade rules; ensuring fair and equitable treatment of all participants (principle of non-discrimination); stimulating economic activity through guaranteed policy bindings; and promoting trade and development through progressive liberalization. As GATS does not distinguish between means of delivery, trade in services via electronic means is covered under GATS. While GATS contains explicit commitments for telecommunications and financial services that underlie e-commerce, digital trade and information flows and other trade barriers are not specifically included. The GATS has two sets of exceptions: General and National Security Exceptions under which signatories can restrict trade in the interest of protecting public health, public morals, privacy, national

https://www.thebalance.com/what-is-balance-of-payments-components-and-deficit-3306278
[8] Foreign Exchange Reserves: Purpose, Ranking by Country
https://www.thebalance.com/foreign-exchange-reserves-3306258
[9] World Trade Organization
https://en.wikipedia.org/wiki/World_Trade_Organization
[10] The General Agreement on Trade in Services (GATS): objectives, coverage and disciplines
https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm

security or intellectual property as long as these measures are necessary, proportionate, reasonable and do not discriminate against WTO members.

2.3 Information Technology Agreement (ITA)

Information Technology Agreement (ITA), 'Plurilateral' agreement emerged from the Uruguay Round and was designed to achieve lowering of all taxes and tariffs on the identified information technology products by signatories to zero - this was applicable on Most Favoured Nation (MFN) basis.[11] During the Singapore Ministerial Conference of the WTO, a proposal for the expansion of world trade in information technology products was adopted vide the "Ministerial Declaration on Trade in Information Technology Products" dated 13th December 1996.[12]

The declaration was adopted by 14 parties including the QUAD Countries (USA, Canada, Japan and EU), Singapore and Hong Kong, representing about 80% of the world trade in these products. The agreement became effective once the number of countries joining the agreement represented 90% of the trade in information technology products. The two major objectives of the ITA was to increase trade and competition through trade liberalization for information technology (IT) products and secondly the global diffusion of information technology. Therefore, a critical and substantial mass of 90 percent was identified as the benchmark for its implementation in 1997.

The mandate of ITA-1 was to establish tariff-free trade in six product groups namely: computers, telecom equipment, semiconductors, semiconductor manufacturing and testing equipment, software and scientific instruments. The participating countries agreed to bind and eliminate all customs and other duties and charges on information technology products by the year 2000. However, the important issue of Non-tariff measures (NTMs) was left to be investigated by the parties as part of the on-going ITA process. While the WTO ITA is expected to expand trade in the technology products that underlie digital trade, it does not tackle the nontariff barriers that can pose significant limitations.

[11] Information Technology Agreement, https://www.wto.org/english/tratop_e/inftec_e/inftec_e.htm
[12] Ministerial Declaration on Trade in Information Technology Products
https://www.wto.org/english/docs_e/legal_e/itadec_e.htm

2.4 Developments from the Doha Round

The WTO has dealt with the Internet and digitally enabled trade in a fragmented manner. The need for addressing new topics like e-commerce and data flows has been raised, rules have not been formalized amongst members. The GATT's rules on tariffs and national treatment have provided strong support for tariff reduction and elimination on ICT hardware but these rules have suffered from fundamental limitations from the start. The ambitious interpretation in the WTO's dispute settlement has pushed the interpretation of WTO frameworks as yet there is no consensus amongst member nations.

The Doha Development Agenda, more often referred to as the Doha Round trade talks, is the latest cycle of negotiations under the WTO. The Doha round is based on the idea of a single undertaking, which means that, in effect, "nothing is agreed until everything is agreed".[13] In 2005-07, during a period of optimism in the Doha Round talks on services liberalisation, negotiators attempted to clarify and update the meaning of GATS commitments on Internet infrastructure services, such as computer and related services (CRS).

A 2007 draft on understanding on the scope of the CRS category clarifies that CRS includes a long list of services connected with computers, computer systems, computing, software and data processing, data storage, data hosting or database services — alone or in combination.[14] This clarification would ensure that services, such as search, hosted software, and cloud computing would qualify for coverage under CRS, a category in which many members have made full commitments.

A 2009 Background Note by the Secretariat on Computer and Related Services highlighted that some computer services have become nearly impossible to distinguish from value-added telecommunications services.[15] It stressed that the terms used in the corresponding CPC definitions of the GATS list are fairly outdated, "where, for example

[13] The Doha Round https://www.wto.org/english/tratop_e/dda_e/dda_e.htm

[14] Amy Porges and Alice Enders, Data Moving Across Borders: The Future of Digital Trade Policy, April 2016 http://e15initiative.org/wp-content/uploads/2015/09/E15-Digital-Economy-Porges-and-Enders-Final.pdf

[15] Computer and Related Services, Background Note by the Secretariat https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=38673,98867,95716,65358,56588,5962&CurrentCatalogueIdIndex=2&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True

would "web hosting" fall within the definitions provided? Regarding computer software, software provided in physical format usually crosses borders as a good, but whether it also represents a service on a physical carrier medium was a question left unresolved by the WTO discussions on electronic commerce."[16] Concrete results on e-commerce have been stymied by the deadlock in WTO and the GATS framework leaves may issues unresolved. Although GATS states nothing explicitly about cross-border flow of information, WTO members have begun to apply GATS and GATT in disputes. As a result, dispute settlement panels and the Appellate Body have become the decision makers on GATS and Internet issues.

2.5 Digital Trade and Dispute Settlement at the WTO

Panels and the Appellate Body at the WTO have correctly understood that GATS commitments are technologically neutral. The dispute resolution bodies have found that measures must not be arbitrary, or unjustifiable discrimination or disguised restriction on trade services. The dispute settlement process has resolved the question of whether a GATS commitment on a conventional service would include that service when delivered electronically.

In Mexico – Telecoms, the panel addressed the issue whether, cross-border supply between two Members occurs only if the supplier itself operates, or is present, on the other side of the border, or if cross- border supply can occur also if a supplier simply "hands off" traffic at the border.[17] The relevant take-away from this ruling for digital services trade is that 'remote' supply through all possible means of delivery, including all means of cross-border telecommunications, must be allowed in order to comply with a full mode 1 commitment. Conversely, where an unlimited market access commitment exists, a Member's prohibition of even a single means of delivery through mode 1 will give rise to a violation, even if alternative means of 'non-remote' or local delivery are allowed, or if supply is permitted through other means of delivery or modes of supply.

[16] Ibid
[17] DS204: Mexico — Measures Affecting Telecommunications Services https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds204_e.htm

In U.S. – Gambling, the WTO panel confirmed that mode 1 commitments cover the supply of services through electronic means.[18] Then, in China – Publications and Audiovisual Products, considered the issue of whether GATS commitments cover technological developments that were not contemplated at the time commitments were undertaken.[19] The panel and Appellate Body agreed that GATS commitments are not tied to the technology that existed as of the date those commitments were made.

In China – Electronic Payments, the panel reviewed previous WTO case law in order to determine the scope of services covered by specific commitments.[20] The panel in China – Electronic Payments held that a "'sector' may include "any service activity that falls within the scope of the definition of that sector", whether or not these activities are explicitly enumerated in the definition of that sector or subsector. This ruling is relevant to the interpretation of the scope and coverage of digital services commitments because they frequently involve many different services, and trading realities necessarily require services to operate together to deliver an integrated service to customers, of course including the transfer of data between customers and service suppliers.

Despite the resolution of these disputes, there are many issues that need to be clarified. For example, the ambiguity on the classification of digital content that is not fixed on carrier media. Member states remain conflicted over whether a goods or services classification is more appropriate for the balancing of rights. The panel on China – Publications and Audiovisual Products also left these issues open; it declined to rule on GATT claims regarding regulatory discrimination against imported music CDs and e-publications, and avoided ruling on the nature or legal status of recorded digital content. The arguments regarding classification of intangibles have long since subsided into stalemate as governments have stopped investing in discussing them in the WTO.

A related question is the issue of whether a website transaction for instance, online banking is to be classi ed as cross-border trade under Mode 1 or as supply abroad under Mode 2. modes of supply on the basis of the origin of the service supplier and consumer,

---

[18] DS285: United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm

[19] Panel issues report on US-China dispute over publications and audiovisual products https://www.wto.org/english/news_e/news09_e/363r_e.htm

[20] (DS413) China - Electronic Payment Services , https://www.wto.org/english/tratop_e/dispu_e/cases_e/1pagesum_e/ds413sum_e.pdf

and where the supplier and consumer are when the service is delivered. When online banking services can be delivered anywhere in the world by logging into a browser, it becomes impossible for governments to predict in advance which modes they will need to take into account when negotiating commitments.

The GATS positive-list architecture can create problems for any service (digitally delivered or not) that now exists but was not explicitly named in the Provisional Central Product Classification (CPC). The GATS was born as a positive-list agreement, in which no service is covered unless it has been listed by name in a member's schedule.

2.6 Declaration on Global Electronic Commerce

In May 1998, WTO members established the "comprehensive" Work Programme on Electronic Commerce "to examine all trade-related issues relating to global electronic commerce, taking into account the economic, financial, and development needs of developing countries."[21] The 1998 declaration establishing the program also included a statement that "members will continue their current practice of not imposing customs duties on electronic transmission." Reflecting the lack of agreement in the final WTO Ministerial Declaration, the latest report for the work program stated that there was no consensus on how to move forward beyond the information sharing stage to identify specific outcomes or recommendations. In the draft decision in November 2015, members agreed to continue periodic reviews of the work program, the current moratorium on customs duties on electronic transmissions, and having the other WTO bodies explore the relationship between existing WTO agreements and e-commerce based on proposals submitted by members.[22]

2.7 Trade-Related Aspects of Intellectual Property Rights (TRIPS)

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) TRIPS was negotiated at the end of the Uruguay Round of the General Agreement on Tariffs and Trade

[21] Work programme on electronic commerce, https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm
[22] Draft decision agreed on electronic commerce, https://www.wto.org/english/news_e/news15_e/gc_30nov15_e.htm

(GATT) in 1994.[23] TRIPS administered by the WTO is an international legal agreement between all the member nations and sets down minimum standards for the regulation by national governments of many forms of intellectual property (IP) as applied to nationals of other WTO member nations.[24] The TRIPs agreement gives set of provisions deals with domestic procedures and remedies for the enforcement of intellectual property rights.

Member countries have to prepare necessary national laws to implement the TRIPs provisions. TRIPs cover eight areas for IPRs legislation including patent, copyright and geographical indications. With TRIPs, the WTO also emerged as the institution for the protection and promotion of intellectual property globally as until then the World Intellectual Property Organisation (WIPO) was the exclusive international institution dealing with intellectual property. TRIPS incorporates the main substantive provisions of WIPO conventions by reference, making them obligations under TRIPS.

Among other provisions, the TRIPS section on copyright and related rights includes specific provisions on computer programs and compilations of data. It requires protections for computer programs—whether in source or object code—as literary works under the WIPO Berne Convention for the Protection of Literary and Artistic Works (Berne Convention).[25] TRIPS also clarifies that databases and other compilations of data or other material, whether in machine readable form or not, are eligible for copyright protection even when the databases include data not under copyright protection.

WTO members were required to fully implement TRIPS by 1996, with exceptions for developing country members by 2000 and least- developed-country (LDC) members until July 1, 2021, for full implementation. Like the GATS, TRIPS predates the era of ubiquitous Internet access and commercially significant e-commerce. TRIPS includes a provision for WTO members to "undertake reviews in the light of any relevant new developments which might warrant modification or amendment" of the agreement.

The TRIPS Agreement does not specifically cover IPR protection and enforcement in the digital environment, but arguably has application to the digital environment and sets a foundation for IPR provisions in subsequent mega-regional trade negotiations and

---

[23] Intellectual property: protection and enforcement, https://www.wto.org/ENGLISH/thewto_e/whatis_e/tif_e/agrm7_e.htm

[24] Trade-Related Aspects of Intellectual Property Rights
https://www.wto.org/english/tratop_e/trips_e/trips_e.htm

[25] Berne Convention for the Protection of Literary and Artistic Works, http://www.wipo.int/treaties/en/ip/berne/

agreements, many of which are "TRIPS-plus." The TRIPS Council has engaged in discussions on the agreement's relationship to electronic commerce as part of the WTO Work Programme on Electronic Commerce, focusing on protection and enforcement of copyright and related rights, trademarks, and new technologies and access to these technologies.

2.8 Digital Trade and WTO: Present Status

The Doha Member States designed the GATS language that would remain unchanged as technology evolves, but now seek clarity on specific points and want to update these rules. Several delegations have insisted that no new commitments or disciplines can be negotiated in the framework of the E-Commerce Work Programme. Academics and business leaders have also argued that the WTO's rules are incomplete, out of date and in need of clarification.[26] As recently as 2011, the U.S. was questioning whether digital trade should be governed under the commitments of goods and services and if these rules covered mobile telephony and cloud computing. The 10th Ministerial Conference of the WTO, in December 2015, concluded with no clear path forward for the Doha Development Agenda (DDA), reflecting an ongoing wide division among members. Most developing countries have maintained the need for a single package in continuing with the Doha Round talks. Conversely, advanced economies, including the United States and EU, are arguing that the Doha agenda has proven untenable and that a different approach is needed. While members claim to remain committed to addressing the outstanding issues of the round, both agricultural and nonagricultural, the Nairobi Ministerial Declaration acknowledged the division over the future of the Doha Round, and failed to reaffirm its continuation, leaving its future uncertain.

With the stalling of the Doha Round of negotiations, WTO members and experts have raised various options[27] to address emerging issues such as digital trade including:

[26] Burri 2013; Makiyama 2011; National Board of Trade, Sweden 2012, Aaronson 2017.

[27] Meltzer, Joshua P. 2016. Maximizing the Opportunities of the Internet for International Trade. E15 Expert Group on the Digital Economy – Policy Options Paper. E15 Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum.

- **Updating the rules within the WTO framework to address digital trade. Options could include expanding the multilateral GATS to cover cross-border data flows, technology transfer, or greater market access issues.**

- **Using the existing plurilateral WTO frameworks such as expanding the ITA, Telecommunications, or the Trade Facilitation Agreement to address digital trade and tackle barriers**

- **Establishing a permanent WTO working group[28] dedicated to exploring digital issues, possibly based on the current Work Programme, or to create a new stand- alone trade agreement specific to data services or digital trade, possibly initially as an open plurilateral deal.**

- **Creating a separate digital trade-specific WTO agreement, an "e-WTO" as some have suggested. USTR Ambassador Froman noted that "[n]ew rules on critical 21st century issues, such as e-commerce and the digital economy, are emerging.... a better path forward is a new form of pragmatic multilateralism.**

In July 2016, the U.S. put forward a submission under the WTO Work Programme on Electronic Commerce offering "trade-related policies that can contribute meaningfully to the flourishing of trade through electronic and digital means" but without specific negotiating proposals.[29] The non-paper includes 16 policies included in the U.S. submission are a copy of provisions proposed in other mega-regional and plurilateral agreements. Similarly, China put forward a proposal in November 2016 in which it seeks "to clarify and to improve the application of existing multilateral trading rules" with a focus on facilitating e- commerce.[30]

There are increased attempts by some WTO members to seek negotiating mandate for e-commerce at the forthcoming Ministerial Conference of the WTO (MC 11) to be held in December 2017. In April 2017, at the sides of the United Nations Conference on Trade and Development (UNCTAD)'s 'E-Commerce Week',[31] a group of developing countries, calling

---

[28] Rachel F. Fefer, Shayerah Ilias Akhtar, Wayne M. Morrison, Digital Trade and U.S. Trade Policy, June 6, 2017 https://fas.org/sgp/crs/misc/R44565.pdf

[29] WTO, "Non-Paper from the United States," JOB/GC/94, July 4, 2016

[30] WTO, "Communication from the People's Republic of China," JOB/CTG/2, November 4, 2016

[31] UNCTAD E-Commerce Week http://unctad.org/en/conferences/e-week2017/Pages/default.aspx

themselves the "Group of Friends of E-Commerce for Development" (GFED) gathered for their first ministerial meeting to reveal a roadmap devised to push for the incorporation of e-commerce mandate at the WTO Ministerial in December 2017.[32]

The roadmap consists of seven key issues: e-commerce readiness and strategy, ICT infrastructure and services, trade logistics, payment solutions, legal and regulatory frameworks, e-commerce skills development and technical assistance, and access to financing. The Friends of E-Commerce for Development (FED) currently include: Argentina, Chile, Colombia, Costa Rica, Kenya, Nigeria, Mexico, Pakistan, Sri Lanka, and Uruguay.As the WTO continues to grapple with the digital trade governments have pushed through with negotiations in plurilateral and bilateral free-trade agreements (FTAs).

3. Plurilateral and Mega-regional Trade Agreements

The stalled Doha Round and the desire by some parties to address new topics such as e-commerce are two of the drivers behind the rise of digital rulemaking in agreements outside the multilateral trading system. Countries have therefore attempted to make progress in regional free trade agreements (FTAs) and in the plurilateral Trade in Services Agreement (TiSA).

Earlier trade agreements used to be about negotiated tariffs and market access, but over time more legal areas have been added to the process. The U.S. was the first nation to include provisions related to cross-border information ows in its trade agreements, as well as the first to use trade policies to govern cross-border information flows.[33] Most chapters contain provisions on nondiscrimination of digital products, prohibition of customs duties, transparency, and cooperation topics such as SMEs, cross-border information flows, and promoting dialogues to develop e-commerce. Some of the FTAs also include cooperation

[32] Friends for E-Commerce for Development: Mapping e-Trade for All Development Objectives into a WTO Framework for E-Commerce
https://www.ip-watch.org/weblog/wp-content/uploads/2017/04/FEDs-mapping-e-Trade-for-All-into-Trade-Policy-April-2017.pdf?f049a7

[33] Susan Ariel Aaronson, The Digital Trade Imbalance and Its Implications for Internet Governance, Centre for International Governance Innovation and the Royal Institute of International Affairs, 2016
https://www.eff.org/files/2016/01/23/gcig_no25_1.pdf

on consumer protection, as well as providing for electronic authentication and paperless trading. All FTAs allow certain exceptions to ensure that each party is able to achieve legitimate public policy objectives, protecting regulatory flexibility.

The United States has included an e-commerce chapter in its FTAs since it signed an agreement with Singapore in 2003.[34] In subsequent years the U.S. continues to expand on, digital trade provisions in its bilateral agreements with the Netherlands, Japan, France, Ireland. The U.S.-South Korea FTA (KORUS)[35] contains the most detailed digital trade provisions in a U.S. FTA currently in force.

Most significantly, KORUS was the first attempt in a U.S. FTA to explicitly address cross-border information flows. The e-commerce chapter contains an article that recognizes its importance and discourages the use of barriers to cross-border data but does not mention explicitly localization requirements. The financial services chapter of KORUS also contains a specific, enforceable commitment to allow cross-border data flows "for data processing where such processing is required in the institution's ordinary course of business."

Apart from the bi-laterals there are several mega-regional trade agreements that include provisions that are relevant for the digital economy.

[34] United States - Singapore Free Trade Agreement, https://ustr.gov/sites/default/files/uploads/agreements/fta/singapore/asset_upload_file708_4036.pdf
[35]The U.S.-South Korea Free Trade Agreement (KORUS FTA): Provisions and Implementation, https://fas.org/sgp/crs/row/RL34330.pdf

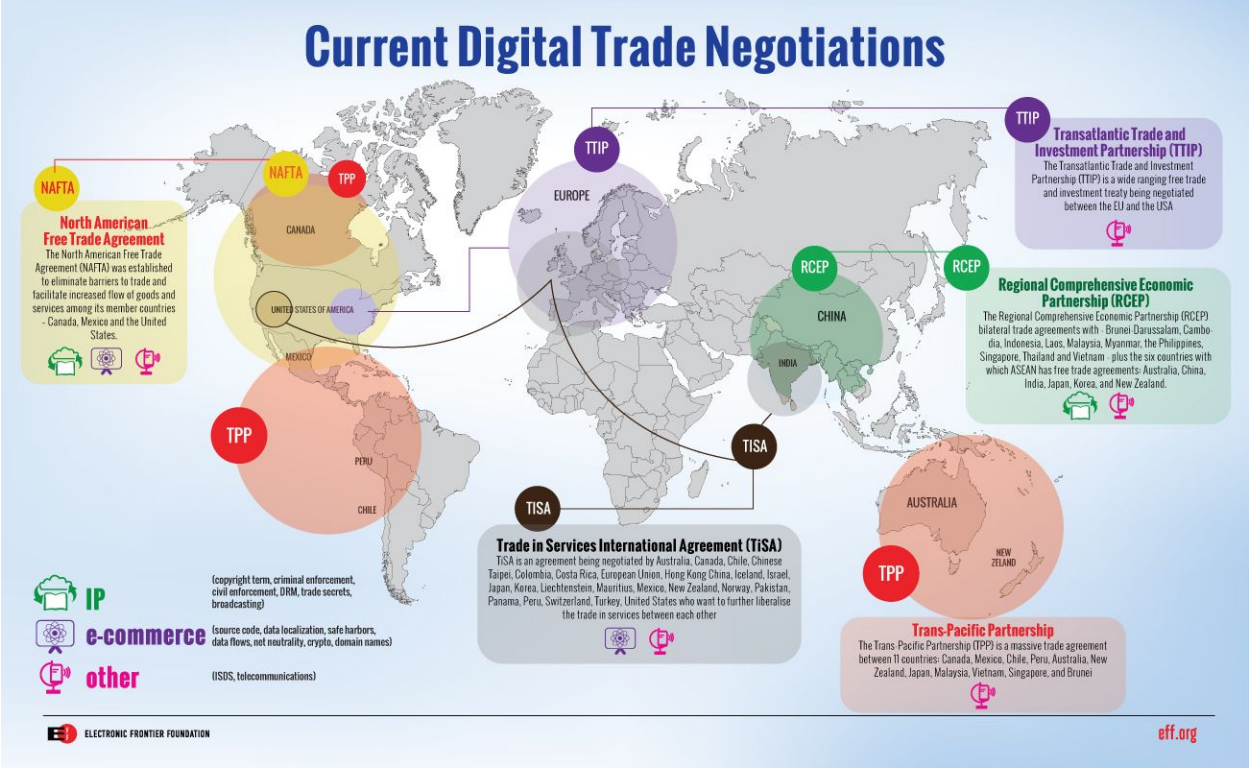

Image 1: Current Global Trade Negotiations

Table 1: Global Trade Negotiations Member Nations

RCEP	TPP	TiSA	ACTA	NAFTA
Australia	Australia	Australia	Australia	Canada
Brunei	Brunei	Canada	Canada	Mexico
Cambodia	Canada	Chile	Japan	USA
China	Chile	Chinese Taipei	Morocco	
India	Japan	Colombia	New Zealand	
Indonesia	Malaysia	Costa Rica	Singapore	

Japan	Mexico	EU	South Korea	
Laos	New Zealand	Hong Kong	EU	
Malaysia	Peru	Iceland	USA	
Myanmar	Singapore	Israel		
New Zealand	USA	Japan		
Philippines	Vietnam	Korea		
Singapore		Liechtenstein		
South Korea		Mauritius		
Thailand		Mexico		
Vietnam		New Zealand		
		Norway		
		Pakistan		
		Panama		
		Peru		
		Switzerland		
		Turkey		
		USA		

3.1 Trans-Pacific Partnership (TPP)

The Trans-Pacific Partnership (TPP)[36] was the first trade agreement to include binding commitments that facilitate cross-border information flows and limit digital protectionism. Specifically, the U.S. wanted to establish clear rules governing when nations could limit information flows.[37] Proponents of the agreement including the Obama Administration had asserted that "TPP will help preserve the open Internet and prevent its breakup into multiple, balkanized networks in which data flows are more expensive and more frequently blocked."[38] On the other hand, critics have said that the secret multinational trade agreement undermines Internet freedom and access to information.[39]

The TPP chapter on e-commerce requires TPP governments to ban data localisation mandates and allow business to access markets without using or locating computing facilities in its territory.[40] Article 14.11., the key article related to information flows notes that "each party shall allow the cross-border transfer of information by electronic means...when this activity is for the conduct of the business of a covered person." These provisions cover not just IT and cloud businesses, but also manufacturing businesses and service businesses.[41] Experts have highlighted it is not clear if the language in the e-commerce chapter cover all cross- border information flows by all Internet actors such as suppliers and consumers of digital transmissions.[42] The USTR, based on the service chapter, says Internet users are covered but the language in the ecommerce chapter raises questions.

Notably, TPP governments will be required to adopt or maintain a framework providing for protection of users' personal information. Article 14.8. "Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of

---

[36] https://www.eff.org/issues/tpp

[37] Inside U.S. Trade. 2012. "USTR Official: U.S. Still Faces Big Challenges on TPP Data Flow Proposal." Inside U.S. Trade, September 27. insidetrade.com/Inside-US-Trade/Inside-US-Trade-09/28/2012/ustr-official-us-still-faces-big-challenges-on-tpp-data-flow-proposal/menu-id-710.html.

[38] Summary, Chapter 14 Electronic Commerce, https://medium.com/the-trans-pacific-partnership/electronic-commerce-87766c98a068

[39] Electronic Frontier Foundation (EFF), What Was the Trans-Pacific Partnership Agreement (TPP)? https://www.eff.org/deeplinks/2015/10/final-leaked-tpp-text-all-we-feared

[40] Chapter 14, Electronic Commerce, https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf

[41] Chapter 11 on nancial services provides nancial institutions and cross-border financial service suppliers with a parallel right to transfer data, but it omits protection against unreasonable data localisation requirements.

[42] Ibid 17

electronic commerce." TPP also includes very specific language related to privacy of consumers and parties agreed to new and enhanced privacy rules. Article 14.7 of TPP requires the parties to "adopt or maintain consumer protection laws." The countries agreed to publish information on personal privacy protection and "endeavor to adopt non-discriminatory practices." In earlier FTA's such as U.S.-Korea, the Parties simply stated that they "recognize the importance of maintain and adopting transparent and effective measures to protect consumers." The negotiating countries agreed to develop mechanisms to promote compatibility among different privacy regimes.

The TPP incorporates the general exceptions delineated in the GATS. Nations can limit information flows under the "exceptions" rules as TPP parties are guaranteed "the full right to regulate in the public interest, including for national security and other policy reasons.[43] It is expected that the censoring and filtering can be seen as disruptive for trade and the agreement would allow TPP nations to sue other signatories as government measures that violate commitment in the e-commerce chapter could be subject to investor-state dispute settlement.[44] The two nations that have records of censorship and filtering, Malaysia and Vietnam, were given two years to revise their policies but after that could be subject to such challenges.

One of the most controversial provisions included in the TPP negotiations was under the Intellectual Property (IP) chapter. The provision seeks to increase the international standard term of copyright set by the Berne Convention as life of the author plus an additional 50 years for six of the signatory countries. This standard term is followed by more than half of the TPP countries including Canada, Japan, Malaysia, New Zealand, Brunei, and Vietnam. Under the TPP terms[45], all these countries would be required to extend copyright term to a minimum term of the life of the author plus 70 years, mirroring the terms of the controversial US Sonny Bono Copyright Term Extension Actor[46] the "Mickey Mouse Act"[47] The U.S. and Japan (and, to a lesser extent, Australia) want to protect

---

[43] Chapter 29, Exceptions and General Provisions, https://ustr.gov/sites/default/files/TPP-Final-Text-Exceptions-and- General-Provisions.pdf and USTR, "Summary," https://ustr.gov/sites/default/files/TPP-Chapter-Summary- Exceptions-and-General-Provisions.pdf

[44] Marty Hansen and Gabriel Slater, The TPP's Electronic Commerce Chapter, Global Policy Watch https://www.globalpolicywatch.com/2015/11/the-tpps-electronic-commerce-chapter/

[45] Trans-Pacific Partnership, Intellectual Property Chapter Draft - February, 2011 https://www.keionline.org/sites/default/files/tpp-10feb2011-us-text-ipr-chapter.pdf

[46] Lawrence Lessig, Free Culture, http://www.authorama.com/free-culture-18.html

[47] Joyce Slaton, A Mickey mouse Copyright Law?

and enhance online copyright, believing that strong copyright protections further innovation, which is a key factor in the competitiveness of these nations.[48]

Critics have stressed that the TPP IP chapter would force the adoption of the U.S. approach, which they believe does not provide due process to individuals who allegedly breach online copyright.[49] Moreover, they note that, if approved, the TPP would require countries such as Chile (which has established a judicial notice-and-takedown regime) to change to the U.S. system (which they argue provides less protection to Internet users' expression and privacy). Further, signatories would also be required to adopt criminal sanctions for copyright infringement that occurs without a commercial motivation including fines and jails.[50] Proponents maintain that TPP approach on IP is balanced because it allows the dissemination of content and protects individuals who want to assess that content online with exceptions and limitations for "fair use" — hence, non-commercial sharing would not be criminalized.[51]

The chapter on cross-border services allows TPP service businesses to market and supply services in any other TPP party without being required to establish a local presence. This provision reduces paperwork and trade costs that can be a severe barrier to SMEs. Susan Aaron has interpreted the rules governing services cover both Internet service providers and Internet users.[52]

Provisions prohibiting performance requirements such as local content requirements, requirements to use local technology, or forced technology transfer were included in the investment chapter. The chapter also bars a party from requiring transfer of, or access to, source code of mass-market software owned by a person of another TPP party, as a

---

https://www.wired.com/1999/01/a-mickey-mouse-copyright-law/

[48] IP Commission 2013 http://www.ipcommission.org/report/ip_commission_report_052213.pdf

[49] The Trouble with the TPP, Day 3: Copyright Term Extension, http://www.michaelgeist.ca/2016/01/the-trouble-with-the-tpp-day-3-copyright-term-extension/

[50] Jeremy Malcolm, Sneaky Change to the TPP Drastically Extends Criminal Penalties https://www.eff.org/deeplinks/2016/02/sneaky-change-tpp-drastically-extends-criminal-penalties

[51] Remarks by Deputy USTR Robert Holleyman to the U.S. Chamber of Commerce Global Intellectual Property Center 2015 Global IP Summit, https://ustr.gov/about-us/policy-offices/press-office/speechestranscripts/2015/November/Remarks-Deputy-Holleyman-Global-IP-Center-2015

[52] Susan Ariel Aaronson, What does TPP mean for the Open Internet? From Policy Brief on Trade Agreements and Internet Governance Prepared for the Global Commission on Internet Governance, November 16, 2015 https://tpplegal.files.wordpress.com/2015/12/iiep-paper.pdf

condition for the import, distribution, sale, or use of such software or products containing it.

Custom duties on digital products including software, ebooks, audio, video, video games, or other digitally encoded content are also covered by the agreement. Another key provision relates to barring TPP parties makers or suppliers of goods that use encryption for commercial applications (such as routers) to transfer or disclose proprietary encryption technology, production processes, or other information (keys) to government or a domestic partner, or to partner with a domestic partner, or to use a particular type of encryption, as a condition of being able to make, import, sell, distribute or use these goods. A separate provision prohibits any party from banning imports of commercial cryptographic goods (goods that implement or incorporate cryptography, sold to the general public).

The telecommunications chapter includes and improves upon the text of the WTO Basic Telecom Reference Paper. The governments also agree that their telecom regulations will not generally discriminate against specific technologies, and agree to work cooperatively to promote competition in international mobile roaming.

The agreement had been shelved following the withdrawal of the U.S. from the negotiation process.[53] Over the past year, countries eager to keep the pact alive have continued dialogue and rallied support of less enthusiastic members to move forward with the agreement without the U.S. A revised framework is expected to be proposed for approval at the Asia-Pacific Economic Cooperation (APEC) TPP-11 Ministerial Meeting in November.[54] Most recently, negotiators met in September in Japan to discuss what parts of the original deal they wished to shelve and issues that they can aim to reach a broad agreement on in November.

Although the remaining members have voiced continued commitment to the deal, adoption of the pact linking 11 countries with a combined GDP of $12.4 trillion has stalled at times,

[53] New signs of life for Pacific TPP trade deal Trump nixed
http://www.washingtontimes.com/news/2017/aug/17/new-signs-life-pacific-tpp-trade-deal-trump-nixed/
[54] https://www.eff.org/deeplinks/2017/03/will-tpp-live-nafta-and-rcep

raising fears that other countries may follow the U.S.[55] At a meeting in Australia in August 2017, Vietnam raised the prospect of changes IP provisions in the original pact. Vietnam's desire to shelve the IP provisions around pharmaceutical data is likely to win broad support, as Japanese and New Zealand officials have indicated they back the change. Even if the TPP-11 move ahead with ratification of the agreement technical difficulties need to be resolved. The original pact required ratification by at least six countries accounting for 85 percent of the combined GDP of members, a condition which cannot be fulfilled after the US withdrawal. Japan's FTA with EU may provide a workaround to this requirement and the November talks will likely provide more clarity.

3.2 Trade in Services Agreement (TiSA)

The plurilateral Trade in Services Agreement (TiSA) negotiations was launched in 2013.[56] TISA has notable presence of both developed and developing countries. Besides the 28 EU countries, the TiSA negotiators include: Australia, Canada, Chile, Chinese Taipei, Colombia, Costa Rica, Hong Kong, Iceland, Israel, Japan, Korea, Liechtenstein, Mauritius, Mexico, New Zealand, Norway, Pakistan, Panama, Peru, Switzerland, Turkey and the the United States. According to the TiSA negotiating framework, the forum is open to all WTO members and they can join during discussions and after ratifying the agreement. The negotiators had agreed on a work programme notionally targeting agreement on the overall text by September 2016 however the negotiations have slowed down.

The TiSA's architecture addresses some of the structural flaws of the GATS and participants are discussing rulemaking through sectoral annexes. As of early 2016, these include annexes on telecommunications, e-commerce, localisation (including local presence, local content, and local technology), financial services, and others.[57] Recent proposals that financial service suppliers be guaranteed the right to move data across borders in the ordinary course of business, and that all service suppliers be guaranteed the

[55] Reuters, Without U.S., 11 nations in TPP inch closer to a deal, http://www.reuters.com/article/us-trade-tpp-japan/without-u-s-11-nations-in-tpp-inch-closer-to-a-deal-idUSKCN1BX1DY

[56] Jeremy Malcolm, TISA: Yet Another Leaked Treaty You've Never Heard Of Makes Secret Rules for the Internet https://www.eff.org/deeplinks/2015/05/tisa-yet-another-leaked-treaty-youve-never-heard-makes-secret-rules-internet

[57] Jeremy Malcolm, Secret New Internet Rules in the Trade in Services Agreement, https://www.eff.org/deeplinks/2016/05/secret-new-internet-rules-trade-services-agreement

right to move data.[58] Although six of the parties including Canada, Chile, and Mexico have suggested that the free flow of information isn't suited for resolution in a trade agreement at all, simply proposing. "The Parties recognize that each Party may have its own regulatory requirements concerning the transfer of information by electronic means."[59]

The TiSA text also includes a contentious provision banning mandatory transfer or access to source code. Japan and Switzerland have suggested that the prohibition on a party demanding access to product source code of products from foreign service providers could be overridden "to achieve a legitimate public policy objective, provided that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or disguised a restriction on trade."[60]

The language on "Open Networks, Network Access and Use" contains provisions that are relevant to the issue of net neutrality. A previously separate provision on interoperability of governmental online procedures and services has been included along with new proposed language that would require each party to "endeavor not to restrict the ability of service suppliers to supply services over the Internet on a cross-border and technologically neutral basis."

On the "Location of Computing Facilities" Canada, Chile and Peru have pushed for text, that will allow countries to retain more latitude to adopt national requirements about local hosting of data where these "seek to ensure the security and confidentiality of communications." A "legitimate public policy objective" exception is also proposed.

A new leak of the ecommerce chapter from the November 2016 negotiating round has exposed a U.S. proposal on Internet intermediary safe harbors.[61] The proposal is seeks to establish immunity for intermediaries for liability as laid down under the Communications Decency Act or the Section 230.[62] Like Section 230, the U.S. provision excludes intellectual property rights and criminal law enforcement, but otherwise provides a shield protecting

[58] Inside US Trade (2014b)
[59] Ibid
[60] New provisons TiSA, Wikileaks https://wikileaks.org/tisa/New-Provisions/page-1.html
[61] Leaked TISA Safe Harbor Proposal: the Right Idea in the Wrong Place, https://www.eff.org/deeplinks/2016/10/tisa-proposes-new-global-rules-data-flows-and-safe-harbors
[62] CDA https://www.eff.org/issues/cda230

online intermediaries against a range of laws that would otherwise that would otherwise hold them responsible for what their users say or do online.

EU appears to be opposing the inclusion of safe harbor provision as Europe's equivalent to CDA 230, its E-Commerce Directive, simply doesn't measure up to this U.S. proposal. Although Europe is also considering adopting a Good Samaritan provision to clarify that providers will not become liable for user content by reason of steps they take to filter out and eradicate illegal content on their platforms, there is no similar proposal to expand safe harbor protection for user content that intermediaries leave online.[63] Indeed, if anything, Europe is planning to lump intermediaries with additional responsibility for user content.[64] It is expected that either the proposed text will be watered down in the final agreement or abandoned altogether.

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.[65]

Also notably absent from the TiSA text is legally binding human rights clause that would benefit users.

3.3 Transatlantic Trade and Investment Partnership (TTIP)

The Agreement on Transatlantic Trade and Investment Partnership (TTIP) between the EU and the U.S. began at the same time as negotiations on TiSA.[66] Several contentious issues remain unresolved and subsequently negotiations have slowed down.[67] Unlike the TPP negotiations, the TTIP talks have unfolded in the midst of contentious transatlantic digital relations.

---

[63] Facebook moves to head off tougher regulation in Germany http://www.reuters.com/article/us-germany-facebook/facebook-moves-to-head-off-tougher-regulation-in-germany-idUSKBN1502CA

[64] Upload Filtering Mandate Would Shred European Copyright Safe Harbor https://www.eff.org/deeplinks/2016/10/upload-filtering-mandate-would-shred-european-copyright-safe-harbor

[65] Wikileaks, TISA Annex on Electronic Commerce <https://wikileaks.org/tisa/document/20151001_Annex-on-Electronic-Commerce/20151001_Annex-on-Electronic-Commerce.pdf>.

[66] Transatlantic Trade and Investment Partnership (T-TIP) https://ustr.gov/ttip

[67] Jeremy Malcolm, Why Releasing Text Isn't Enough: Behind the Scenes of TTIP, https://www.eff.org/deeplinks/2016/05/why-releasing-text-isnt-enough-behind-scenes-ttip

On the issue of data protection and privacy, a sharp divergence exists between the market-centric approach of the U.S. and some other APEC economies and the highly regulatory approach of the EU.[68] In 2015, the European Court of Justice struck down the U.S.-EU Safe Harbor agreement as incompatible with EU privacy rules.[69] The United States and the EU then concluded the Privacy Shield[70] agreement in February 2016 in a new attempt to calibrate EU privacy protections with EU-U.S. data flows, but privacy experts from EU member states raised serious concerns about Privacy Shield in April 2016.[71]

EU and U.S. data protection negotiators have accelerated their ongoing work on replacing Safe Harbour, and agreed in February 2016 on a new Privacy Shield that imposes increased data privacy-related obligations on U.S. companies.[72] By 2018, current data protection regulations in the 28 EU member states will be replaced by the EU's General Data Protection Regulation (GDPR), due to be adopted in April 2016.[73] In the area of data privacy, TTIP does not contemplate the new GDPR framework.[74]

More recently, action[75] against U.S. technology companies, such as Google that stems from competition law in EU has impacted the negotiations.[76] U.S. Trade Representative Michael Froman optimistically argued for conclusion of the negotiations by the end of 2016 however, EU Commissioner Cecilia Malmström has confirmed that the EU would not conclude a "TTIP light".[77]

---

[68] International Trade, Internet Governance and the Shaping of the Digital Economy https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2997254

[69] Karen Kornbulah, The Implications of the European Safe Harbor Decision, https://www.cfr.org/blog/implications-european-safe-harbor-decision

[70] The EU-U.S. Privacy Shield Is a Victory for Common Sense and Transatlantic Good Will https://www.cfr.org/blog/eu-us-privacy-shield-victory-common-sense-and-transatlantic-good-will

[71] Statement of the Article 29 Working Party on the Opinion on the EU-US Privacy Shield, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf

[72] Maldoff (2016) and other coverage of Privacy Shield at https://iapp. org/tag/trans-border-data- ow.

[73] General Data Protection Regulation, https://gdpr-info.eu

[74] Judgment in Case C-362/14 Press and Information Maximillian Schrems v Data Protection Commissioner https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[75] Europe v. Google: A Dispute About Competition, Political Power, and Sovereignty https://www.cfr.org/blog/europe-v-google-dispute-about-competition-political-power-and-sovereignty

[76] Google's Android charged with breaking EU competition law http://www.wired.co.uk/article/google-android-broken-eu-antitrust-law

[77] Inside US Trade (11 March 2016)

In 2016, Greenpeace posted the consolidated negotiating text for electronic communications/telecommunication services, an important area but distinct from e-commerce.[78] The leaks do not reveal much concerning digital rights issues in the current text because text on most of those issues has not been tabled yet. At present, only the EU has made its e-commerce proposals public. The EU's proposal leaves out almost all of the TPP digital economy provisions listed above and includes a reservation for "new services" as in the TiSA.[79] Europe also insists on maintaining the artificial barriers that require a separate license to be obtained to make digital content available in each country is stalling negotiations from moving forward.[80]

Another document from March 2016 on the 'Tactical State of Play of the TTIP Negotiations' released by EU reveals that e-commerce provisions being discussed include "all proposals except for the provisions on data flows and computing facilities," addressing non-discriminatory treatment of digital products (except audio-visual services), and considering EU proposals on e-trust and e-authentication services and on the prohibition of requirements for prior authorization for online services.[81]

The EU note also mentioned negotiations concerning conformity assessment principles for ICT products that use encryption, with the TPP text as the basis of these discussions. On this issue, the EU stressed "the sensitivities of Member States, which are competent in this area and which would not like to see its right to regulate curtailed in a security-related area."[82]

An IP chapter is missing as U.S. remains unwilling to table, at this stage, concrete proposals on more sensitive offensive interests that have been expressed by some of its right holders or that are explicitly referred to in its TPA for instance on patents, on technical protection measures and digital rights management or on enforcement.[83] The EU has warned that

---

[78] The TTIP Leaks and the Future of Electronic Commerce in International Trade Law, https://www.cfr.org/blog/ttip-leaks-and-future-electronic-commerce-international-trade-law
[79]Transatlantic Trade and Investment Partnership Trade in Services, Investment and E-commerce http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf
[80] Jeremy Malcolm, A European Digital Single Market Is Only Possible if Internet Users Are Heard, https://www.eff.org/deeplinks/2015/03/achieve-european-digital-single-market-users-must-be-heard
[81] Ibid
[82]Ibid
[83] Why Releasing Text Isn't Enough: Behind the Scenes of TTIP, https://www.eff.org/deeplinks/2016/05/why-releasing-text-isnt-enough-behind-scenes-ttip

bringing sensitive proposals that would require changes in EU law to the table at a late stage of the negotiation may have a negative impact on stakeholders and has very limited chances of being accepted.

In response the U.S. reiterated its understanding that the IP chapter should not be a standard TPP type text, but also insisted that such a departure from its "model" creates some difficulties in terms of addressing the demands included in the IPR related sections of its Trade Protection Authority (TPA). in 2015, the TPA passed a law which compels the USTR to negotiate trade agreements with the objective of providing rightholders with "the legal and technological means to control the use of their works through the Internet and other global communication media, and to prevent the unauthorized use of their works". A failure to secure this outcome in TTIP would likely create difficulties for the agreement's passage through Congress, much as the TPP is currently encountering difficulties from Congressional hardliners over the USTR's failure to agree to 12 year terms of protection for biologic medicines.[84]

Similarly, the Europeans are concerned about the lack of progress from the U.S. side in implementing copyright and patent law changes in U.S. domestic law.[85] Europe describes these as including "the draft laws on patent reform (addressing the problem of patent trolls) and on the copyright sectors identified as offensive interests by the EU (broadcasting rights, public performance and resale rights)."[86]

3.4 North-American Free Trade Agreement (NAFTA)

The opening round of a series of negotiations over a proposed revised North American Free Trade Agreement (NAFTA) began in march 2017 between between trade representatives from the United States, Canada, and Mexico.[87] The negotiations are expected to rotate between three countries with a timeline for agreement set at the end date of mid-2018.

Reports confirm that the NAFTA will include provisions on IP although there is no leaked chapter for reference yet.[88] The renegotiation of the NAFTA has created another

[84]Decision Time On Biologics Exclusivity: Eight Years Is No Compromise, https://www.ip-watch.org/2015/07/27/decision-time-on-biologics-exclusivity-eight-years-is-no-compromise/
[85] Legislative Solutions for Patent Reform, https://www.eff.org/issues/legislative-solutions-patent-reform
[86] Ibid 78
[87] NAFTA, https://www.eff.org/issues/nafta
[88] Canada Pushes Back Against U.S. Copyright Demands in NAFTA

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 USTR.[89] It is believed that the U.S. will be pushing for a template laid down in the TPP as the basis for negotiations. Reports also suggest that that Hollywood has succeeded in encouraging the USTR to omit a provision requiring the parties to have balanced copyright limitations and exceptions, such as fair use.[90]

While Mexico's stance on IP is unclear Canada preferred starting point for negotiation over IP is the original NAFTA, augmented by some newer instruments that Canada has subsequently signed and ratified such as the WIPO Internet Treaties, and its trade agreement with with the EU, the Comprehensive Economic and Trade Agreement (CETA).[91] In the TPP talks Canada was a latecomer was prohibited from revisiting that text.[92] However in the NAFTA negotiations think tanks and civil society have been pushing for Canada to stand its ground on the IP provisions advocate for similar balance in patent law, for example through provisions to address the problem of patent trolling.[93]

The e-commerce chapter is called digital trade in the NAFTA negotiations although the U.S. text proposal is based heavily on the TPP's text.[94] Canada and U.S. share agreement on most of the chapter's key objectives, including fostering the free flow of data online, and prohibiting data localization measures such as mandates that data must be stored on local servers. Reconciling local privacy laws amongst the NAFTA countries will prove to be difficult as the countries have different regimes in place. It is expected that the agreement will include a reference to the APEC and OECD privacy frameworks, an existing "lowest common denominator" between the three countries.

Another area for negotiations in the NAFTA where differences between the parties in the Digital Trade chapter may arise will be over the ISP safe harbor language. The text

---

https://www.eff.org/deeplinks/2017/09/canada-pushes-back-against-us-copyright-demands-nafta

[89] USTR Puts IP Focus In Digital Trade In NAFTA Renegotiation Objectives
https://www.ip-watch.org/2017/07/18/ustr-puts-ip-focus-digital-trade-nafta-renegotiation-objectives/

[90] Calls to backtrack on copyright balance put tech backing for NAFTA in doubt
http://www.project-disco.org/intellectual-property/092217-calls-to-backtrack-on-copyright-balance-put-tech-backing-for-nafta-in-doubt/#.WcqqEq17FAY

[91] WIPO, https://www.eff.org/issues/wipo

[92] Canada Joins TPP as a Second-Tier Negotiator: Entertainment Lobby Approves, Civil Society Does Not
https://www.eff.org/deeplinks/2012/10/canada-joins-tpp

[93] Centre for International Governance Innovation (CIGI), NAFTA 2.0 and Intellectual Property Rights

[94] Ibid 47

proposed by U.S. is based on CDA Section 230.[95] Unlike the U.S. Canada and Mexico do not have a statutory rule that protects Internet intermediaries from liability for user content. Countries may negotiate on the obligations or water down the CDA 230 language in order to reach an agreement. A provision on the ban on review of source code of imported products may also prove to be controversial as it introduces an issue that does not exist between the NAFTA countries, as none of them has imposed a source code review mandate.

3.5 The Regional Comprehensive Economic Partnership (RCEP)

Regional Comprehensive Economic Partnership (RCEP) is a free trade agreement (FTA) aimed at broadening regional economic integration and liberalising trade and investment between the 10 ASEAN economies and its trading partners.[96] The idea of RCEP was first introduced at an ASEAN Summit in 2011 and formal negotiations were launched in 2012. The negotiating countries include Australia, China, India, Japan, Korea, and New Zealand. The total population covered by RCEP exceeds 3 billion, and with the combined GDP of about 17 trillion U.S. dollars accounting for about 40% of the world's trade makes RCEP and covering half of the world's population is the biggest mega-regional trade agreement that is under negotiation. If ratified, the RCEP will not only be the first trade agreement for the digital economy will also set the rules for trade across Asia over the next decade.

Over the last five years, the scope of the agreement has grown to include commitments similar to the TPP including provisions dealing with IP,[97] investment,[98] goods, services,[99] telecommunications,[100] and competition.[101] Discussions on ecommerce issues including rules on software, data flows, and regulatory standards that have not been addressed in other trade mechanisms are also being included in the RCEP negotiations. Reports suggest

---

[95] Section 230 of the Communications Decency Act, https://www.eff.org/issues/cda230
[96] Jeremy Malcolm, RCEP: The Other Closed-Door Agreement to Compromise Users' Rights
https://www.eff.org/deeplinks/2016/04/rcep-other-closed-door-agreement-compromise-users-rights
[97] RCEP - draft IP chapter (15 Oct 2015 version)
http://www.bilaterals.org/rcep-draft-ip-chapter-15-oct-2015
[98] RCEP - draft chapter on investment: temporary safeguard measures (Dec 2016)
http://www.bilaterals.org/?rcep-draft-investment-chapter
[99] RCEP - draft chapter on trade in services (Aug 2015)
http://www.bilaterals.org/?rcep-draft-chapter-on-trade-in
[100] RCEP - Telecommunications services - Korea proposal (Aug 2015)
http://www.bilaterals.org/?rcep-telecommunications-services
[101] Competition Chapter, http://www.bilaterals.org/IMG/pdf/rcep-competition.pdf

that Japan, Australia, South Korea, and New Zealand have been pushing for binding commitments from the RCEP members on ecommerce. A separate working group on ecommerce (WGEC) has been established with the aim of formalising a chapter on ecommerce in the final agreement.[102] Many of the TPP issues such as cross-border data flows, privacy and cybersecurity cooperation were laid out in the ecommerce terms of reference.

The proposed elements for negotiations are also understood to include domestic regulatory frameworks for market access, customs duties on electronic transmission, non-discriminatory treatment of digital products, paperless trading, electronic signatures, digital certificates and online consumer protection issues such as storage and transfer of personal data protection and spam.Controversial issues such as prohibition on requirements concerning the location of computing facilities and allowing cross-border transfer of information by electronic means are also expected to be included within the scope of the chapter. Further, countries including Australia and Japan have proposed making a permanent commitment to zero duties on digital transmissions, and prohibiting rules requiring on compulsory disclosure of source codes.

There is no consensus between China, India, Indonesia and other Southeast Asian countries on many of these issues, and it is possible that the RCEP might not lay down strong legal obligations on electronic commerce similar to that of the TPP. The latest information from the negotiating room suggest that the e-commerce chapter of RCEP will be far less ambitious, dealing mostly with familiar and uncontentious issues such as standards for electronic payments and signatures.[103]

Concerns have also been raised on provisions included under the leaked IP chapter notably on enforcement in a digital environment and failure to include fair-use exception may end up expanding the the digital divide. RCEP attempts to enshrine stringent obligations for the protection of broadcasters that remain controversial and are currently still under negotiation at WIPO.[104]

---

[102] Terms of Reference, Working Group on
http://www.bilaterals.org/IMG/pdf/ecommerce_draft_terms_of_reference.pdf
[103] Jyoti Panday, E-commerce RCEP Chapter: Have Big Tech's Demands Fizzled?
https://www.eff.org/deeplinks/2017/08/e-commerce-rcep-chapter-have-big-techs-demands-fizzled
[104] Jeremy Malcolm, RCEP: The Other Closed-Door Agreement to Compromise Users' Rights

4. Digital Trade and Internet Governance

While trade agreements aim to promote trade through liberalization, this often leads to a commercialised and commoditised approach to many of the issues they make rules on. On internet related matters, the push for such a commoditized framework of rules is evident in introduction of core internet governance issues such as privacy, data transfers and net neutrality as 'ecommerce' provisions in trade agreements. Digital issues that are being treated in trade agreements are rapidly extending from those that are closely analogous to rules on trade in goods, such as duties and market access restrictions, to those that are further removed, such as rules on spam, network neutrality, and country-code domain names. Given that there is no global internet governance regime that creates hard law obligations, there is a danger of the trade law regime becoming the de-facto international rules on the subject.

In this section we address some of the emerging themes and issues in the context of the digital economy that are increasingly being included in trade agreements. A comparison of the various issues included across current trade negotiations is included as Annex I.

4.1 Paperless Trading

In order to facilitate cross-border trade governments strive to make trade procedures as efficient as possible, in particular through implementation of automated customs systems, electronic single windows and other digital customs and trade facilitation initiatives. These paperless trade measures are rapidly becoming essential not only to maintain trade competitiveness, but also to address the trade control and logistics challenges associated with an increase in small shipments and cross-border e-commerce.[105] Paperless trade generally refers to the conduct of international trade transactions using electronic rather than paper-based data and documents.[106] Overall, the significant benefits for both Governments and traders have led an increasing number of countries to promote paperless trade, including as part of multilateral and preferential trade agreements.

https://www.eff.org/deeplinks/2016/04/rcep-other-closed-door-agreement-compromise-users-rights

[105] Yann Duval and Kong Mengjing Digital Trade Facilitation: Paperless Trade in Regional Trade Agreements, https://www.adb.org/sites/default/files/publication/321851/adbi-wp747.pdf

[106] Sung Heun Ha and Sang Won Lim (2014).

An analysis of the number of paperless trade measures in RTAs entered into force globally since 2005 highlights the number has essentially doubled, with a large majority of RTAs now featuring one more measures aiming to exchange trade-related data and information electronically.[107] While 30 of the 138 RTAs reviewed feature one or more Articles dedicated to "Paperless Trading" or "Paperless Trade Administration", provisions related to more specific paperless trade measures are found in different chapters, including but not limited to chapters on Customs and trade facilitation as well as on e-commerce. In many cases, recent RTAs are found to go further than the WTO TFA in promoting digital trade facilitation and the application of modern information and communication technologies to trade procedures – with the possible exception of e-payment of duties and fees, which is not specifically mentioned in any of the RTAs reviewed.

Nations believe that paperless trade generates significant economy-wide savings, including direct savings to traders in the form of lower compliance costs, as well as indirect savings from faster movement of goods and lower inventory costs.[108] In addition, through reduction in clearance times, it can increase port efficiency and reduce port congestion and related problems. Importantly, the use of electronic rather than paper documents can also help enhance regulatory control and compliance by governments, especially when relevant data and documents can be exchanged among agencies and across borders. In particular, the availability or more accurate and timely data in electronic form can enable trade control agencies to more efficiently evaluate the compliance risks associated with individual shipments, enabling them to identify high-risk transactions, ultimately boosting customs revenue while also speeding up the trade of compliant traders.[109]

The "Framework Agreement on Facilitation of Cross-Border Paperless Trade in Asia and the Pacific" (FA-PT) opened for signature on 1 October 2016, as the newest UN treaty in the

[107] Ibid 92

[108] UNNExT Briefs on single window implementation in Republic of Korea, as well as Senegal, Singapore and Thailand. http://unnext.unescap.org

[109] For example, Ghana Customs reports that its electronic Single Window launched in 2015 helped boost revenue collection by almost 15% in one year, while cutting down waiting time and approval for classification of goods from 2 weeks to 2 days – See more at: http://thebftonline.com/business/economy/21250/single-window-boosts-revenue-collection-148-in-one-year.html#sthash.bASAWHGE .dpuf

area of trade and development.[110] The FA-PT is not a regional trade agreement in the common sense of the term, as it does not include any trade liberalization commitments and focuses solely on enabling cross-border trade-related electronic data exchange among parties. It has been described as a regional "digital complement" to the WTO Trade Facilitation Agreement (TFA).[111] Developed and negotiated by ESCAP Member States following adoption of a resolution on Enabling Paperless Trade [...] for inclusive and sustainable intra-regional trade facilitation in 2012, it can be expected to provide a supportive and dedicated framework to accelerate the harmonized implementation of paperless trade commitments made by ESCAP Members with each other through RTAs.

Many of the recent RTAs implicitly or explicitly call upon the parties to develop electronic exchange of trade-related data and documents and work towards interoperability of paperless trade systems. However, they provide little detail on how to do so beyond recommending cooperation among the Parties taking into account existing international standards and tools. In this context, the new UN treaty on facilitation of cross-border paperless trade in Asia and the Pacific (FA-PT) provides a useful multilateral framework through which paperless trade-related RTA commitments may be concretized.

Detailed provisions on electronic authentication and electronic signature, nor does the WTO TFA. In contrast, other RTAs generally seek to promote acceptance and mutual recognition of electronic authentication and signatures, including by encouraging the parties to maintain flexible and technology neutral laws and regulations in this area. These measures are typically found in the articles titled "Electronic Authentication" and/or "Electronic Signature"[19] under the chapter of Electronic Commerce.

In KOR-US and TPP, this is done by specifying what type of legislation parties should not adopt, e.g., laws that would "prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction" (TPP Article 14.6) or "deny a signature legal validity solely on the basis that the signature is in electronic form" (KOR-US Article 15.4). Interoperability of electronic authentication and/or digital

[110] Any of the 53 Member States of the United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) may become a party. See: http://www.unescap.org/resources/framework-agreement-facilitation-cross-border-paperless-trade-asia-and-pacific

[111] http://www.tfafacility.org/new-un-treaty-facilitate-paperless-trade-asia-and-pacific-support-trade-facilitation-agreement

certificates is also encouraged in both the agreements, in the TPP. On 12 June 2007, the OECD Council adopted a Recommendation encouraging efforts by Member countries to establish compatible, technology-neutral approaches for effective domestic and cross-border electronic authentication of persons and entities.[112] This Recommendation reaffirms the important role of electronic authentication in fostering trust online and the continued development of the digital economy.

4.2 Custom Duties

Wireless technologies have evaporated geographical barriers for transactions but are also impacting traditional manufacturing and supply chains. Advances in technology such as e-commerce, 3D printing and data mining are driving the digital economy and force trade practices to be evaluated and adapted for constantly changing realities. Goods remain the dominant product that is traded across borders, and as these physical products add in a digital component it will be essential to revisit customs policies that were written for an analogue world.

Consider the global 3D printing market, the size of which has reportedly topped US$4 billion in 2014, with a compound annual growth rate over the past three years of 34%.3 The industry is projected to surpass US$21 billion by 2020, as the technology matures and faster, more affordable printers come to market.[113] Traditionally, material objects (whether chips, sweaters or automobiles) have been built in factories controlled by a single corporate entity that designs the product, manages its supply chain, constructs and sells it, directly or indirectly. 3D printing is about to kick off an era of digital transformation that will redefine such classic models. 3D printing will affect customs duties, especially if it causes the actual production place to shift from one country to another: the consumer

[112]OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, http://www.oecd.org/sti/ieconomy/38921342.pdf

[113]3D Printing Issues and impacts, http://www.ey.com/Publication/vwLUAssets/ey-3d-printing-taxation-issues-and-impacts/$FILE/ey-3d-printing-issues-impacts.pdf

downloads the object design from a foreign server and locally conducts the manufacturing process, which would otherwise have taken place abroad. As

As physical borders disappear, the digital economy raises many new questions in the area of customs duties. 3D printing, cross-border financial services and the Internet of Things (IoT) are focusing national and supranational legislators to think of alternative ways to tax these technologies and business models.

At the Bali Ministerial Conference in December 2013, WTO members decided to extend the existing "moratorium" on e-commerce and to abstain from imposing customs duties on electronic transmissions until the 10th Ministerial Conference. In 2015, WTO members meeting as the General Council agreed on on a draft ministerial decision on electronic commerce.[114] Under the draft decision, the WTO members would be asked to continue the practice of not imposing customs duties on electronic transmissions until the next session of the Ministerial Conference in 2017.

The US now wants a permanent moratorium on customs duties on electronic transmissions. "Permanent moratorium would be a very good idea and clearly we want the WTO to be part of the discussion on the future of the Internet," US trade envoy Michael Punke said after the general council meeting at the WTO adding that, "It would be sad if the WTO miss out on that opportunity." [115] The European Union, guiding principles on custom duty related negotiations can be found in the EU's Union Customs Code (UCC).[116]

Developing countries, such as India, Brazil, South Africa, China and Nigeria, are concerned about the implications of foregoing customs revenue on electronic transmissions. At the same meeting, India made a brief statement against preparing any recommendations on e-commerce at this juncture. The Indian trade envoy said the discussion which is taking place on e-commerce in various WTO bodies, including the moratorium for not imposing

---

[114] Draft decision agreed on electronic commerce,
https://www.wto.org/english/news_e/news15_e/gc_30nov15_e.htm
[115] India, US on a collision course over e-commerce, IP norms
http://www.livemint.com/Politics/FNMRmLJElPC6zwA7K4NZQL/India-US-on-a-collision-course-over-ecommerce-IP-norms.html
[116] The Union Customs Code and the digital economy
http://www.ey.com/gl/en/services/tax/vat--gst-and-other-sales-taxes/ey-managing-indirect-taxes-in-the-digital-age-ch6-case-study-the-union-customs-code-and-the-digital-economy

customs duties on electronic transmissions, is not advanced enough to make recommendations.

In a recent informal meeting with members, the trade representative from Panama at the WTO who has been appointed as a "friend" by the WTO Council to oversee discussion on e-commerce conceded that there is simply not enough information to fully appreciate the consequences of a permanent moratorium on customs duties on electronic transmissions. If the moratorium on e-commerce expires at the Nairobi meeting due to a lack of consensus, then customs duties can be imposed by WTO members on electronic transmission, which would be a setback to the US in its drive to negotiate new trade rules for e-commerce.

Not surprisingly, the U.S. is pushing rules for custom duties on electronic goods and services through various bilateral, and regional FTAs. On May 1, 2015, Deputy USTR Ambassador Robert Holleyman II gave a speech urging for custom duties on digital products to be prohibited.[117] He stressed that the United States' trading partners should refrain from discriminating against the digital products of foreign providers and collaborate to develop rules to prevent not only discriminatory and protectionist barriers. The leaked TPP, TTIP and NAFTA texts include provisions on custom duties and it is expected that the e-commerce chapter in RCEP will contain similar provisions.

Discussions and suggestions on custom duties in trade agreements have ranged in suggestions offered. They include increasing import duty rates and addressing whether separate tariff headings are required, applying export controls or restrictions, to designing new customs valuation rules for importing intangibles which would mean deciding how to appraise electronic data for customs purposes. Some countries have also suggested increasing rates of value-added tax (VAT) or introducing new taxes on services.

4.3 Cross-border Data Flows and Data Localization

The digital economy relies on cross-border provision of services and goods, and in the past government trade regulators have embraced the borderless nature of the Internet or adopted light-touch regulation. But with the growing perception of data

[117] Remarks by Deputy U.S. Trade Representative Robert Holleyman to the New Democrat Network, https://ustr.gov/about-us/policy-offices/press-office/speechestranscripts/2015/may/remarks-deputy-us-trade

as the new oil, governments around the world are now flexing their muscles and stepping up efforts to limit or tax cross-border data flows. Multiple countries have enacted laws localizing storage and processing of data within their territory or subjecting cross-border transfers to to strict conditions.[118] National localization is creating tension within trade negotiations such as RCEP, NAFTA, and TiSA in which countries like the United States, Singapore, Thailand and Japan, along with tech companies, are seeking to prohibit data localization practices.

Government's push for data localization to achieve diverse policy goals even though there is an inherent conflict between the logic of data localization efforts and the policy objectives that countries pursue by participating in free trade agreements. Resolving localization demands and reconciling conflicting ideologies and interests may be difficult to achieve in the context of trade agreements. Experts are also concerned that trade solutions to data localization may get caught up in the wider socio-politics of trade and Internet governance. Negotiating on data localization for the protection of personal information creates similar concerns, in addition to the the risk of compromise on protections that should be a minimum guarantee as countries could lay down localization conditions as a trade-off for respecting privacy rights.

Government demands for localization are driven by diverse rationales, one of which is and policy impetus could be security or surveillance concerns. China's Security Law (CSL) which limits operations and maintenance of Critical Internet Infrastructure (CII) to Mainland China as matter of national and cyber security is one recent example. Vietnam and Indonesia mandate maintaining in-country servers for access by law enforcement agencies. The desire to attract investment, fuel innovation and create competitive advantage for local companies is another important logic driving localization efforts. When framed from the narrative of economic and employment gains, localization is politically appealing and enjoys

[118] Data Localization Laws: an Emerging Global Trend
http://www.jurist.org/hotline/2017/01/Courtney-Bowman-data-localization.php

support of local business constituencies. This approach seems to be at working for some countries. Google and Amazon Web Services (AMS) have announced data centers in Singapore, Taiwan and Japan. Alibaba Cloud the computing arm of the Chinese company announced that it would be setting up data centers in India and Indonesia.[119]

Protection of national autonomy or efforts to reign in the hegemony of U.S. firms is used to drum-up support for introducing rules for transfers of data. India's telecom regulator issued a consultation paper exploring measures to address cross-border flow of information and jurisdictional challenges in the digital ecosystem. The regulator's move appears to be triggered by its displeasure with Apple's refusal to list an app developed by the regulator that tracks user's messages and call logs to identify spam.[120] Beyond the economic rationale, there is a growing perception that nations able to control data flows will fare better in the Internet governance order. For developing and developed countries alike, leadership with regard to digital economy is linked to establishing their claims of sovereignty in cyberspace. Therefore, nations mandate storage and processing of data by specific entities or network architectures within their jurisdiction. In a similar vein, governments may also lay down conditions for allowing transfer of data such as the company's nation of incorporation or principal sites of operations and management. The new Chinese cybersecurity regulation defines the notion of territory not based on location of operations but also includes ownership to be linked to territory.

Not all localization demands are blanket bans on data transfers or on the use of foreign servers. Establishing local facilities can also be incentivized by raising the costs of the data transfer to other jurisdictions either through tedious procedures

---

[119] Alibaba Cloud to open data centres in India, Indonesia, http://www.thehindu.com/business/alibaba-cloud-to-open-data-centres-in-india-indonesia/article18955632.ece

[120] Trai to start consultation process on data ownership http://economictimes.indiatimes.com/articleshow/59978434.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst http://economictimes.indiatimes.com/news/economy/policy/trai-to-start-consultation-process-on-data-ownership/articleshow/59978434.cms

or through strict compliance obligations. A recent example would be the security review procedure for transfer of personal information laid down under the Chinese cybersecurity law. Other localization laws maybe narrow in scope. South Korea's Land Survey Act banning exporting local mapping data to foreign companies that do not operate domestic data servers. India's National Data Sharing and Accessibility Policy requires all data collected using public funds to be stored within the borders of India.

Another important issue driving localization demands is privacy and protection of personal information. The inclusion of commitments prohibiting localisation mandates in treaties is seen as a victory for user rights, security and openness of the Internet. However concerns about the lack of control over user data and its transfer, processing and storage in jurisdictions with autocratic governments, a weak rule of law, or surveillance programs, remain. This has led governments to recognise data protection as a legitimate reason to limit transfer of data. For example, without such exceptions sensitive health information from Canada and Australia could be processed in jurisdictions with weaker privacy protections. The European Union also maintains that data protection and privacy are legitimate reasons to place limits cross-border transfer of data.

Not surprisingly, there is strong pushback from the US and large tech firms on the stance. Last week, the Information Technology Industry Council (ITIC) a US-based technology group has alleged that several countries, including India, China, South Korea, Russia, Vietnam, Canada, Mexico and Indonesia have turned to discriminatory policies and forced localisation that unfairly disadvantage American companies.[121] The group has submitted a report to the Trump Administration and is urging for an intervention from the Trump administration to remove barriers to trade.

[121] Trump admin urged to remove barriers to digital trade, https://www.outlookindia.com/newsscroll/trump-admin-urged-to-remove-barriers-to-digital-trade/1114082

The jury is still out on whether data protection based restrictions on data flows are protectionist and against trade and liberalisation, or whether such exemptions are necessary to guarantee the rights of citizens. Privacy experts have argued that data protection is qualitatively different from forced localization and the issue of data localization for data protection would disappear if nations implement stronger privacy laws or adopted baseline best practices.[122] Nevertheless countries continue to pursue carving exemptions for data protection in trade agreements.

Several regional trade agreements under discussion include provisions addressing the cross-border transfer of personal information. Texts and analysis of TTIP, TPP, TISA and NAFTA seems to suggest an emerging strategy on data localization linked to transfer of personal information. Participating nations commit to general obligations to not restrict data flows or to require localization of infrastructure, facilities or restriction on transfer of ICT goods and services. For the RCEP, which includes countries with strong national localization strategies or ambitions such as China and India, and countries like Australia and Japan that oppose localization, it is as yet unclear how data localization will be treated.

A strategy to harmonize national approaches followed in the TPP which may see adoption in other trade agreements such as NAFTA and RCEP would be to create exceptions for countries to not comply with general obligations against data localisations. Exceptions allowing restrictions have to based on 'legitimate public policy concerns' and are expected to provide the flexibility to accommodate national approaches in regional agreements. A foreseeable concern with such exceptions could be the possibility of countries using then to push for protectionist rules. While national security is a legitimate policy goals, allowing only national

[122] Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows 14-15 September 2016, The World Economic Forum, Geneva http://www3.weforum.org/docs/Background_Paper_Forum_workshop%2009.2016.pdf

companies to process personal data is also a barrier to trade and may lead to fragmented Internet. Seeking data to be treated according to higher standards of privacy and protection is also a legitimate policy pursuit. Not including such exceptions in some cases would essentially require certain countries to roll-back data protections guaranteed to citizens in order to allow cross-border transfer. Global trade bodies recognise the need for flexibility and the World Trade Agreement provides such exceptions under Article XIV GATS. A lot depends on the implementation of restrictions crafted under these exceptions.

4.4 Intellectual Property Rights

Over the years IPR issues have expanded beyond WIPO and have been included under the WTO framework through the TRIPS agreement. Following the Doha Round countries have also started to promote IPR provisions and commercial interests through two type of treaties investment protection agreements and FTAs. Several countries have been pushing to expand the scope of coverage and the duration of intellectual property rights, an approach that benefits large film studios, publishers, record labels and information vendors.

As noted above many countries have also sought to add new 'TRIPS plus' clauses that reduce the flexibility of the TRIPS agreement. The EU and U.S. are especially active when it comes to promoting IPR through the FTAs. As of 2017, the U.S. had signed free trade agreements (FTAs) with 20 countries, while the EU has FTAs with Chile, Mexico, and South Korea, among others, and is negotiating more with India, Asian bloc nations and the Mercosur (Mercado Común del Sur, or Common Market of the South).

Provisions that introduce TRIPS-plus clauses included in FTAs and mega-regional trade agreements such as the TPP, TTIP, NAFTA and RCEP cover several areas.[123]

[123]Beatriz Busaniche, Intellectual Property Rights and Free Trade Agreements: A Never-Ending Story, The Wealth of the Commons - A World Beyond Market and State

Patent Term Extension

Provisions that extend the duration of medicinal patents for as many as five years beyond the 20 years already provided for in the TRIPS are part of several trade agreements. The rationale given is that this compensates patent holders for the time needed to produce test data for marketing the drug in a given area.[124]

The patent term adjustment provisions has several implications including enabling rights holder to delay launch of the product in relatively low-priced markets, particularly developing countries. It would also not only deny access to a new medicine in the lower priced markets it creates conditions where even after the expiry of a patent in the developed countries, the product would retain monopoly status in the developing countries. This could on an average give at least two years of extended monopoly, further impacting generic growth and patient access.Provisions that link marketing approval by the drug regulator to the patent status of the drug also impact the availability of generics and extend monopolies in less-developed countries.

Data Exclusivity for Test Data

Some countries seek exclusive protection for the test data on drugs and agrotoxics. Such protection ensures that a drug regulator cannot rely on the innovator's data for approval of second and subsequent manufacturer's application for a specified period from the date of marketing approval to the innovator.[125] The provision reduces the flexible terms of the TRIPS that otherwise make it possible for the countries to recognize test data to approve a generic drug.

---

http://wealthofthecommons.org/essay/intellectual-property-rights-and-free-trade-agreements-never-ending-story#footnote1_lmmdb5q

[124] Impact Of The TPP On The Pharma Industry, Intellectual Property Watch https://www.ip-watch.org/2015/12/02/impact-of-the-tpp-on-the-pharma-industry/

[125] Ibid

This legal provision did not exist in the TRIPS and was deliberately excluded in that negotiation, but was included in US agreements. This has direct implications for access to medicines as it impedes generic drugs from entering the market. It also ensures extended monopoly for innovators in developing countries, though the patent may have expired in developed countries. This is because innovators launch their new drugs in low-priced countries years after their launch in the developed economies.

Expansion of Copyright Terms

One of the most contentious issue that is included in trade agreements is the extension of the copyright term to life plus 70 years, despite a broad consensus that this makes no economic sense, and simply amounts to a transfer of wealth from users to large, rights-holding corporations.[126] Some agreements have contemplated extending terms upto 120 years. Such extensions will make life more difficult for libraries and archives, for journalists, and for ordinary users seeking to make use of works from long-dead authors that rightfully belong in the public domain.

Many agreements include texts laying down transition periods which allow some countries a longer period for complying with some of their obligations, including copyright term. For example, in TPP Malaysia has been allowed two years to extend its copyright term to life plus 70 years. For Vietnam, the transition period is five years. New Zealand is the country receiving the most "generous" allowance; its term will increase to life plus 60 years initially, rising to the full life plus 70 year term within eight years. Yet Canada, on the other hand, has not been given any transition period at all.

[126] TPP's Copyright Trap, https://www.eff.org/issues/tpps-copyright-trap

Digital Rights Management

New trade agreements increasingly include obligations such as protecting Digital Rights Management (DRM) that use technology to regulate the number of times a work in digital format may be used, and the conditions of use. Such restrictive technical measures can, for example, track usage to determine whether a work has been copied, loaned, read one or more times, shared, and even printed, in the case of texts. In some legal systems, such as the Digital Millennium Copyright Act of the US evading these technical measures is a crime, even when done to exercise a right, such as access to works in the public domain, or fair use. In the U.S., such provisions have been used by business competitors to try to block printer cartridge refill services, competing garage door openers, and to lock mobile phones to particular network providers.

Some nations have a trade obligation to implement anti-circumvention laws, but this obligation is less strict than many national implementations in law. The TPP text on DRM would have compelled signatory nations to enact laws banning circumvention of digital locks or technological protection measures (TPMs).[127] The TPP parties' flexibility to allow DRM circumvention also requires them to consider whether rightsholders have already taken measures to allow those non-infringing uses to be made. This might mean that rightsholders will rely on the walled-garden sharing capabilities built into their DRM systems, such as Ultraviolet, to oppose users being granted broader rights to circumvent DRM.[128]

The provision was included despite opposition from countries like Chile. This would have required countries like New Zealand to completely rewrite its innovative 2008 copyright law, as well as override Australia's carefully-crafted 2007 TPM regime exclusions for region-coding on movies on DVDs, video games, and players, and for

[127] EFF Analysis of the TPM provisions in the U.S., February 2011 proposal for the TPP IP Chapter, 2011, https://www.eff.org/files/filenode/eff_tpp_tpm_analysis_0.pdf
[128] UltraViolet Is Not Enough: Copyright Must Allow Innovation for All https://www.eff.org/deeplinks/2013/11/copyright-must-allow-innovation-for-all

embedded software in devices that restrict access to goods and services for the device—a thoughtful effort by Australian policy makers to avoid the pitfalls experienced with the U.S. digital locks provisions.

The inclusion of DRM provisions in trade agreements is problematic for several reasons. IP regimes vary from nation to nation and reflect national development priorities moreover a nation's limitations and exceptions to copyright are a powerful means of boosting local industry and fostering domestic entrepreneurs. DRM can be used to overrule these priorities, so that foreign companies can trump local domestic policy with technological means.[129]

DRM systems require that their users take a restrictive license from a cartel, often at a high cost. These licenses have the effect of turning publishers and performers and authors into customers for developed-world intermediaries to whom they become beholden. DRM technologies cannot be embodied in FOSS and so any field where DRM is adopted crowds out FOSS and eliminates the development benefits therein. [130]

DRM systems retard innovation, putting new features under the veto of incumbent industries who fear being out-competed by new market entrants. "Renewable" DRM can be used to cheat consumers by removing or altering features after they have bought their devices DRM systems can't protect themselves, they require "anti-circumvention" laws to silence researchers who discover their flaws Anti-circumvention laws have been used to silence and even jail researchers who embarrassed entertainment companies and DRM vendors with revelations about the failings in their systems.

---

[129] Digital Rights Management: A failure in the developed world, a danger to the developing world. For the International Telecommunications Union, ITU-R Working Party 6M Report on Content Protection Technologies http://www.twn.my/title2/FTAs/Intellectual_Property/Copyright/digitalrightsmanagementEFF.pdf

[130]How Trade Agreements Harm Open Access and Open Source https://www.eff.org/deeplinks/2015/10/how-trade-agreements-harm-open-access-and-open-source

The ability of disabled people to benefit from digital media is badly undermined by DRM. Copyright law often affords rights to disabled people that trump the rights of author DRM lets private rightsholders unilaterally prevent the exercise of those rights. DRM also undermines distance education by raising the cost of providing instructional materials and by placing barriers to.

Alongside the prohibition on circumvention of DRM in the TPP was a similar prohibition on the removal of rights management information, with equivalent civil and criminal penalties. Since this offense is, once again, independent of the infringement of copyright, it could implicate a user who crops out an identifying watermark from an image, even if they are using that image for fair use purposes and even if they otherwise provide attribution of the original author by some other means. The distribution of devices for decrypting encrypted satellite and cable signals is also proscribed in many agreements posing a further hazard to hackers wishing to experiment with or to repurpose broadcast media.

Intermediary Liability

In addition to copyright terms trade agreements also tackle rules for intermediary liability for third party content. The U.S. particularly seeks to push its DMCA notice-and-takedown system through its FTAs and RTAs. This has the effect of lowering the standards and safeguards that are prevalent in other liability regimes. For example in the TPP the allows variations of other liability regimes such as Canada's notice-and-notice or Japanese safeguards of independent assessment of takedown notices but the benefits are limited in specific jurisdictions.[131] Similarly Chile's system under which ISPs are not required to take down content without a judicial order is explicitly worked in, but no other country joining the TPP in the

[131] TPP Creates Legal Incentives For ISPs To Police The Internet. What Is At Risk? Your Rights. https://www.eff.org/deeplinks/2012/08/tpp-creates-liabilities-isps-and-put-your-rights-risk

future will be allowed to have a similar system. The agreement entrenches flawed notice-and-takedown regime as an international standard.[132]

In the NAFTA negotiations Hollywood lobby is attempting to changes to the safe harbors of the DMCA that have provided immunity for intermediaries from damages and liability for third party content.[133] Previous U.S. free trade agreements incorporated language that closely tracked DMCA and technology associations such as CCIA have advocated inclusion of a similar provision in NAFTA.[134] Recording Industry Association of America (RIAA)[135] and the Motion Picture Association of America (MPAA)[136] supports a safe harbor provision in NAFTA that is limited to "passive intermediaries without requisite knowledge of the infringement on their platforms, and inapplicable to services actively engaged in communicating to the public." In amicus briefs in several cases interpreting the DMCA, RIAA and other copyright industry associations have argued that the DMCA's hosting safe harbor, applies only to the act of storing content uploaded by the user, but not to subsequently making the content available to the public.

The courts have rejected this overly-narrow interpretation of the DMCA yet that is exactly what RIAA seeks to incorporate in NAFTA. RIAA further seeks that NAFTA require that injunctions should be available against all intermediaries, including ISPs and search engines, and that such injunction "be dynamic, i.e., covering future domain changes." Such injunctive relief would go well beyond the current standards.

---

[132] Canada Must Fix Rightsholder Abuse of its Copyright Notice System
https://www.eff.org/deeplinks/2015/04/call-canada-fix-rightsholder-abuse-its-copyright-notice-system
[133] Jonathan Band, Digital Issues in NAFTA: Copyright Industry Comments on NAFTA
http://www.project-disco.org/intellectual-property/062917-digital-issues-in-nafta-copyright-industry-comments-on-nafta/#.Wc0a60x7FAY
[134] Comment from Matthew Schruers, Computer & Communications Industry Association
https://www.regulations.gov/document?D=USTR-2017-0006-1121
[135] {Request to Testify] Recording Industry Association of America
https://www.regulations.gov/document?D=USTR-2017-0006-1304
[136] Motion Picture Association of America
https://www.regulations.gov/document?D=USTR-2017-0006-1397

MPAA recommends for NAFTA "a new approach" that involves "moving to high-level language that establishes intermediary liability and appropriate limitations on liability." It observes that other countries have responded "more effectively and nimbly" to online infringement "through site blocking, notice-and-staydown, and injunctive relief." MPAA obviously hopes to leverage its "new approach" in NAFTA to amend safe harbours to obtain these remedies. The changes RIAA and MPAA seek are incompatible with the trade negotiating objectives set by Congress, which require that IP provisions of trade agreements "reflect a standard of protection similar to that found in U.S. law."[137]Moreover, they would be enormously controversial, and could very well derail the NAFTA negotiations.

In the last few years FTAs have included new clauses that impose "secondary liability" on Internet service providers, search engines and other types of services. These FTAs impose joint liability on these services for the actions of Internet users and requires services to look into, monitor, and swiftly act in response to a report of a copyright violation (without specifying what type of report triggers the duty and without guaranteeing the involvement of a judge). Such clauses override domestic judicial systems, constitutional due process guarantees and the presumption of innocence, and constitute a direct threat to freedom of expression on the Internet.

Criminal Enforcement and Civil Damages

Controversially some trade agreements have also included provisions on damages for copyright violations through which rightsholders can submit "any legitimate measure of value" to a judicial authority for determination of damages, including the suggested retail price of infringing goods. Additionally, judges must have the power to order pre-established damages (at the rightsholder's election), or

[137] Bipartisan Congressional Trade Priorities and Accountability Act of 2015 https://www.congress.gov/bill/114th-congress/senate-bill/995/related-bills

additional damages, each of which may go beyond compensating the rightsholder for its actual loss, and thereby create a disproportionate chilling effect for users and innovators. No exception to these damages provisions is made in cases where the rightsholder cannot be found after a diligent search, which introduction of orphan works in jeopardy.

In addition to liability of fines and criminal penalties, some agreements introduce strict measures where any materials and implements used in the creation of infringing copies can also be destroyed. The same applies to devices and products used for circumventing DRM or removing rights management information Because multi-use devices such as computers are used for a diverse range of purposes, this is once again a disproportionate penalty.

In some cases, the penalties for copyright infringement can even include jail time through provisions which make any act of willful copyright infringement on a commercial scale rendering the infringer liable to criminal penalties, even if they were not carried out for financial gain, provided that they have a substantial prejudicial impact on the rightsholder.

Dispute Settlement Mechanism

Several mega-regional and plurilateral trade agreements include provisions which enables private investors to use the investor dispute settlement mechanisms to interpret the IP Chapter as well as the TRIPS Agreement. In TPP IPR was a covered asset in the Investment Chapter and provided the arbitrators in the ISDS mechanism with discretion to interpret and decide on compliance with the TRIPS Agreement, even though the WTO has its own dispute settlement mechanism. Further, the IPR provision also curtail government's' ability to use a compulsory license as a tool to negotiate price with the rights holder, as was done by Brazil for antiretroviral medicines. Such provisions not only lead to forum shopping between the WTO Dispute Settlement Body and the ISDS mechanism, but also empower the private rights holder investors to bring cases against governments and benefit from

sanctions. In the past similar provisions were included in the NAFTA which led to the Canadian government and the judiciary of a country will be subject to arbitration proceedings by a private investor.[138]

Trade Secrets

Provisions that protect trade secrets are a common feature of IP chapters in trade agreements. Recent regional agreements have included provisions that criminalize those who gain "unauthorized, willful access to a trade secret held in a computer system," without any mandatory exception for cases where the information is accessed or disclosed in the public interest. Dangerously vague text on the misuse of trade secrets, which could be used to enact harsh criminal punishments against anyone who reveals or even accesses information through a "computer system" that is allegedly confidential. There is no evident explanation for the differential treatment given to trade secrets accessed or misappropriated by means of a computer system, as opposed to by other means. Such provisions stem from U.S. laws that have been used to persecute hackers for offenses that would otherwise have been considered much more minor.[139]

Domain Names

Provisions regarding issues of domain name dispute obliges countries to establish an appropriate procedure to resolve domain name disputes are also being included in plurilateral and regional FTAs. Usually such clauses appear in the IP chapter since it is structured as a trademark remedy against cybersquatting. Through domain name related clauses, a treaty member commits to implementing a dispute resolution system in their ccTLD system, based on the Uniform Domain Name Dispute Resolution Policy (UDRP). The UDRP is a policy designed by ICANN at the

[138] https://scrip.pharmamedtechbi.com/companies/198600152
[139]Cindy Cohn, Aaron's Law Reintroduced: CFAA Didn't Fix Itself
https://www.eff.org/deeplinks/2015/04/aarons-law-reintroduced-cfaa-didnt-fix-itself

global level for generic top level domains (gTLDs), but inclusion of such provisions in FTAs mandates adopting its principles at the national level.[140]

Another regulation that affects the domain name realm is a request in the treaties to allow online public access to a reliable and accurate domain registrant database (equivalent to a WHOIS database).[141] Such a clause pose inherent conflict to privacy laws as they seek to facilitate access to relevant data about a domain name registrant and to discourage anonymity in unlawful activities conducted over the web. Such clauses raise privacy issues and leaves possible conflicts between treaty obligations and national law unsolved. Inclusion of domain names related prescription of rules in trade agreements completely disregards the fact that most country code domain registries have their own, open, community-driven processes for determining rules for managing domain name disputes. More than that, this top-down rulemaking on domain names is in direct contravention of the multi-stakeholder model of Internet governance.

4.5 Unsolicited Emails and Malware

In both the TPP and the TiSA included provisions on spam or the issue of transmission of bulk unsolicited emails. Article 14.14 in the TPP text requires "measures regarding unsolicited commercial electronic messages" to be taken, but offers weakest possible guidance on what these should be.[142] The measures may include requirements on suppliers to allow users to opt out from receipt of messages, or require opt-in consent, or... "otherwise provide for the minimisation" of such messages. In sum, by backing away from a meaningful commitment to do anything, it requires nothing substantive at all. As with the TPP wording, the leaked draft of the TiSA e-commerce chapter includes language on spam, in article 5.

[140]Uniform Domain Name Dispute Resolution Policy
https://www.icann.org/resources/pages/policy-2012-02-25-en
[141] ICANN WHOIS https://whois.icann.org/en
[142] Maira Sutton, Medium
https://medium.com/@maira/this-provision-on-spam-control-in-article-14-14-e2e7694e2ba0

Given that spam is not a content but a consent issue and in light of the weak rules, it is apparent that trade agreements are not the most useful venue for addressing the spam problem.

Importantly, even though agreements cover SPAM they say nothing about malware. As Susan Aaronson points out malware is an important trade issue as it can be redefined as malicious cross-border information flows.[143] Malware not only damages business but has significant negative effects on human rights and cybersecurity. So far U.S. led trade agreements have included voluntary language on cyber security and cyber theft but not to try to address malware. Neither TiSA nor TPP draft text does not discuss cyber security or malware explicitly.

4.6 Prohibition on Source Code Disclosure

Another contentious issue on which rules are being set through trade agreements is the disclosure of source code. which would prohibit such open source or code audit mandates being introduced in the future. The TPP prohibits signer countries from asking software companies for access to their source codes. The TiSA negotiators also included language stating that no party may require the transfer of or access to source code, again similar to TPP's. TPP Article 14.17 of the text of the Electronic Commerce chapter provides, "No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory." The chapter says that governments cannot force suppliers to give up their source codes to foreign governments, even for national security reasons.

The provision on source code in TPP would also prohibit any requirement that code be submitted for private review by regulatory authorities. The clause forecloses the possibility of audit by the responsible licensing authority, health and safety

[143] Aaronson 2016

watchdog, or consumer protection agency. Only devices and software used in bespoke applications (not for a mass market) or in critical infrastructure would be exempt under the terms of the TPP language, though the precise ambit of these exemptions remains unclear. The NAFTA text also includes a similar provision which mandates that countries should not require the transfer of or access to mass-market software source code as a condition for the import, distribution, sale of use of such software or of products containing such software.

Proponents of the U.S. industries seek an "assertive U.S. negotiating stance is source code and proprietary algorithms."[144] On the face of it, in an environment where the Internet of Things is burgeoning and software quality is an important trade issue such restrictions seems to make no sense at all. Such demands stem from fears that in the absence of protection for software, other countries will be able to share them with national-champion competitors or state-owned enterprises. From this view trade secrets are an important aspect of source code and algorithm protection, the U.S. should require trade agreement parties to establish criminal procedures and penalties for trade secret theft, including by cyber systems.[145]

Prohibition on source code disclosure demands have increased in response to measures enforced by China that require the disclosure of source code to the Chinese government. part of China's framework regulations for information security in critical infrastructure, known as the Multi-Level Protection Scheme (MLPS).[146] The MLPS regulations limit products from being sold for use in Chinese information systems above a certain security level, unless their source code is disclosed to the government. Although this measure is presented as protection against security flaws and deliberate backdoors being inserted into critical

---

[144]Stuart N. Brotman, The road ahead for technology-related trade agreement terms https://www.brookings.edu/blog/techtank/2017/02/02/the-road-ahead-for-technology-related-trade-agreement-terms/

[145] Ibid

[146] USTR Releases Annual Special 301 Report on Intellectual Property Rights, https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/april/ustr-releases-annual-special-301

software, it is also seen by U.S. companies as an impingement upon their ability to keep their code proprietary.

U.S. software companies are pushing for mandates that prevent mandatory disclosure as they provide the bulk of mass market software in the market.[147] However the TPP provision does not resolve these issues as the MLPS regulations only apply to software used in critical infrastructure—which is expressly exempted from the TPP provision. Infact, these provisions could, indeed, undermine cyber security efforts.[148] Multiple recent reports on serious security vulnerabilities in cable modems and routers paint a dire picture of the state of security of the devices that millions of users depend upon to connect to the Internet.[149] Such vulnerabilities can be exploited to disable our access, snoop on personal information, or launch malicious attacks on third parties. Other devices that are important for our security, or even to our physical health and safety—such as home alarm systems[150] and, terrifyingly, a cardio server used in hospitals[151]—have also been the subject of recent vulnerability disclosures.

Having access to the source code of the software embedded in these devices allows security researchers to quickly uncover and eliminate such vulnerabilities. Such verification is made possible through licensing terms such as GNU General Public License[152], which applies to some of the core software, that legally compel manufacturers and suppliers to make their code available. Cybersecurity experts have also been pushing to impose legal or regulatory requirements for source code

---

[147] Aaronson 2016
[148] TPP Threatens Security and Safety by Locking Down U.S. Policy on Source Code Audit
https://www.eff.org/deeplinks/2015/12/tpp-threatens-security-and-safety-locking-down-us-policy-source-code-audit
[149] ARRIS Cable Modem has a Backdoor in the Backdoor,
https://w00tsec.blogspot.in/2015/11/arris-cable-modem-has-backdoor-in.html
[150] RSI Videofied Security Alarm Protocol Flawed, Attackers Can Intercept Alarms
http://news.softpedia.com/news/rsi-videofied-security-alarm-protocol-flawed-attackers-can-intercept-alarms-496920.shtml
[151] Vulnerability Note VU#630239
Epiphany Cardio Server is vulnerable to SQL and LDAP injection
http://www.kb.cert.org/vuls/id/630239
[152] GNU Operating System, http://www.gnu.org/licenses/gpl-3.0.en.html

disclosure and last year 260 cybersecurity experts called upon the Federal Communications Commission to impose just such a requirement.[153]

Source code disclosure also has significant implications for competition as it can make it impossible for competition authorities to open up the market for the repair of products with embedded software. If the source code in manufacturing or closed embedded systems are not shared it impacts innovation as markets for entrepreneurs to use their understanding of that code to make new devices that interoperate with proprietary software.

4.7 Access: Net Neutrality

Trade agreements also cover nascent technological areas where national policies have not been contemplated or regulation is in the early stages. For example, the the telecommunications chapter in the TPP agreement included provisions which requires member states to adopt network neutrality laws. The proposal requires that member states ensure that businesses from other member states have access to public telecommunications services, including Internet services, in all member states "on reasonable and non-discriminatory terms and conditions."

The language of the text is very clear in classifying ISPs as telecommunication service providers.[154] However the net neutrality provisions do not consider issues such as blocking and filtering. Moreover, the provision is not a mandated obligation and therefore it does not advance the issue.[155] In countries with no net neutrality laws here is no requirement to implement anything in order to comply with the agreement. For countries with net neutrality provisions, the TPP typically falls well

[153] Here's Why Cybersecurity Experts Want Public Source Routershttps://motherboard.vice.com/en_us/article/heres-why-cybersecurity-experts-want-open-source-routers
[154] Controversial Trade Deal May Actually Help Net Neutrality, https://www.wired.com/2015/11/tpp-net-neutrality/
[155] The Trouble with the TPP, Day 20: Unenforceable Net Neutrality Rules http://www.michaelgeist.ca/2016/01/the-trouble-with-the-tpp-day-20-unenforceable-net-neutrality-rules/

short of what they already have in place. In Canada, the CRTC's Internet Traffic Management Practices go far beyond the TPP, offering more comprehensive coverage, a complaints mechanism, and enforceable obligations overseen by the CRTC.[156] Although it stops short of requiring that member states adopt network neutrality laws the provision may give regulators authority to impose more strict rules on ISPs. The agreement requires that member states give its regulators the authority to create regulations to ensure access if necessary.

The requirements also apply to "interconnection" deals—the agreements ISPs strike to carry each other's data—which must also be offered at "reasonable rates." The proposal also calls for member states to ensure that telcos offer international roaming for mobile phones at "reasonable rates" and offer phone number portability between providers. While such terms are meant to avoid discrimination these are weak. For example "reasonable rates" and "non-discriminatory" are broad terms that are open to interpretation and will have to be decided at the national level. It also leaves states free not to intervene if regulators decide that telecommunications providers voluntarily meet the requirements.

4.8 Online Protection of Personal Information

Unlike the other categories of clauses, there is no unique language in these treaties about data protection, and no single specific chapter for dealing with this issue. This clause is usually contained in sections related to the content of the data or to telecommunications. Some of the clauses state, in general terms, that a treaty member may take measures necessary to ensure the security and confidentiality of telecommunication messages, and to protect the privacy of nonpublic personal data of subscribers to public telecommunications services – sometimes subject to

[156] Internet Traffic Management Practices
http://www.crtc.gc.ca/eng/internet/traf.htm

non-discriminatory terms. Several treaties establish a system of cooperation on personal data protection. The treaties also provide clauses on personal data in intellectual-property-related procedures (such as the protection of pharmaceutical data) or financial services, but these are not directly related to internet or telecommunications issues.

It is worth pointing out that EU treaties tend to establish a high level of protection as compared to all other agreements.[157] This is understandable given data protection regulations within the EU. Public support for strong data protection has a long and proud history in the European Union. Europeans view privacy as a vital human and consumer right. All 28 EU member states are also members of the Council of Europe, a group of 47 European countries, and as such, they are required under human rights law to secure the protection of personal data.22 Every EU citizen has the right to personal data protection and firms can only collect that data under specific conditions. The European Union also requires member states to investigate privacy violations.

The European Commission's Directive on Data Protection, which went into effect in October 1998, prohibits the transfer of personal data to non-European Union countries that do not meet the European Union's "adequacy" standard for privacy protection. Finally, the EU parliament voted in favour of the revised data protection rules in 2014. Parliamentarians agreed that non-European companies would have to fully meet the EU data protection law when offering goods and services to European consumers.[158] More recently, the EC insisted that "data protection in the European Union is a fundamental right".[159] Earlier this year, a working document on digital trade agenda released by the EU Member of Parliament acknowledged that,

[157] Celia Lerman, Impact of Free Trade Agreements on Internet Policy, a Latin America Case Study, http://repository.upenn.edu/cgi/viewcontent.cgi?article=1009&context=internetpolicyobservatory
[158] (European Commission 2014a
[159] (European Council 2015).

"Promoting the free flow of data and protecting the right to data protection and privacy actually go hand in hand."

The EU requires other countries to create independent government data protection agencies and to register databases with those agencies; in some instances, the commission must grant prior approval before personal data processing begins. Surprisingly, given its strong commitment to privacy, the EC has included only aspirational language on privacy in its free trade agreements. For example, in its agreement with Korea, chapter 6 refers to trade in data, and article 7.43 of the services chapter says that each party should reaffirm its commitment to protecting fundamental rights and freedoms of individuals and adopt adequate safeguards to the protection of privacy. Moreover, neither the European Union nor Canada included binding privacy provisions in their recent trade agreement, which was completed in 2014 but is not yet approved. Given the import of firms that use the free business model to the US economy, the United States has opposed any efforts to mandate a specific approach to data protection.

To bridge these differences in regulatory strategy, the "Safe Harbor Framework" or GDPR is coming into effect. European policy makers have developed guidance for rms on how companies can comply in the interim as the two develop a new approach to Safe Harbor (European Commission — Justice 2015c). According to EU Justice Minister Vera Jourová (2015), "The U.S. has already committed to stronger oversight by the Department of Commerce, [and to] stronger cooperation between European Data Protection Authorities and the Federal Trade Commission. This will transform the system from a purely self-regulating one to an oversight system that is more responsive as well as pro-active. We are also working with the U.S. to put into place an annual joint review mechanism that will cover all aspects of the functioning of the new framework, including the use of exemptions for law enforcement and national security grounds."

Meanwhile, companies are finding ways to meet the demands of their European customers. For example, Microsoft announced that, starting in 2016, it will allow European customers to store cloud data on German servers. Under German law, Microsoft would be unable to access its customers' data unlesstheircustomersexplicitlyauthorizeditorDeutsche Telekom approved a request to access the data. Microsoft frames it as a way to keep Europeans' data beyond the reach of US intelligence agencies (Segal 2015).

EU negotiators have tried to finesse the EU and US approaches in TiSA. In December 2014, the EU's trade spokesperson noted that only one of the participants had "proposed two provisions that should ensure free data ows and prohibit requirements to store data locally." The commission also underlined that "such provisions should be without prejudice to data protection requirements." Hence, the commission recognizes the need for clarity, noting privacy is a general "exception" in the GATS.

The "EU has asked for further clarification on these proposals and made it very clear that it cannot and will not agree to any language that could potentially prevent the EU from enforcing its own data protection standards." The spokesperson also noted that the GATS data protection standards, which include an exemption for future data protection measures "not inconsistent with the provisions of this Agreement," have thus far, according to the commission, "never led to any WTO country, either formally or informally, challenging EU rules on data protection (or any other country's system of data protection)." But the commission acknowledged that it will have "to analyse very carefully how any data transfer obligations in TiSA interact with that existing exception" (Ermert 2014).

Although the European Union has not used trade agreements to disseminate its approach to privacy, the EU Directive has had an effect on trade. Some nations, such as India and China, are weighing how to make their laws interoperable with EU privacy provisions. Meanwhile, other countries, such as the Philippines, have

adopted EU data protection policies. The EU would like to make its regulations on data protection global, which could have huge consequences for firms built on the mass acquisition of personal data, such as Facebook, Google, and so on. Such companies would have to change their business models.

While there is no global framework for data protection, there are regional initiatives such as the Asia Pacific Economic Cooperation (APEC) Privacy Principles and the Cross Border Privacy Rules (CBPR) systems principles and guidelines for the development of a system of voluntary cross-border transfer of personal information.[160] In addition to Canada, Japan, Mexico, and the US, nearly two dozen private companies are also participatory members in the CBPR framework. Earlier this year, South Korea became the fifth member and Singapore and the Philippines are expected to join in the near future. Many trade agreements use the APEC framework as a baseline.

Part IV: Transparency and Openness in Trade Negotiations

Governance of the Internet is not a single-issue area. Its governance encompasses a constellation of administrative and technical coordinating tasks necessary to keep the Internet operational and to enact related public policy. The tasks range from technical standard setting and the administration of domain names and numbers to setting policies related to cyber security and privacy. As the Internet has evolved, many of these functions have been carried out by the private sector and by the Internet's technical community — which includes the Internet Engineering Task Force (IETF) and its institutional home, the Internet Society; the World Wide Web Consortium; regional Internet registries; and ICANN.

[160] Asia Pacific Economic Cooperation (APEC) Privacy Principles https://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

Tensions between multilateral oversight and private-sector-led multi-stakeholder oversight can be seen in many of the global policy controversies around the Internet, ranging from long-standing questions about how to transition US oversight of Internet names and numbers to debates about types of interconnection that arose at the World Conference on International Telecommunications convened in Dubai in 2012. Tensions between governments and the private sector are also evident in debates about encryption that mediate competing values in cyberspace, such as law enforcement and national security versus individual privacy and economic security.

The determination as to which of these standards is broadly applied often depends upon private corporate decisions about their inclusion in commercial products. Private contracts among different tiers of ISPs use BGP (border gateway protocols) and undersea cables to connect the many networks that make up the Internet. National governments control copyright and intellectual property laws, although they are subject to negotiation and litigation, sometimes within the frameworks of the WIPO and WTO.

The United Nations Charter, the Laws of Armed Conflict (LOAC) and various regional organizations provide a general overarching framework as national governments try to manage problems of security and espionage. The Council of Europe's Convention on Cybercrime (2014) in Budapest provides a legal framework that has been ratified by 42 states. Bilateral negotiations, track two dialogues, regular forums and independent commissions strive to develop norms and con dence-building measures. Much of the governance efforts occur within national legal frameworks. Providing security is a classic function of government, and some observers believe that growing insecurity will lead to an increased role for governments in cyberspace.

Many states desire to extend their sovereignty in cyberspace, seeking the technological means to do so. As Diebert and Rohozinski (2010) put it, "securing

cyberspace has definitely entailed a 'return of the state' but not in ways that suggest a return to the traditional Westphalian paradigm of state sovereignty." Moreover, while accounts of cyberwar have been exaggerated, cyber espionage is rampant and more than 30 governments are reputed to have developed offensive capabilities and doctrines for the use of cyber weapons.[161]

Efforts to attack or secure a government network also involve the use of cyber weapons by non-state actors. The number of criminal attacks has increased, with estimates of global costs ranging from US$80–400 billion annually.[162] Corporations and private actors, however, can also help to protect the Internet, and this often entails devolution of responsibilities and authority (Deibert and Rohozinski 2010, 30; see Demchak and Dombrowski 2011). Governments want to protect the Internet so their societies can continue to benefit from it, but at the same time, they also want to protect their societies from what might come through the Internet.

Given the complexity of issues the multi-stakeholder approach works best. However, multi-stakeholderism is sometimes viewed as a value in itself rather than a possible set of approaches for meeting more salient public interest objectives such as human rights, Internet security and performance, or financial stability. The more appropriate approach to responsible and efficacious governance requires determining what types of administration are optimal in any particular functional and political context. For example, in the area of Internet governance, some policy-making tasks may appropriately be relegated to the private sector, some to the purview of traditional sovereign state governance or international treaty negotiations, and some more appropriately as multi-stakeholder.

In order to foster electronic trade, while harmonising the regulatory environment, several organisations have developed international frameworks, such as the Guidelines on the Protection of Transborder Data Flows of Personal Data, included

[161] (Rid 2013)
[162] (Lewis and Baker 2013, 5).

in the OECD Electronic Commerce initiative. governments and business actors have been calling for harmonised rules to enable international trade.

Indeed, shared rules and principles seem to be as useful as they are needed to guarantee a common level of consumer protection, data protection, and cybercrime prevention. Given the rise of ecommerce and digital issues it is critical to determine which issues of governance are appropriate to be included in trade agreements. Further, as often happens in intergovernmental settings, the pace of negotiations has been relatively slow due to the difficulty of finding compromise amongst divergent economic interests.

Notably, it is possible to see a clear division between developing and developed countries on the pace and the content of the digital trade agenda. While the latter are pushing for a speedy way forward and comprehensive talks, the former are being more conservative with issues that should be included and are emphasising the need for capacity building.In parallel to multilateral venues, groups of countries have joined together to more swiftly negotiate plurilateral agreements. More importantly, there is an urgent need to open up the processes where the rules for the digital trade agenda are being set.

Rethinking Internet and Trade

Table: Transparency in trade policymaking: A comparative perspective US-EU

	US	EU
Release of negotiating mandate / negotiating objectives	· No FTA-specific negotiating mandate · Broadly defined objectives under trade promotion authority	Release of negotiating mandate since 2014 (CETA and TTIP negotiations)

Impact assessments and reviews	· **Ad hoc for Congressional hearings;** · **More systematic for environmental reviews**	**Systematic for comprehensive ex-ante studies**
Negotiating texts	**Negotiating texts available only to cleared members of trade advisory committees**	**Position papers and negotiating texts increasingly available online, eg. TTIP and EU-Tunisia FTA**
Information on negotiation rounds	**Short and irregular ex-ante briefings on agenda of negotiations, and short chief negotiator reports after rounds**	**Extensive reports on the content of negotiations leaving out certain specific positions**
Online consultation: release of public comments	**Public comments received on negotiating objectives for TPP and TTIP, but not on specific text proposals**	**Limited to summary of statistical results**
Investor-state dispute settlement	· **Private hearings; release of documents conditioned to approval by all parties;** · **New commitments to transparency under TPP regarding proceedings and documents and third-party participation through *amici curiae***	· **UNCITRAL (2014) transparency rules in CETA: open hearings and release of documents conditioned to approval by all parties**

Source:

Trade agreements are disconnected from democratic oversight, swamped in the influence of influence from lobbyists and special interests. Agreements are negotiated with levels of confidentiality that go far beyond those necessary for effective deal-making. The present processes of trade negotiations resulted in a

loss of public trust in government's ability to negotiate trade agreements that provide for the good of all. Existing global trade rules are not equipped to address the unique challenges and governance issues that new technologies and business models raise. In the absence of legal certainties and global frameworks governments draw up unilateral rules to regulate domestic markets. This creates several risks including barriers to access for small and large companies, higher costs for consumers and ultimately the risk of fragmentation. For instance, in some countries technology firms are forced to hand over the source code of products to a regulator as a requirement to access a market. Such rules negatively impact people's human rights and create uncertainty and distrust regarding the use or safety of certain products.

Table 3: Transparency in regional trade agreements

	Publish textual provisions	Consolidated texts published after each round	Textual proposals open to public comments and hearing	Leaks
RCEP	No	No	No	Yes
TPP	No			Yes
TiSA				
TTIP				Yes
NAFTA				

When these secretive, omnibus proposals are finally released, they do not stand scrutiny and are subject to public outrage. The adoption of global or regional trade

rules need to balance competition and innovation at the national and regional level. Powerful private and public actors have found a way to use these secret trade agreements to push for regulation that would not survive the scrutiny of a more transparent, democratic rulemaking process. Trade agreements are multilateral and allow for very limited access. In contrast most internet governance venues allow for the participation of the civil society, private sector and technical communities on equal footing with governments.

The opacity of process associated with trade negotiations is at odds with multistakeholder, open, accountable forms of participation practiced at various internet governance venues. Further, the adoption of global or regional trade rules needs to be researched and studied from diverse fields to understand the impact of agreements on the internet and the information society. However, the confidentiality of trade processes and secrecy of negotiations prevents meaningful engagement from stakeholders that will be impacted by these rules.

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.

Given the complexity of trade negotiations and the fast-changing pace of the digital environment, government officials, even with the advice of established businesses, are not always equipped to negotiate fair trade deals. Stakeholders can provide invaluable expertise to ensure that trade negotiators maximize the economic potential of trade while preventing it from being captured by special interests. In many cases, a wider and open process can offer a more balanced view of the

economic and political stakes of negotiations, thereby bringing more legitimacy to trade policymaking.

It is vital to open up trade processes where rules for internet governance are being negotiated and decided so that participation from stakeholders can ensure that policies and laws are developed to defend and promote free expression and innovation. Given the borderless nature of the Internet, it is also valuable to encourage greater consistency in the rules and issues that are being introduced through these agreements. To this end, we have come together to develop a set of resources to help introduce participatory norms and open digital trade processes.

Brussels Declaration on Trade and Internet

"...The procedural deficits that define modern trade agreement negotiations have resulted in instruments that are unduly deferential to the interests of a narrow class of established industry stakeholders, and fail to address the needs of broader affected communities. This stands in stark contrast to the more open Internet governance process norms, to which the governments that negotiate trade agreements also notionally subscribe, which if fully realized would be better adapted to incorporate the values of these communities, such as free expression and cultural facilitation, into trade policies."

Main Demands of the Brussels Declaration

- **Pro-active dissemination of information, including the regular release of draft proposals and consolidated texts**
- **Opportunities for meaningful involvement and collaboration with civil society representatives**
- **Apply freedom of information principles to the development and negotiation of government positions**
- **Require balanced representation on any trade advisory bodies or processes, including implementation bodies**

- **Take affirmative measures to engage organizations and experts representing Internet users and consumers**
- **Ensure the resulting agreements support realization of the targets of the UN 2030 Agenda for Sustainable Development**

Annex I:

Table compiling various issues included in current trade negotiations available here