hinrich foundation
advancing sustainable global trade

Digital Policy Alert

MARCH 2026

Why Digital Is Different: Making Digital Trade Policy for the 21st Century

BY TOMMASO GIARDINI AND VLADISLAV ALIFIROV

Contents

Contents

The full dataset for this report is available here.

Foreword: Why Digital is Different

One of the least profiled features of a new era of "America First" is its demand for digital trade commitments in bilateral tariff deals wrangled on US terms from trading partners.

In March 2026, as the US renewed global trade upheaval by deploying a barrage of powerful tariff weapons against dozens of countries, one of the most intriguing targets the White House set among its sights in a blizzard of Section 301 sorties is to regain US control over the global governance of digital trade.

The fog of trade war can veil its trophies. How the world governs digital trade is now a matter of utmost priority to incumbent and aspiring hegemons alike. The race to dominate global regulation of digital trade, decades in the making, is now at a suddenly brutal pivot. It highlights the way decisive power in shaping such trade rules shifted across the planet over the last quarter-century, why the US wants it back, and how policymakers need to understand that digital is different.

The US sets a premium so high on the governance of global digital trade commitments that it has continued to pursue digital trade negotiations even as it retreats from established multilateral systems it once led and championed. This is not a pretext to raise tariffs or extract tactical concessions. One of the least profiled features of a new era of "America First" is its demand for digital trade commitments in bilateral tariff deals wrangled on US terms from trading partners. Its aggressive unilateralism to regain dominance over global digital trade is yielding short-term gains. That said, it places its own staying power at risk over the longer term.

Simply put, the US is playing catch-up in a race it spent much of last decade sitting out. As US participation in global digital trade governance faded, the rest of the world amped up mutual digital trade commitments at a voracious pace. Riddled by regulatory fragmentation in some cases, honored only in the breach in others, country after country and region after region still kept driving a global boom in digital trade agreements. Increasingly, it became clear that for this boom to go on — and still work — hinges on transparency in rules and their implementation.

These developments set the backdrop to a joint initiative by Digital Policy Alert and the Hinrich Foundation to support policymakers as they grapple with how to navigate and engage the hard choices they now face and difficult decisions they must make in escalating global digital trade commitments. Digital Policy Alert's *Why Digital Is Different: Making Digital Trade Policy for the 21st Century*, supported by the Hinrich Foundation, is the most comprehensive casebook to date on global digital trade commitments. It is intended as a global commons to enhance transparency for rulemakers, drawing on state-of-the-art analysis on 25 years' worth of data to catalog digital trade rules strewn across the world, classify them by taxonomy, chart how they were made and evolved, and highlight what matters most in how or whether they are effectively harnessed in the decades ahead.

Our analysis covers the 2,587 extant digital trade commitments signed between 163 jurisdictions in 163 agreements thus far in the 21st century. *Why Digital Is Different* tracks their provenance and trajectory; how the rules morphed over

Even as it undertakes a long-awaited upgrade, the provisions in the CPTPP's electronic commerce chapter still substantively influence the formulation of similar commitments across other regions and continents.

geography and time; how each swiftly sprouting limb changed as different countries bound them into regulation.

The changes tell the story of a quiet but seismic migration in digital trade's geographic heartland. The US spearheaded digital trade policy throughout the early 2000s, establishing early commitments through free trade agreements (FTAs). But Washington, driven by changing political attitudes at home and rising geopolitical contest abroad, increasingly ceded its leadership just as other jurisdictions worldwide started engaging with gusto in digital trade negotiations.

The epitome of this shift was the US withdrawal from the Trans-Pacific Partnership in January 2017. So too was what the other 11 members of the short-lived pact cobbled back together in March 2018 as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). The CPTPP still serves today as a model for other digital trade negotiations. Even as it undertakes a long-awaited upgrade, the provisions in the CPTPP's electronic commerce chapter still substantively influence the formulation of similar commitments across other regions and continents. At a fundamental level, the CPTPP set a gold standard in showing how finding common ground on digital trade among a diverse group of countries was possible. It catalyzed digital trade negotiations swiftly taken up by others. Most governments today enter digital trade commitments through regional, rather than bilateral, frameworks.

In the eight years since the CPTPP launched, regional digital trade agreements became all the rage. Over half of all 2,587 extant digital trade commitments analyzed in our report were negotiated in the past four years.

Washington, driven by changing political attitudes at home and rising geopolitical contest abroad, increasingly ceded its leadership in digital trade policymaking.

The threat of fresh Section 301 investigations into other countries' digital policies has grown substantially after the Supreme Court in February 2026 overturned US tariffs imposed under the International Emergency Economic Powers Act.

Early commitments became increasingly binding over time as more jurisdictions included them. Commitments came to cover an ever-broader range of topics. The number of governments engaging in digital trade negotiations mushroomed. Topics that began in advanced economies' discussions now draw diverse continents and the world's poorest countries, epitomized by the African Continental Free Trade Area's Digital Trade Protocol with 54 participants and 208 provisions on the cusp of coming into force. The World Trade Organization (WTO) Electronic Commerce Agreement, if it ever comes into force, would provide even broader geographic coverage: 72 governments co-sponsor it at the time of writing.

The US is not currently one of the co-sponsors. It kept a seat at the negotiating table all the way from the initiative's inception in December 2017 until the eve of co-sponsors agreeing on the deal's "stabilized text" in July 2024. Along the way, it withdrew its support for key provisions on data flows and source code in the WTO context in 2023. Geopolitical friction with one of the agreement's co-sponsors, China, likely played a role.

But, in 2025, following a multi-year hiatus, the US returned to negotiate digital trade commitments in a novel and contentious way, through bilateral "tariff deals." The US now prefers a consistent pattern of wresting digital trade commitments on its terms from trading partners, focusing on the prohibition of digital services taxes, facilitation of data flows, a prohibition on customs duties on electronic transmissions, cooperation on cybersecurity, and the removal of market entry conditions such as source-code disclosure mandates. The aggressive US pushback especially in the past year against these and other forms of digital policy convergence in other major jurisdictions, particularly the European Union (EU), has been effective: at the international level, US-led "tariff deals" now defer to US terms on these digital trade commitments, sometimes complemented by additional demands. Even in domestic jurisdictions, Digital Policy Alert has observed a chilling effect, meaning countries are regulating their digital trade less and, if so, less bindingly, in areas where the US had applied policy pressure on them.

The US is poised to continue with this approach. Government statements on bilateral "tariff deals" that are not yet finalized include language on digital trade similar to finalized ones. Furthermore, the threat of fresh Section 301 investigations into other countries' digital policies has grown substantially after the Supreme Court in February 2026 overturned US tariffs imposed under the International Emergency Economic Powers Act. The US Trade Representative in March 2026 launched Section 301 investigations into excess capacity and forced labor. The USTR has decried a range of digital policies in other countries in its 2025 National Trade Estimates report. The first Trump administration concluded Section 301 investigations into various digital services taxes. We expect Section 301 and other potential weapons such as sectoral tariffs to become the next basis for US unilateralism, in which digital policy looks like a prize quarry.

The US still wants digital trade commitments, but does not want to negotiate them in multilateral rules-based venues. It prefers its transactional strategy that has brought considerable wins in the short term. Two examples of the US negotiating commitments on these issues are its trade deal with Indonesia last year that reversed Jakarta's longstanding claim to a right to impose customs

The crux for the future of global digital trade governance lies in weighing perceived short-term gains against a different, longer-term strategy to foster global digital trade growth.

duties on electronic transmissions and, separately, a commitment by Korea to the US to facilitate the cross-border transfer of location data. Some deals include consultation clauses and poison pills that allow the US to terminate agreements if counterparts conclude trade arrangements with third countries that the US does not deem suitable.

The crux for the future of global digital trade governance lies in weighing these perceived short-term gains against a different, longer-term strategy to foster global digital trade growth. Tackling specific policies that hinder digital trade today seems sensible. The regulatory fragmentation that besets the global digital economy is indisputable as a challenge. As governments worldwide continue to each regulate the digital economy differently, companies face an increasingly complex patchwork of compliance requirements. The complexity and cost render cross-border trade unsustainable especially for smaller businesses. As digital technologies, especially artificial intelligence (AI), become increasingly important for global prosperity, so does the burden of fragmentation.

But there are no short-term solutions: Governments need to identify commonalities and build bridges between regimes. By establishing regulatory interoperability, governments alleviate the challenges facing businesses and consumers increasingly dependent on digital trade. This is a burdensome process. It requires structured dialogues built on trust.

The burden hangs heavier on those that seek to lead. The current path risks eroding both the trust and the forum for mutually beneficial dialogue, further exacerbating the risk of digital fragmentation.

Two challenges stand out:

- The growing number of bilateral and plurilateral commitments cannot compensate for the absence of a multilateral solution, since commitments are valid only for parties to each agreement. So, while the number of commitments to free up data transfer flows may steadily grow, they ultimately cannot enable data to flow freely globally in the absence of a truly multilateral deal.

- Implementing digital trade commitments on the ground opens webs of complexity in domestic policies that governments are still learning to navigate, including knowledge and coordination gaps between negotiators and regulators. These challenges are not going away, but the pursuit of digital trade commitments must remain the priority.

As governments enter a new phase of global digital trade policy negotiations, whether in concert or under duress, Digital Policy Alert and the Hinrich Foundation's *Why Digital Is Different: Making Digital Trade Policy for the 21st Century* sets out a toolkit and a casebook that we hope will show the way to a better deal.

Tommaso Giardini is Associate Director at Digital Policy Alert.

Chuin Wei Yap is Director for International Trade Research at the Hinrich Foundation.

Executive summary

While the first digital trade commitments in FTAs date back to 2001, over half of all commitments were negotiated in the past four years.

Two shifts mark the importance of digital trade commitments in trade agreements[1]:

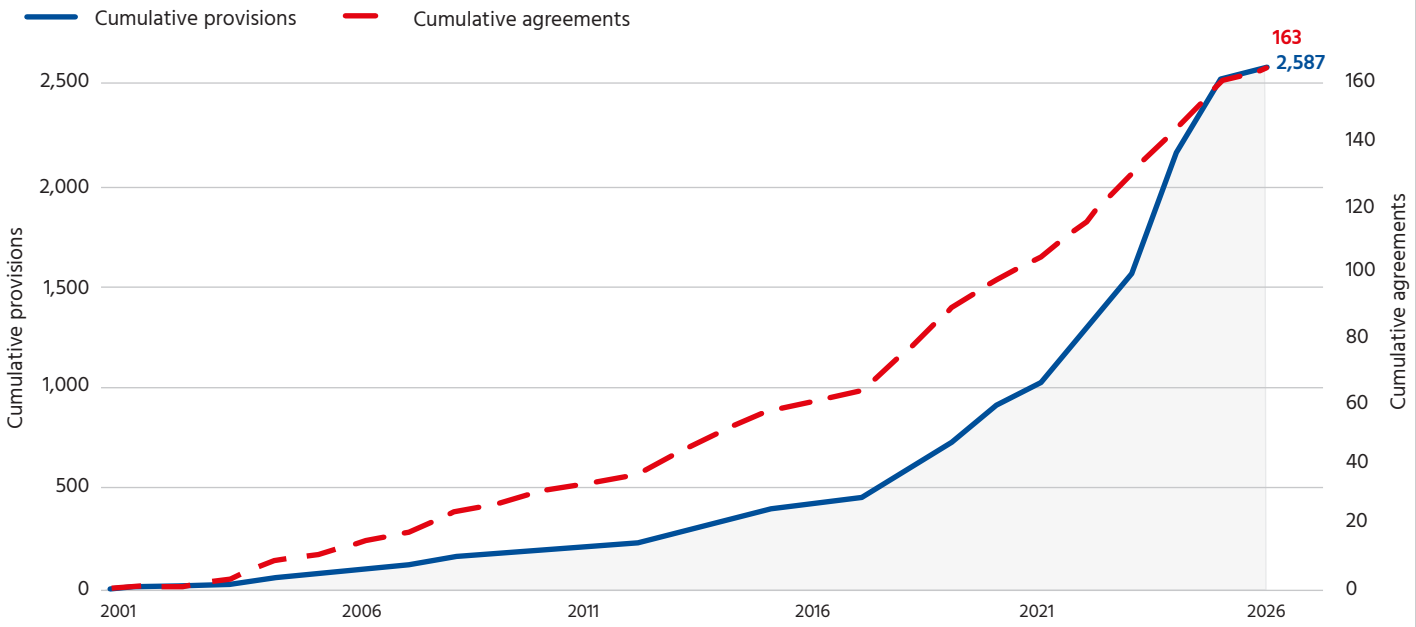
1. Digital trade is growing as an ever-larger share of global trade; and
2. Digital trade is shifting from a globalized basis to a greater emphasis on regionalism.

As the digital economy continues growing, governments are nurturing it through international alignment. Digital FTAs, first bilaterally and now increasingly agreed among groups of economies rather than multilaterally, provide fertile ground for such alignment, since they build on established, consensus-based negotiations, but allow governments to move faster than multilateral fora.

Digital trade commitments in FTAs are accordingly mushrooming: They currently comprise 2,587 provisions across 163 agreements between 163 jurisdictions. While the first commitments date back to 2001, over half of all commitments were negotiated in the past four years.

Figure 1 – The acceleration of digital trade

Cumulative provisions and agreements, 2001–2026



Source: Digital Policy Alert

As the importance of digital technology for economic growth and to every livelihood is poised to sharply rise, so is the importance of digital trade commitments.

The recent trend of digital trade commitments struck in regional, rather than bilateral, agreements has spurred this acceleration. These commitments are increasingly binding. As the importance of digital technology for economic growth and to every livelihood is poised to sharply rise, so is the importance of digital trade commitments.

Without appropriate transparency, however, the risks undermine the potential gains from digital trade. Insights into the crafting and nature of digital trade commitments remove unnecessary friction in negotiations between governments. But obtaining transparency on digital trade commitments is a daunting challenge. FTA texts are spread across a myriad of government websites, with differing versions stored in disparate documents, often in incoherent formats. Negotiations covering cutting-edge technology are stuck in technology from the past millennium.

This digital trade toolkit, a joint initiative by Digital Policy Alert and the Hinrich Foundation, provides the greatest level of transparency available on a global basis to fill this policy and evidence gap. Its aim is to enable more governments to pursue more ambitious digital trade commitments. To do so, it builds on, analyzes, and compares digital FTAs using a novel dataset[2], including the full text of all digital trade commitments worldwide, as well as the state-of-the-art Clairk artificial intelligence analytical resource built by Digital Policy Alert[3], an independent, public repository that tracks global policy changes affecting the digital economy.

We begin by presenting aggregate findings on the current state of digital trade commitments and their evolution over the past 25 years. We outline how rapidly digital trade commitments have changed and grown, which topics they cover, to which level of binding-ness, and where the center of gravity of digital trade negotiations now lies and the directions in which it is moving.

This sets the stage for the detailed analysis of six clusters of digital trade commitments in depth. This analysis covers the text of all existing provisions. First, we identify components that recur systematically across formulations of digital trade commitments worldwide. This provides policymakers with a systemic view of the approaches available to enter into commitments in each topic of digital trade, enabling them to distill similarities and differences between digital provisions in different FTAs. Second, we explain how commitments evolved over time and across regions, identifying geographical patterns that help negotiators identify areas of convergence with various trading partners and understanding ongoing shifts in counterparts' priorities and strategies. To ensure that these insights serve the development of the next generation of digital trade agreements, we reference recent developments at the domestic and international level to enrich our findings.

The full dataset for this report is available here.

A brief history of digital trade

The US spearheaded digital trade commitments in the early 2000s but ceded its leading position just as interest from other jurisdictions worldwide began to accelerate.

This report presents the first comprehensive inventory of digital trade commitments in FTAs. Drawing on 2,587 individual provisions across 163 agreements signed between 2001 and 2026, it offers a systematic, data-driven account of digital trade commitments and their evolution. This section provides a snapshot of the current state of digital trade, traces the evolution of digital trade over 25 years, and outlines the contents of this toolkit.

The state of digital trade

Digital trade is mushrooming. This novel area of trade has evolved from a handful of provisions on electronic commerce in a 2001 agreement into a widespread and common element of trade commitments. The acceleration of digital trade has been particularly strong since 2018: Over half of all digital trade commitments stem from the past four years.

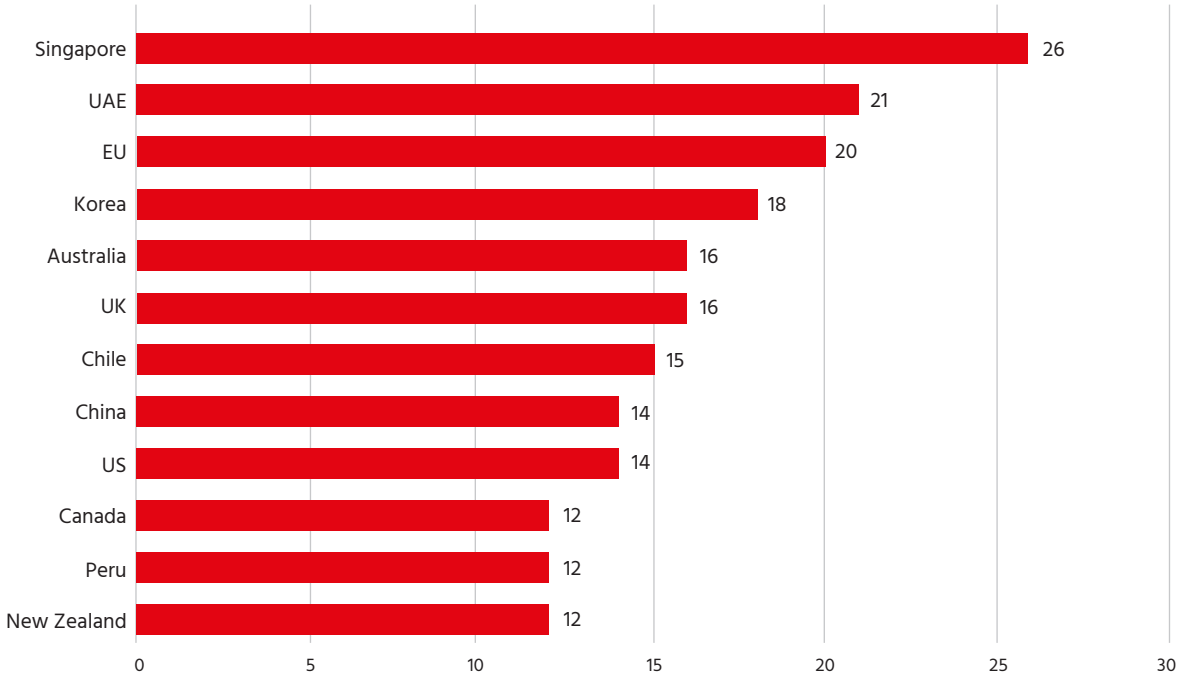
The geographic distribution of commitments reveals how digital trade has spread across continents and how its center of gravity has shifted. The US spearheaded digital trade commitments in the early 2000s but ceded its leading position just as interest from other jurisdictions worldwide began to accelerate. This shift was partly driven by the absence of the US as regional frameworks began to proliferate, starting from its withdrawal from the Trans-Pacific Partnership in 2017. Such regional frameworks are a core driver behind the recent acceleration of digital trade agreements worldwide: Most governments increasingly enter digital trade commitments through regional, rather than bilateral, frameworks.

In total, 163 jurisdictions have entered into digital trade commitments. On a regional basis, governments from Asia participate in the most agreements, followed by the Americas, Europe, and Africa. In terms of individual economies, Singapore participates in the most (26) agreements, in line with its dependence on trade as a small and open economy, as well as its focus on the digital economy. Notably, other governments that frequently participate in digital trade are either small and open economies, such as the United Arab Emirates (UAE) and Chile, or major economic powers. Specifically, they include the UAE (21 agreements), the EU (20), Korea (18), Australia (16), the UK (16), Chile (15), China (14), the US (14), Canada (12), Peru (12), and New Zealand (12).

Digital trade increasingly covers an ever-growing range of topics. Foundational topics, such as electronic transactions, have been subject to commitments for 25 years. More novel topics, such as AI, emerged around 2020. Foundational topics comprise a large share of commitments: The five most common topics — customs duties, cooperation, consumer protection, data protection, and electronic authentication and signatures — account for over 40% of all commitments. Novel topics accordingly appear less frequently, with the five newest topics accounting for only 3% of commitments to date.

Figure 2 – Principal negotiators

Agreements by jurisdiction



Source: Digital Policy Alert

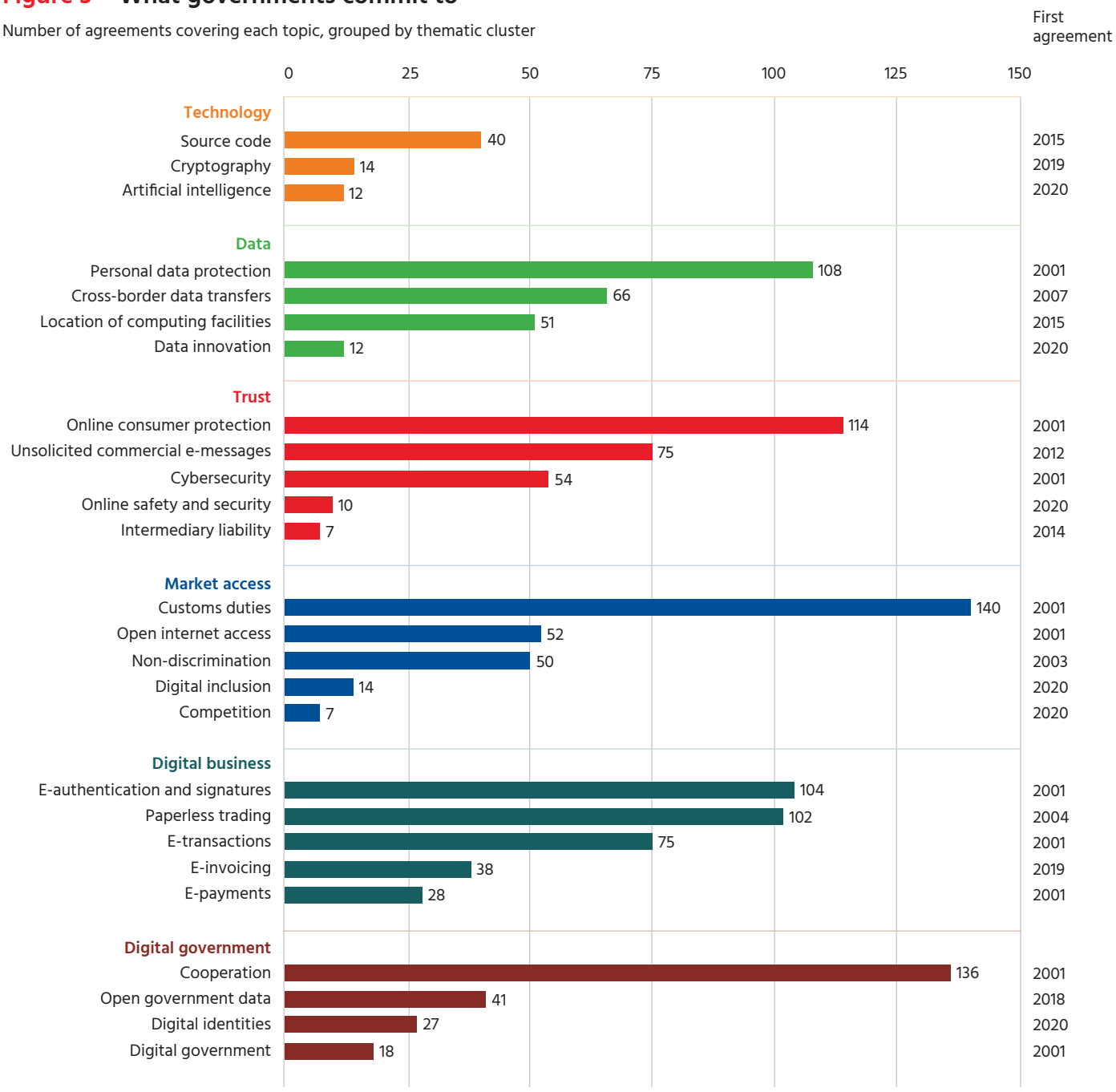
In terms of breadth, agreements now cover four times the number of provisions that early-stage agreements did.

Consider the following simplified[4] lifecycle of a digital trade topic. At the domestic level, political attention on a novel policy area or technology, such as online safety or AI rules, causes an increase in domestic rulemaking. As different governments begin to individually regulate the same policy area or technology, the risk of regulatory diversity and fragmentation creates demand for international alignment. This motivates the inclusion of the novel topic into trade negotiations. When a novel topic enters the trade landscape, it usually does so in non-binding language. As consensus builds and formulations converge, the language hardens towards binding obligations. The foundational digital trade topics have largely completed this lifecycle, while emerging topics, such as online safety, are still in the early stages.

This explains how digital trade commitments have simultaneously increased in breadth and in binding-ness. In terms of breadth, agreements now cover four times the number of provisions that early-stage agreements did. Novel topics are broadening the scope, in non-binding language, but making up only a small percentage of all commitments. Meanwhile, the continuous spread of binding commitments on foundational topics has caused the share of binding commitments, as opposed to non-binding ones, to rise sharply in the past years.

Figure 3 – What governments commit to

Number of agreements covering each topic, grouped by thematic cluster



Source: Digital Policy Alert

By 2010, digital trade commitments spanned North America, parts of Latin America and the Caribbean, much of East and Southeast Asia, Oceania, the EU, and the Middle East.

The evolution of digital trade

Digital trade commitments now cover over 20 different topics with ever-growing binding-ness. This coverage evolved in three phases over the past 25 years.

Early agreements were narrow and non-binding

From 2001 to 2010, coverage grew from two jurisdictions, Jordan and the US, to 74. The core drivers of this growth include bilateral FTAs negotiated by the US and Singapore with various partners, as well as the agreement between the EU and the Caribbean Forum (CARIFORUM) member states. By 2010, digital trade commitments spanned North America, parts of Latin America and the Caribbean, much of East and Southeast Asia, Oceania, the EU, and the Middle East.

Ten digital trade topics were present in the very first agreement, the Jordan-US Joint Statement on Electronic Commerce: Customs duties, electronic authentication and signatures, electronic transactions, consumer protection, data protection, cybersecurity, cooperation, internet access, electronic payments, and digital government. Throughout the 2000s, commitments on three novel topics began to emerge: Non-discrimination in 2003 (Singapore-US FTA and US-Chile FTA), paperless trading in 2004 (Australia-US FTA and Australia-Thailand FTA), and data transfers in 2007 (US-Korea FTA).

Across this period, a total of 31 agreements included 197 digital trade provisions. Among these provisions, recognition language featured prominently. 43 provisions used "recognize" formulations, for instance recognizing the economic growth and opportunities provided by electronic commerce, without establishing commitments. Twenty-eight provisions contained binding "shall" commitments, for example that each party shall maintain domestic legal frameworks governing electronic transactions. Finally, 16 provisions used "shall endeavor" language, representing a less binding commitment.[5]

Binding-ness increased as geographic and topical coverage stalled

Between 2011 and 2017, geographic coverage began to expand, growing by 18 jurisdictions to 92. The EU's association agreements with Eastern European countries expanded coverage, while Latin American intra-regional agreements wove a dense fabric of commitments across the region. Asian coverage deepened through novel agreements driven primarily by Australia and Korea.

Yet this phase brought only four new topics: Unsolicited commercial electronic messages in 2012 (Australia-Malaysia FTA), intermediary liability in 2014 (EU association agreements with Georgia and Moldova), as well as location of computing facilities and source code in 2015 (Japan-Mongolia Economic Partnership Agreement, or EPA).

Binding-ness, however, increased substantially. Thirty-one agreements produced 259 digital trade provisions. Among these agreements, 45 provisions used recognition language, while 68 used binding "shall" language and 22 used "shall endeavor." Two factors contributed to this shift towards binding-ness. First, for topics that were covered in non-binding language in the first phase of digital FTAs, formulations had hardened into binding commitments. Second, the three

Since 2018, the proliferation of regional agreements and dedicated digital economy agreements has broadened their coverage to 163 jurisdictions.

new topics were of such salience that hard language was used from the start. Domestic rules establishing intermediary liability, demanding data localization, and mandating source code disclosure risked hindering digital trade, prompting governments to directly establish binding commitments.

Geographic and topical coverage, and binding-ness, are mushrooming

Since 2018, the proliferation of regional agreements and dedicated digital economy agreements has broadened their coverage to 163 jurisdictions. Major agreements include the CPTPP (2018, 11 parties at the time of signing), the US-Mexico-Canada Agreement (USMCA, 2018, three parties), and the Regional Comprehensive Economic Partnership (RCEP, 2020, 15 parties), among others. Furthermore, the Digital Trade Protocol of the African Continental Free Trade Areas (AfCFTA), which was signed in 2024 but is yet to enter into force, would establish digital trade commitments among 54 African countries. Finally, the plurilateral Joint Statement Initiative on Electronic Commerce under the WTO has led to the release of a stabilized text for an Agreement on Electronic Commerce in July 2024. It is yet to enter in force but would expand geographic coverage substantially if it does, as 72 WTO member states currently co-sponsor the agreement. However, the likelihood of such entry of a plurilateral agreement into the WTO legal framework remains fraught with contention. In parallel, digital economy agreements such as the US-Japan Digital Trade Agreement (2019), the Digital Economy Partnership Agreement (DEPA, 2020), and the Australia-Singapore Digital Economy Agreement, or DEA (2020), provided unprecedented depth and ambition.

Nine new topics emerged in this phase: Open government data in 2018 (USMCA), electronic invoicing and cryptography in 2019 (New Zealand-Singapore Closer Economic Partnership, or CEP, Upgrade and US-Japan Digital Trade Agreement), as well as AI, competition, data innovation, digital identities, digital inclusion, and online safety in 2020 (Australia-Singapore DEA and/or DEPA).

In total, 101 agreements produced 2,148 digital trade provisions in this phase, with over half of all digital trade commitments stemming from the past four years. Among these agreements, provisions include 903 “shall” requirements, 580 “shall endeavor” formulations, and 720 “recognize” formulations. The share of binding commitments, as opposed to mere recognitions, thus rose sharply in the last phase. Notably, these agreements combine binding commitments on well-established topics, such as source code and customs duties, with non-binding commitments on novel topics. These topics include digital inclusion (ensuring all individuals have access to and the skills to participate in the digital economy) and digital identities (digital mechanisms for identifying natural or juridical persons). Furthermore, various agreements follow standards set by the CPTPP, combining binding and non-binding language. To date, the AfCFTA contains the most (208) digital trade provisions.

Of the total 2,587 provisions, digital trade commitments span 26 distinct topics, such as data protection, grouped into six thematic clusters: technology, data, trust, market access, digital business, and digital government.

How to read this report

Of the total 2,587 provisions, we identified digital trade commitments on 26 distinct topics, such as data protection, grouped into six thematic clusters.

A. **Technology** commitments include provisions on AI, source code protection, and cryptography. These provisions address the governance of the technologies that underpin digital trade, from AI cooperation to prohibiting forced source code disclosure.

B. **Data** commitments comprise provisions on personal data protection, cross-border data transfers, location of computing facilities, and data innovation. These provisions include commitments to adopt legal frameworks for personal data protection and obligations to allow cross-border data transfers, balancing consumer trust and ease of business.

C. **Trust** commitments encompass provisions on online consumer protection, unsolicited commercial electronic messages, online safety and security, intermediary liability, and cybersecurity. These provisions set ground rules for the protection of individuals, creating the basis of trust on which digital trade can flourish.

D. **Market access** commitments include provisions on non-discrimination, customs duties, competition, open internet access, and digital inclusion. These provisions regulate the market entry barriers facing companies engaged in digital trade.

E. **Digital business** commitments include electronic transactions, paperless trading, electronic authentication and electronic signatures, electronic invoicing, and electronic payments. These provisions establish the legal infrastructure for digital trade, ensuring that electronic contracts are legally valid, that electronic signatures are not denied legal effect, and that trade administration documents can be submitted electronically.

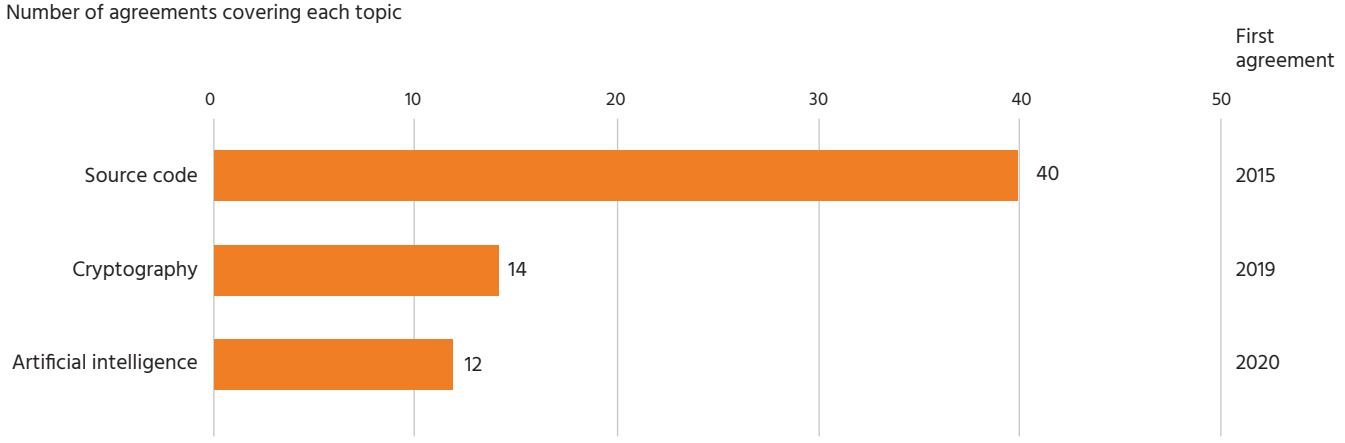
F. **Digital government** commitments include cooperation, open government data, digital government, and digital identities. These provisions commit governments to make data publicly available, promote digital inclusion for marginalized groups, and digitally transform government services, to accelerate their countries' digital trade.

Each section first presents the relevant topics and the level of detail of our analysis. Then, for each topic, we analyze the text of all provisions to identify recurring components. We explain how commitments evolved across time and regions, identifying geographic patterns. Where possible, we reference recent domestic and international developments.

Section A: Technologies

Figure 4 – Technology commitments

Number of agreements covering each topic



Source: Digital Policy Alert

Commitments on AI in digital trade comprise 12 dedicated AI provisions within 12 agreements between 29 jurisdictions that focus on cooperation.

Digital trade commitments on technologies and components thereof cover AI, source code, and cryptography. Given the ever-growing importance of AI in the global economy and geopolitical rivalry, we analyze commitments on AI in greater depth. For source code commitments, we also cover recent commitments made by various countries with the US in bilateral "tariff deals."

Artificial intelligence

Commitments on AI in digital trade comprise 12 dedicated AI provisions[6] within 12 agreements between 29 jurisdictions that focus on cooperation. The provisions consistently recognize the importance of AI, its governance, and international alignment thereon. All provisions cover collaboration on developing governance frameworks guided by international principles, albeit in non-binding or recognition language. Seven provisions additionally cover cooperation, on information sharing, the promotion of responsible AI use, and cooperation between research and industry, in both binding and non-binding language.

Components

AI provisions contain four components:

1. a recognition of AI's importance and benefits;
2. a commitment to cooperate on AI;
3. a recognition of the need for AI governance frameworks; and
4. a commitment to collaborate on developing such AI governance frameworks.

The Australia-Singapore DEA, signed in August 2020, established the most comprehensive and binding approach to date, incorporating all four components and formulating both the first commitment between the governments to cooperate on AI in "shall cooperate" language and the second commitment to collaborate on AI governance in "shall endeavor" language.

Provisions open with a first recognition that AI is becoming increasingly important to digital trade. Some further recognize the significant social and economic benefits to persons and enterprises, as well as the reality that parties may take different legal approaches to use and develop AI.

The first commitment concerns cooperation. In accordance with their respective laws and policies, parties are to cooperate by sharing research and industry practices related to AI; promoting and sustaining the responsible, safe, or ethical use and adoption of AI by businesses and communities; and encouraging commercialization and collaboration between research and industry.

The second recognition concerns the importance of developing ethical governance and regulatory frameworks for the trusted, safe, and responsible use of AI. Emphasizing the cross-border nature of digital trade or the digital economy, provisions acknowledge the benefits of ensuring that governance frameworks are internationally aligned as far as possible or practicable.

The second commitment relates to collaboration on such AI governance frameworks. Parties commit to collaborate on and promote the development and adoption of AI governance frameworks in relevant regional and international fora. In doing so, parties commit to take into consideration internationally recognized principles or guidelines. Specific principles are sometimes explicitly referenced, such as explainability, transparency, fairness, and human-centered values. Similarly, existing governance frameworks, namely the Organisation for Economic Co-operation and Development (OECD) AI Principles and the Global Partnership on AI are sometimes mentioned. Furthermore, some provisions commit to promote dialogue and experience-sharing on regulations, policies, and initiatives relating to AI.

Evolution

AI provisions first emerged in 2020, with two similar approaches that diverged on the commitment to cooperate.

- The Australia-Singapore DEA, signed in August 2020, established the most comprehensive and binding approach to date. It incorporated all four components, formulating the first commitment between the governments to cooperate on AI in "shall cooperate" language and the second commitment, to collaborate on AI governance in "shall endeavor" language.

- The DEPA, signed in June 2020 between Chile, New Zealand, and Singapore, established a narrower AI provision. It included both recognitions but only the commitment to collaborate on AI governance is in "shall endeavor" language. There is no commitment on cooperation and thus no binding commitment in this approach, only endeavors. The DEPA was since updated by a Protocol and expanded to include Korea, but the AI provision was not changed.

In 2022, the year in which AI reached a broad consumer base through the launch of ChatGPT, Singapore adopted new AI provisions in two agreements, separately with Korea and the United Kingdom. The UK-Singapore DEA, signed in February 2022, followed the Australia-Singapore DEA but formulated the commitment to

In 2025, as US-driven instability troubled the global trading system, two novel provisions combined standard components with new language.

cooperate on a "shall endeavor" level of binding-ness. Notably, this provision also covered other emerging technologies beyond AI. The Korea-Singapore Digital Partnership Agreement, signed in November 2022, followed the approach of the DEPA.

In 2023, three AI provisions emerged, all including the UAE as a party. Its Comprehensive Economic Partnership Agreements (CEPAs) with Türkiye, signed in March 2023, and Georgia, signed October 2023, followed the approach of the UK-Singapore DEA. They included all components, with both commitments formulated in "shall endeavor" language. The Gulf Cooperation Council (GCC)-Korea FTA, signed in December 2023 but yet to enter into force, used the DEPA formulation.

The three AI provisions established in 2024 all also included the UAE as a party. Two provisions, namely the Korea-UAE CEPA, signed in May 2024 and yet to enter into force, and the Chile-UAE CEPA, signed in July 2024, included the DEPA formulation. The Australia-UAE CEPA, signed in November 2024, resurfaced the approach of the 2020 Australia-Singapore DEA: It incorporated all four components and formulated the commitment to cooperate in "shall" language. This demonstrated Australia's consistent position as well as the UAE's preparedness to enter ambitious commitments with willing partners.

In 2025, as US-driven instability troubled the global trading system, two novel provisions combined standard components with new language. The European Free Trade Association (EFTA)-Singapore DEA, signed in September 2025 but yet to enter into force, included all four components, albeit with reduced binding-ness. It formulated the first commitment as "may cooperate" and only recognized the importance of collaboration on governance, without establishing any commitment. The Association of Southeast Asian Nations and China's ASEAN-China FTA 3.0 Upgrade Protocol, signed in October 2025 but yet to enter into force, also incorporated all four components with distinctive formulations. The first commitment used "shall cooperate" but reduced the specific cooperation activities to "encouraging," while the second commitment used "shall endeavor" language. These novel approaches are thus less binding than earlier models.

Geographic patterns

The commitments reveal the following patterns:

- AI provisions are geographically spread, with commitments spanning across the Asia-Pacific, Europe, the Middle East, and South America. The upgraded ASEAN-China FTA covers the most countries while DEPA provides the broadest geographical spread.

- Singapore has entered into several AI commitments, showing its leadership in this emerging topic of digital trade. Australia has consistently incorporated all components with binding language, signaling its ambition. The UAE's six commitments were negotiated between 2023 and 2024, demonstrating the Gulf state's desire to be at the Middle East's forefront in the digital era, but vary in binding-ness, showcasing the UAE's flexibility.

The second Trump administration rescinded a Biden-era Executive Order on AI and issued an AI Action Plan focused on accelerating AI innovation, building American AI infrastructure, and leading in international AI diplomacy and security.

– Beyond these provisions, three Memorandums of Understanding on AI cooperation, signed in 2022 and 2024, specified the commitments between Australia, Korea, and Singapore.

Notably, as AI becomes a battleground for geopolitical rivalry, the EU and the US have not entered into any AI commitments in trade agreements. Domestically, the two governments pursue widely different regulatory approaches The EU adopted the comprehensive AI Act in 2024 and is currently working on its implementation. The second Trump administration rescinded a Biden-era Executive Order on AI and issued an AI Action Plan focused on accelerating AI innovation, building American AI infrastructure, and leading in international AI diplomacy and security.

Recent developments

In 2025, AI was included in a new form of contentious trade negotiation: Several "tariff deals" between the US and its trading partners include language on AI. Specifically, the Technology Prosperity Deals with Japan, Korea, and the UK contain sections on accelerating AI adoption and innovation. The language focuses on the advancement of pro-innovation AI policy frameworks. Furthermore, Japan's Strategic Trade and Investment Deal includes a commitment to invest US$550 billion, on projects to be selected by the US President, including in the AI and semiconductor sectors. Korea's Strategic Trade and Investment Deal is still being finalized, although a recent joint statement contains similar language.

The implementation of these deals is still unclear. In December 2025, reports emerged that the Technology Prosperity Deal with the UK was on hold, including due to disagreements on digital rules, although the UK delayed planned rules for AI. In the past year, US officials have strongly opposed what they call "excessive regulation" of AI and the "European model of fear and overregulation" of AI.

Notably, as AI becomes a battleground for geopolitical rivalry, the EU and the US have not entered into any AI commitments in trade agreements.

A total of 40 source code provisions are found in 36 agreements between 108 jurisdictions, spanning 2015 and 2025, prohibiting parties from requiring the transfer of or access to source code of software as a condition for import, distribution, sale, or use of software or products containing software.

Meanwhile, regulatory activity on AI continues mushrooming: Digital Policy Alert tracked over 1,600 domestic policy and enforcement developments targeting AI providers since January 2020, with a significant increase since the launch of ChatGPT in 2022. This includes AI-specific rules, such as Korea's recently implemented AI Basic Act and Vietnam's recently implemented Law on AI, as well as the enforcement of existing rules to AI providers. In early 2026, authorities worldwide, including in Brazil, Indonesia, the EU, Malaysia, and the US, investigated sexualized deepfakes generated by Grok and disseminated on X. Furthermore, India adopted rules on synthetic content, while China drafted measures to regulate human-like interactive AI services.

Source code

A total of 40 source code provisions are found in 36 agreements between 108 jurisdictions, spanning 2015 and 2025. They prohibit parties from requiring the transfer of or access to source code of software as a condition for import, distribution, sale, or use of software or products containing software. They differ in terms of the scope of the prohibition, for instance regarding the coverage of algorithms and non-mass-market software, as well as exceptions which retain states' right to demand source code disclosure during investigations and conformity assessments.

Components

Source code provisions contain three core components:

1. the prohibition of source code disclosure mandates,
2. scope parameters outlining the reach of this prohibition, and
3. exception mechanisms retaining room for source code disclosure in specific scenarios.

Provisions prohibit parties from requiring the transfer of or access to source code as a mandatory condition for market access. Thirty-four provisions formulate the prohibition as "shall not" or "may not" require language. The prohibition typically covers the import, distribution, sale, or use of software or products containing such software within a party's territory. Thirty provisions specify that the prohibition does not apply to voluntary transfers of source code, made on a commercial basis, under open-source licenses, or in the context of government procurement.

The scope parameters determine whether the prohibition extends only to mass-market software or products and whether it covers algorithms expressed in source code. Eight provisions limit the prohibition to mass-market software or products, explicitly excluding software used for critical infrastructure. Twelve provisions address critical infrastructure separately from the mass-market limitation, allowing access to source code: nine do so by incorporating general or security exceptions that permit measures to ensure security and safety; two contain a direct footnote carve-out permitting access necessary for the effective functioning of critical infrastructure; and one excludes critical infrastructure from the prohibition's scope entirely. Ten provisions expand the prohibition to also cover algorithms expressed in source code.

The USMCA, signed in 2018, established a second approach that is now prevalent in 12 provisions, including algorithms, removing the mass-market limitation to establish a broad prohibition, and introducing targeted exceptions for regulatory and judicial investigations.

The exception mechanisms preserve room for source code disclosure, subject to safeguards against unauthorized disclosure. Nine provisions incorporate general and security exceptions, permitting measures inconsistent with the prohibition where justified under those exceptions. Other provisions define exceptions explicitly:

- 24 provisions permit regulatory bodies, judicial authorities, or law enforcement to require preservation and availability of source code for specific investigations, inspections, examinations, enforcement actions, or judicial proceedings.
- 15 provisions allow access for conformity assessment bodies, meaning governmental or delegated non-governmental bodies verifying compliance with applicable laws, distinguishing them from regulatory or judicial authorities.
- 11 provisions explicitly preserve competition authority access to source code, either for remedying competition law violations or to address barriers to entry in digital markets.
- 13 provisions address intellectual property rights: 11 carve out IP rights and their protection from the scope of the prohibition, while two safeguard the IP status of source code that has been disclosed to authorities.
- Nine provisions clarify that the prohibition does not affect patent applications and disputes.

Evolution

The Japan-Mongolia Economic Partnership Agreement, signed in 2015, established the first source code provision. It limited the prohibition to mass-market software or products, explicitly excluding critical infrastructure and establishing predefined exceptions, such as for patents. The approach was subsequently adopted in the CPTPP and five further agreements until 2022.

The USMCA, signed in 2018, established a second approach that is now prevalent in 12 provisions. It included algorithms, removed the mass-market limitation to establish a broad prohibition, and introduced targeted exceptions for regulatory and judicial investigations. The UK adopted this approach in post-Brexit agreements with Japan (2020), Australia (2021), Singapore (2022), Ukraine (2023), and India (2025, yet to enter into force). The AfCFTA Digital Trade Protocol (2024, yet to enter into force) also followed this approach, adding an Annex on criteria for determining the legitimate and legal public interest reasons for disclosure of source code.

The EU developed its own approach through years of negotiations, including with the UK (2020), New Zealand (2023), and Chile (2023), consolidating its approach in 2025 in agreements with Singapore, Korea, and Indonesia. The agreements with Korea and Indonesia are yet to enter into force. Specifically, the EU expands the prohibition to exports, does not include a mass-market limitation, and provides general and security exceptions. For these exceptions, it specifies legitimate public policy objectives such as cybersecurity and protection against disinformation.

In October 2023, the US withdrew its support for source code commitments under the WTO's Joint Statement Initiative on Electronic Commerce.

Furthermore, it provides carve-outs regarding source code access for competition authorities and conformity assessment bodies. Possible explanations are longstanding tensions between competition policy and trade policy, dating back to the exclusion of competition policy from the WTO Doha Development Round in July 2004, and the relevance of conformity assessment bodies for the oversight of AI under the EU AI Act (see Recent Developments below).

Finally, China has not established source code commitments but mentioned it in three provisions. It will start discussions on source code provisions with ASEAN and consider including source code in future dialogues under RCEP. Furthermore, if both China and Peru enter into other source code commitments in other agreements, they undertake to initiate discussions from those venues. The agreements with ASEAN and Peru are yet to enter into force. China has formally applied to join the CPTPP, which includes a source code provision, in September 2021.

Recent developments

In recent months, source code commitments were included in "tariff deals" between the US and Argentina, Bangladesh, Cambodia, Taiwan, El Salvador, Guatemala, Indonesia, and Malaysia. The commitments, embedded in "Market Entry Conditions" articles, prohibit these governments from requiring the transfer or provision of access to particular technology, production process, source code, or other proprietary knowledge as a condition for doing business. This unilateral prohibition is followed by exceptions for authorities in all deals, with some also excluding critical infrastructure and government procurement.

Notably, in October 2023, the US withdrew its support for source code commitments under the WTO's Joint Statement Initiative on Electronic Commerce. Possible explanations include the US' reluctance to enter into multilateral agreements that include China, and US demands for WTO reform generally. Notwithstanding, after a multi-year hiatus, the US is again pursuing source code commitments, but in bilateral agreements rather than under the WTO framework.

Domestically, source code disclosure requirements are rare. The EU's AI Act, for instance, includes source code access requirements for providers of "high risk AI" (used in safety-critical products or critical areas such as law enforcement and education) and "general purpose AI" (designed to perform a wide range of tasks without need for additional retraining). High risk AI providers must grant source code access to market surveillance authorities if it is necessary to assess conformity with the law and other auditing procedures and verifications are exhausted. Regarding general purpose AI, the newly established AI Office can request access to source code when conducting evaluations to assess compliance and investigate systemic risk.

Cryptography provisions follow a common approach, containing three components: the scope of application, the prohibition, and the exception mechanisms.

Cryptography

Cryptography is a novel element of digital trade, with 14 provisions in 14 agreements between 15 jurisdictions, spanning 2019 and 2025. The provisions prohibit parties from requiring manufacturers or suppliers of commercial information and communication technology (ICT) products using cryptography to transfer or provide access to proprietary cryptographic information, to partner with domestic entities, or to use particular cryptographic algorithms as conditions for market access. All provisions provide exceptions, including for law enforcement access to encrypted communications, financial regulation, government networks and government procurement, and sometimes regulatory and judicial investigations, subject to safeguards.

Components

Cryptography provisions follow a common approach, containing three[7] components: the scope of application, the prohibition, and the exception mechanisms.

Provisions establish the scope of application by stating that "This Article shall apply to information and communication technology (ICT) products that use cryptography." This is consistently accompanied by a clarification that products are goods and do not include financial instruments. Newer provisions further include digital products or services.

Provisions then establish a binding commitment for parties not to require manufacturers or suppliers of commercial cryptographic products, as a condition of manufacture, sale, distribution, import, or use, to:

- transfer or provide access to proprietary cryptographic information, including private keys, secret parameters, algorithm specifications, or design details;
- partner with or cooperate with a person in the party's territory; or
- use or integrate a particular cryptographic algorithm or cipher.

Exception mechanisms clarify that the prohibition shall not apply to:

- requirements relating to access to government-owned or controlled networks, including central banks;
- measures pursuant to supervisory, investigatory, or examination authority relating to financial institutions, financial markets, or financial service suppliers;
- requirements by regulatory bodies or judicial authorities for information needed for investigations, inspections, examinations, enforcement actions, or judicial proceedings, subject to safeguards against unauthorized disclosure; and/or
- competition law remedies following enforcement proceedings.

With two exceptions, provisions conclude with a clarification that the commitment shall not be construed to prevent law enforcement authorities from requiring service suppliers using encryption they control to provide access to unencrypted communications, in accordance with legal procedures. Some provisions extend this to include encrypted communications as well.

Many major economies and economic blocs, including the African Union, China, the EU, India, and Russia, have not entered into any cryptography commitments, reflecting both the novelty and contentiousness of the subject, which lies at the center of geopolitical security concerns.

Evolution

The US-Japan Digital Trade Agreement, signed in 2019, established the first cryptography provision, which served as template for subsequent provisions. It included detailed definitions of cryptographic terms, limited the scope to application to ICT goods designed for commercial applications, established the three core prohibitions, and provided extensive exceptions for law enforcement, financial regulation, government networks and procurement, and financial instruments.

The UK adopted this approach in five post-Brexit agreements with Japan (2020), Australia (2021), New Zealand (2022), Singapore (2022), and Ukraine (2023), adding regulatory and judicial exception provisions permitting preservation and availability of cryptographic information for investigations subject to safeguards and for competition law remedies.

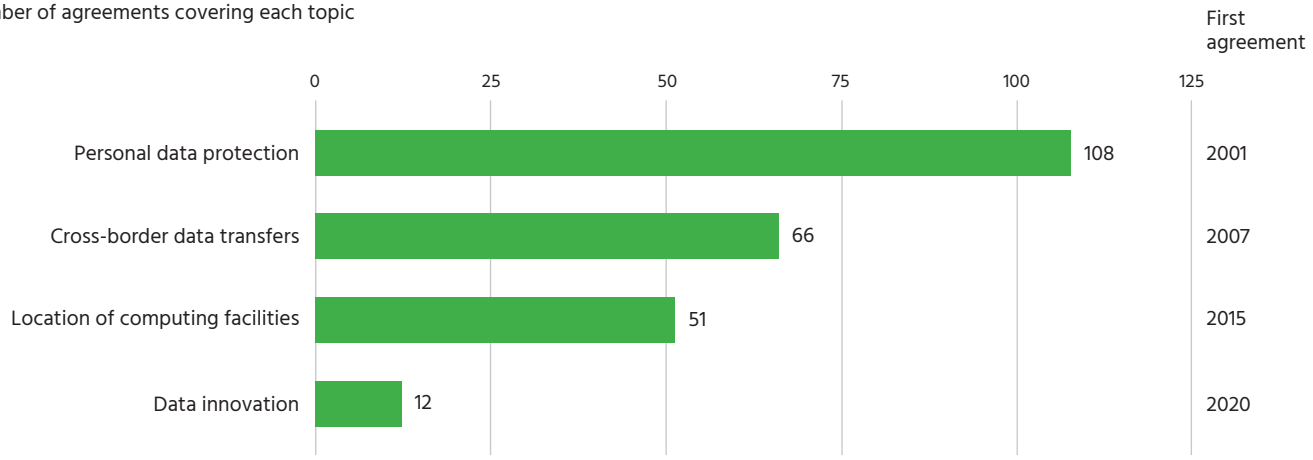
Singapore also participates in five agreements with cryptography provisions, namely with Australia (2020), Korea (2022), the UK (2022), EFTA (2025, yet to enter into force), as well as DEPA (signed in 2020 and updated in 2024). More recently, the UAE started entering into cryptography commitments, in CEPAs with Australia (2024), Chile (2024), and New Zealand (2025). Finally, the Chile-Paraguay FTA (2021) is the only Spanish-language cryptography commitment, although it follows the same structure as the other provisions.

Cryptography commitments are thus still relatively limited in their geographic reach. They span 15 jurisdictions from the Asia-Pacific to the Americas, Europe, and the Middle East. Many major economies and economic blocs, including the African Union, China, the EU, India, and Russia have not entered into any cryptography commitments. This reflects both the novelty and contentiousness of the subject, which lies at the center of geopolitical security concerns.

Section B: Data

Figure 5 – Data commitments

Number of agreements covering each topic



Source: Digital Policy Alert

Cross-border data transfer provisions are a staple of digital trade agreements, with 71 provisions across 66 agreements among 136 jurisdictions, spanning 2007 and 2025.

Digital trade commitments on data comprise provisions on personal data protection, cross-border data transfers, location of computing facilities, and data innovation. In light of the importance of data flows for the global digital economy, commitments on cross-border data transfers and the location of computing facilities are key aspects in the analysis of this report.

Cross-border data transfers

Cross-border data transfer provisions are a staple of digital trade agreements, with 71 provisions across 66 agreements among 136 jurisdictions, spanning 2007 and 2025. The provisions prohibit or restrict parties from impeding the transfer of information, including personal information, by electronic means when conducted for business purposes. While early provisions used non-binding "shall endeavor" language, contemporary provisions predominantly employ binding formulations. Binding provisions, however, include exceptions permitting measures to achieve legitimate public policy objectives, subject to a necessity test and disciplines against arbitrary discrimination.

Components

Data transfer provisions contain three core components:

1. a recognition of regulatory sovereignty;
2. an obligation to permit data transfers; and
3. exceptions for legitimate public policy objectives.

Forty cross-border data transfer provisions begin with a recognition of the importance of data flows and the fact that parties may have their own regulatory requirements concerning the transfer of information by electronic means.

Forty provisions begin with a recognition of the importance of data flows and the fact that parties may have their own regulatory requirements concerning the transfer of information by electronic means. This recognition acknowledges regulatory sovereignty before proceeding to the obligation to permit data transfers.

Provisions then formulate a commitment to refrain from prohibiting or restricting the cross-border transfer of information, including personal information, by electronic means. This commitment applies when data is transferred for business purposes. Fifty-two provisions formulate this commitment in binding "shall" language. Thirteen provisions use non-binding "shall endeavor" language, and one provision uses permissive "may allow" language. The remaining provisions do not contain any specific commitments.

Notably, 11 provisions do not establish a general obligation but rather specify restrictive measures that violate the commitment, including:

- requiring the localization of data in a party's territory for storage or processing;
- prohibiting the transfer to or storage or processing of data in the territory of another party;
- requiring a party's approval prior to data transfers to the territory of another party;
- requiring the use of computing facilities or network elements in a party's territory for data processing, including requiring the use of approved facilities (see the chapter on Location of Computing Facilities below); or
- making cross-border data transfers contingent upon use of computing facilities or network elements in the party's territory or upon localization requirements (see the chapter on "Location of Computing Facilities" below).

Fifty provisions include exceptions permitting parties to adopt or maintain measures inconsistent with the core obligation to achieve legitimate public policy objectives. Often, these exceptions require measures to be necessary to achieve the objective, while others allow each party to adopt measures "it considers necessary." Forty-eight provisions incorporate chapeau disciplines, meaning introductory clauses that set the conditions under which the agreement's members can apply policy exceptions to otherwise inconsistent trade measures. Such chapeau disciplines act as a safeguard against the abuse of these exceptions. Those 48 provisions incorporated chapeau disciplines adapted from the General Agreement on Tariffs and Trade's (GATT) Article XX, requiring that measures not be applied in a manner constituting arbitrary or unjustifiable discrimination or a disguised restriction on trade. Twenty-three provisions add a proportionality test requiring that measures not impose restrictions greater than necessary or required to achieve the objective. Less common exceptions refer to measures necessary for the protection of essential security interests or personal data (if transfers are enabled under "conditions of general application"), as well as exclusions for financial services, information processed by or on behalf of governments, and procurement.

The Chile-Uruguay FTA introduced the approach that dominates to date, requiring parties to allow cross-border transfer of information by electronic means for business purposes, subject to exceptions for legitimate public policy objectives, with necessity tests and chapeau disciplines.

Evolution

Cross-border data transfer provisions first emerged in 2007, in the US-Korea FTA. It recognized the importance of free information flows and the importance of protecting personal information, using non-binding language to commit parties to "endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."

From 2014 to 2017, three binding provisions emerged between Latin American parties, specifically the Mexico-Panama FTA (2014), the Chile-Uruguay FTA (2016), and the Argentina-Chile FTA (2017). The Chile-Uruguay FTA introduced the approach that dominates to date, requiring parties to allow cross-border transfer of information by electronic means for business purposes, subject to exceptions for legitimate public policy objectives, with necessity tests and chapeau disciplines.

In 2018, the CPTPP formulated this approach in English, serving as a template for a range of future provisions. The USMCA reformulated the same commitment as a prohibition ("shall not prohibit or restrict") and omitted the recognition of regulatory requirements. It further specified that measures which accord different treatment to data transfers solely on the basis that they are cross-border, in a manner that modifies competition conditions, do not meet the conditions of the provision. The USMCA's distinctively binding and detailed formulation was subsequently included in the US-Japan Digital Trade Agreement.

Most agreements widely followed the CPTPP model, including various UK post-Brexit agreements and 19 agreements including the UAE since 2022. The RCEP also used the CPTPP formulation, with transition periods for some members.

The EU, however, established a novel approach: Rather than imposing a general obligation to permit transfers, as in the CPTPP/USMCA model, it established a list of specific restrictive measures deemed prohibited (see Components above). This approach emerged in the EU-UK Trade and Cooperation Agreement (TCA) in 2020 and has since been adopted in EU agreements with New Zealand (2023), Chile (2023), Japan (2024), Singapore (2025), Korea (2025), and Indonesia (2025). The agreements with Korea and Indonesia are yet to enter into force. While a 2022 draft of the EU-India FTA also contained this formulation, the provision was not included in the text released by the EU after the recent conclusion of negotiations.

The AfCFTA Digital Trade Protocol, adopted in February 2024 but yet to enter into force, included a provision on data transfers using the CPTPP model and additionally established an entire Annex on cross-border data transfers. The Annex addresses principles for data transfers, requirements for equivalent levels of protection, data transfer mechanisms, and legitimate public policy objectives.

Geographic patterns

Data transfer provisions are global, covering jurisdictions from the Asia-Pacific, the Americas, Europe, the Middle East, and Africa. The UAE participates in the most provisions, all of which were negotiated between 2022 and 2025. Other active governments include Singapore, Chile, and Australia. The AfCFTA represents the agreement with the most expansive jurisdictional coverage, incorporating 54 African jurisdictions.

The stabilized text of the WTO Agreement on Electronic Commerce, which is not yet in force and currently features China and the EU member states as co-sponsors, no longer includes a provision on data transfers, likely due to differences between participants during the negotiation process.

All major economic blocs have entered into data transfer commitments. The US and the EU established their own templates, while China followed the CPTPP template in its commitments towards ASEAN and Peru (both of which are yet to enter into force), as well as in the RCEP. Data transfers remain, however, a highly divisive topic of digital trade: In October 2023, the US withdrew its support for data transfer commitments under the WTO's Joint Statement Initiative on Electronic Commerce. The stabilized text of the WTO Agreement on Electronic Commerce, which is not yet in force and currently features China and the EU member states as co-sponsors, no longer includes a provision on data transfers, likely due to differences between participants during the negotiation process.

Recent developments

Domestic data transfer restrictions continue to emerge: Digital Policy Alert has documented 460 policy and enforcement developments affecting data transfers since January 2020. In 2025, this regulatory activity slowed, as geopolitical tensions rose and the US pushed back on foreign data transfer restrictions. Binding developments, such as laws and regulations, and enforcement developments decreased more than non-binding guidance. One interpretation is that pressure from the US government during bilateral "tariff deal" negotiations acted as a signal worldwide, prompting both counterparts and other governments to restrict data transfers less, and less bindingly.

On the international level, the "tariff deals" in 2026 between the US and Argentina, Bangladesh, Cambodia, Taiwan, El Salvador, Guatemala, Indonesia, and Malaysia contained commitments on data flows.

- Bangladesh, Cambodia, Taiwan, Guatemala, El Salvador, Indonesia, and Malaysia commit to ensuring the free transfer of data across trusted borders for the conduct of business. In their respective Annexes of specific commitments, Bangladesh and El Salvador additionally commit to recognizing the Global Cross-Border Privacy Rules (CBPR) System and Global Privacy Recognition for Processors (PRP) System certifications as valid data transfer mechanisms.

- Argentina commits to providing "certainty regarding the ability to move personal data out of its territory to the US including by recognizing the US as a country or jurisdiction that provides adequate data protection under Argentina's law." Guatemala and Indonesia make a similarly worded guarantee as part of their specific commitments.

These commitments are unilateral and do not apply to the US itself, which recently started restricting transfers of "bulk sensitive personal data and government-related data" to six "countries of concern," including China and Russia. In February 2026, the US Federal Trade Commission sent letters to 13 data brokers to ensure compliance with new data transfer restrictions.

Computing facilities provisions are a common element of digital trade agreements, comprising 55 provisions across 51 agreements between 120 jurisdictions negotiated between 2015 and 2025.

Location of computing facilities

Computing facilities provisions are a common element of digital trade agreements, comprising 55 provisions across 51 agreements between 120 jurisdictions negotiated between 2015 and 2025. The provisions recognize parties' ability to regulate computing facilities, including for security purposes. The core obligation prohibits parties from requiring covered persons to use or locate computing facilities in their territory as a condition for conducting business. Most prohibitions are binding and include exceptions permitting measures to achieve legitimate public policy objectives, subject to necessity tests and chapeau disciplines. Only seven provisions do not include exceptions. Seventeen provisions address financial services separately, establishing conditional prohibitions subject to regulatory access requirements.

Components

Provisions on the location of computing facilities[8] contain three core components:

1. a recognition of parties' regulatory requirements concerning computing facilities;
2. a prohibition of requirements to use of local computing facilities in a business context; and
3. exception mechanisms allowing for such requirements in certain circumstances.

Thirty-two provisions start with a recognition that parties may have their own regulatory requirements regarding the use of computing facilities. These provisions recognize requirements that seek to ensure the security and confidentiality of communications, establishing that the prohibition on computing facilities requirements does not prevent parties from maintaining security and confidentiality requirements that do not mandate localization.

The prohibition typically obliges parties not to require the use or locate computing facilities in their territory as a condition for conducting business in that territory. In 42 provisions, this commitment is drafted in binding language, while single agreements use "endeavor" and "recognition" language, respectively. An alternative approach used in 11 provisions is the enumeration of concrete measures that parties shall not adopt or maintain, in provisions that also cover cross-border data transfers (see chapter above). Such enumerations prohibit two measures related to computing facilities: 1) requiring the use of computing facilities or network elements in the party's territory for processing, including requiring the use of facilities certified or approved in the party's territory, and 2) making cross-border data transfers contingent upon the use of computing facilities or localization requirements in the party's territory.

Forty-one provisions include exceptions permitting parties to adopt or maintain measures inconsistent with the prohibition to achieve legitimate public policy objectives. The exception structure varies in stringency: 24 provisions employ the full three-part structure, requiring that the measure be necessary to achieve the objective and not be applied in a manner constituting arbitrary or unjustifiable discrimination or a disguised restriction on trade, while the remaining 17 include only the chapeau discipline without a necessity test. Some provisions enumerate specific policy objectives that may justify exceptions, including public security, public morals, protection of life or health, and maintenance of public order. This

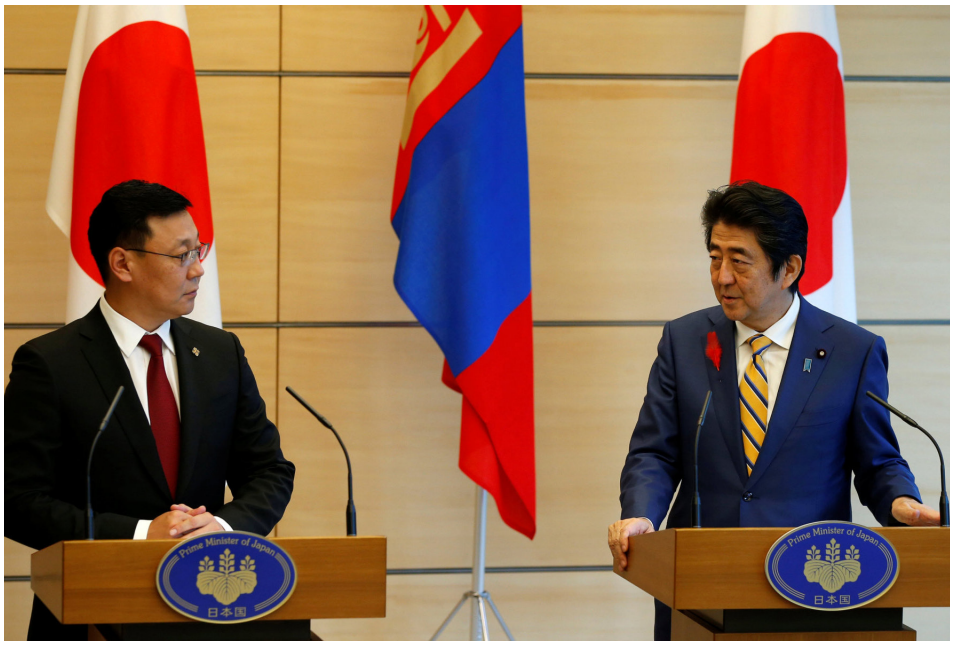
The 2015 Japan-Mongolia Economic Partnership Agreement included the first provision on location of computing facilities, establishing the basic template, including the core prohibition and an exception mechanism for measures necessary to achieve legitimate public policy objectives.

exception structure mirrors that employed in cross-border data transfer provisions. Notably, in contrast to data transfer provisions, some provisions on the location of computing facilities do not include exception mechanisms. This showcases that, despite the commonalities between these two provisions, governments are willing to enter into more binding commitments on the location of computing facilities.

Evolution over time

The 2015 Japan-Mongolia Economic Partnership Agreement included the first provision on location of computing facilities. It established the basic template, including the core prohibition and an exception mechanism for measures necessary to achieve legitimate public policy objectives. The Chile-Uruguay FTA (2016) followed the same approach, adding the recognition of regulatory requirements concerning computing facilities, including requirements to ensure security and confidentiality of communications. The Argentina-Chile FTA (2017) established a commitment to exchange best practices and regulatory frameworks rather than a binding prohibition.

In 2018, the CPTPP established what is by now the most commonly used approach, incorporating a recognition and a binding prohibition, albeit with exceptions for measures necessary to achieve legitimate public policy objectives (see the Components section above). In the same year, the Singapore-Sri Lanka FTA and Peru-Australia FTA used the same formulation, while the USMCA established the strongest commitment to date, containing the core prohibition without exception mechanisms.



The 2015 Japan-Mongolia Economic Partnership Agreement included the first provision on location of computing facilities.

Regarding the major economic blocs, the US has established the strictest commitments, allowing no exceptions, in two agreements covering Canada, Mexico, and Japan, reflecting a longstanding US aversion to foreign requirements on the location of computing facilities, which it considers a substantial barrier to digital trade.

Since then, over 40 agreements have followed the CPTPP model, with three notable exceptions.

- The EU-UK TCA (2020) established the approach of enumerating measures that parties shall not adopt or maintain, including measures related to the location of computing facilities, as opposed to a broad prohibition. This approach has since been adopted in EU and EFTA provisions, establishing a distinct European model.
- The AfCFTA's Digital Trade Protocol, which is yet to enter into force, also adopted the CPTPP template, but additionally stated that parties shall encourage and support the establishment and use of local computing facilities, to promote the development of local digital infrastructure and access. This reflects the focus of the AfCFTA on development matters.
- The US-Japan Digital Trade Agreement (2019) used the strict USMCA formulation and addressed financial services in a separate article (see footnote above). While no other agreement has used such strict language, 18 provisions in other agreements address the location of computing facilities for financial services.

Geographic patterns

Provisions on the location of computing facilities span the Asia-Pacific, the Americas, Europe, the Middle East, and Africa. Singapore, Chile, Australia, and the UK participate in the most provisions. In contrast to its extensive commitments on data transfers, the UAE participates in only four provisions. The AfCFTA provides the broadest geographical range, covering 54 African jurisdictions.

Regarding the major economic blocs, the US has established the strictest commitments, allowing no exceptions, in two agreements covering Canada, Mexico, and Japan. This reflects a longstanding US aversion to foreign requirements on the location of computing facilities, which it considers a substantial barrier to digital trade. The EU has also established a unique approach, which it has adopted in agreements with the UK, New Zealand, Chile, Japan, Singapore, Korea, and Indonesia. The agreements with Korea and Indonesia are yet to enter into force. While a 2022 draft of the EU-India FTA also contained this formulation, the provision was not included in the text released by the EU after the recent conclusion of negotiations. China participates in three agreements with provisions on the location of computing facilities: RCEP, the ASEAN-China FTA 3.0, and the China-Peru Optimization Protocol (although the latter two are yet to enter into force). Despite these commitments, China maintains a series of domestic data localization requirements. Whether China complies with its commitments in digital trade agreements is a subject of debate, signaling the challenge of how broadly exception mechanisms may be interpreted.

The proliferation of data protection provisions and their reference to compatibility signal a growing realization among governments of both the importance of personal data regulation and the necessity of finding bridges between different regulatory regimes to combat fragmentation.

Personal data protection

Personal data protection is a core component of digital trade agreements, with 127 provisions across 108 agreements between 141 jurisdictions, spanning 2001 to 2026. The provisions establish obligations for parties to adopt or maintain legal frameworks protecting the personal data of electronic commerce users. Most provisions adopt binding "shall adopt" language, while some provisions use "shall endeavor" or "may" language. Early provisions used "should" language and some simply recognized the importance of data protection. The most common formulation combines this binding obligation with references to international standards, publication requirements, and encouragement of compatibility mechanisms. The proliferation of data protection provisions and their reference to compatibility signal a growing realization among governments of both the importance of personal data regulation and the necessity of finding bridges between different regulatory regimes to combat fragmentation.

Components

Data protection provisions contain four core components:

1. recognition of the importance of protecting personal data;
2. commitment to adopt or maintain a legal framework for personal data protection;
3. obligations regarding the publication of information; and
4. references to international standards and compatibility.

Seventy-four provisions open with a recognition that protecting personal data enhances consumer confidence in digital trade. Some provisions further recognize the economic and social benefits of protection. Seven provisions, predominantly from EU agreements, explicitly recognize personal data protection and privacy as fundamental rights. Thirteen provisions further affirm that nothing in the agreement prevents parties from adopting or maintaining measures on personal data protection, including with respect to cross-border data transfers.

The core commitment requires parties to adopt or maintain legal frameworks providing for personal data protection. Seventy-nine provisions formulate this obligation using binding "shall adopt or maintain" language, while 15 provisions use "shall endeavor," three provisions use "should adopt", and five provisions use "may adopt." Most provisions clarify that parties may comply through comprehensive privacy laws, sector-specific laws, or laws enforcing voluntary undertakings by enterprises.

Additional obligations concern the publication of information on data protection. Forty-five provisions require parties to publish information on protections provided to users, typically demanding the publication of guidance on how individuals can pursue remedies and how businesses can comply with legal requirements. Forty-four provisions require mechanisms for individuals to seek remedies or recourse for personal data protection violations.

Finally, data protection provisions contain references to international standards and compatibility. Seventy-four provisions direct that parties should take into account the principles and guidelines of relevant international bodies when developing data protection frameworks, such as the Asia-Pacific Economic

Personal data protection provisions first emerged in 2001 through the Jordan-US Joint Statement on Electronic Commerce, which recognized the importance of privacy protection frameworks whilst maintaining free information flows, without establishing a commitment.

Cooperation (APEC) Privacy Framework and OECD recommendations. Twenty-seven provisions include commitments regarding compatibility between different personal data protection regimes, encouraging the development of compatibility mechanisms such as the recognition of regulatory outcomes. Governments' desire to align at the international level, through international standards and compatibility mechanisms, reflects the importance of finding bridges between regulatory regimes to enable companies to operate across borders.

Evolution

Personal data protection provisions first emerged in 2001 through the Jordan-US Joint Statement on Electronic Commerce, which recognized the importance of privacy protection frameworks whilst maintaining free information flows, without establishing a commitment.

From 2003 to 2009, agreements started including commitments of three different kinds. The Australia-Singapore FTA (2003), Australia-Thailand FTA (2004), and New Zealand-Thailand agreement (2005) stated that parties "shall take" measures they consider appropriate and necessary for personal data protection. Canada's agreements with Peru (2008) and Colombia (2008) used "should adopt" language. The Australia-Chile FTA (2008) introduced binding "shall adopt or maintain" language, paired with requirements to take international standards into account, establishing the predominant template. Fifteen provisions, with both binding and non-binding language, emerged between 2010 and 2017.

In 2018, the CPTPP incorporated a provision that combined the recognition of benefits, the binding "shall adopt or maintain" obligation, the obligations regarding the publication of information; and non-binding commitments on the taking into account of international standards and compatibility. The provision established transition periods for Brunei and Vietnam, acknowledging different levels of data protection development.

The CPTPP has since influenced a broad range of agreements, albeit with some variations reflecting the state of regulation and international alignment of their parties. The USMCA, for instance, adopted a similar approach but included references to specific international instruments, including APEC and OECD frameworks. The RCEP used "shall take into account" language for international standards and provided a grace period, delaying the application for Cambodia, Laos, and Myanmar for five years. Despite these variations, the CPTPP's legacy persists to date.

Data protection provisions continue to grow, with four notable developments to date:

1. The UAE signed multiple comprehensive economic partnerships incorporating personal data protection provisions with trading partners across the globe.

2. The EU developed a distinctive approach centered on privacy as a fundamental right. The EU-Canada Comprehensive Economic and Trade Agreement (CETA) already highlighted parties' sovereignty in adopting data protection measures. Subsequent agreements expanded this language, elaborating on legitimate public policy objectives and standards of data protection.

The WTO Agreement on Electronic Commerce (2024), if it comes into force, would replace the AfCFTA Digital Trade Protocol as the geographically broadest provision.

3. The AfCFTA Digital Trade Protocol, which is yet to enter into force, established the most detailed and prescriptive approach to date. The data protection provision included a non-binding "shall endeavor" commitment to establish national data protection authorities and build their capacities, while the Annex on cross-border data flows included a section on principles and standards for data protection.

4. The WTO Agreement on Electronic Commerce, though not yet in force, aims to establish a comprehensive multilateral template incorporating all components with detailed specifications. It further includes a separate sovereignty preservation article affirming parties' rights to adopt data protection measures, including for cross-border transfers.

Geographic patterns

Data protection provisions are among the most geographically widespread digital trade commitments. Coverage spans all major trading regions: Asia-Pacific, Europe, the Americas, the Middle East, and Africa. The WTO Agreement on Electronic Commerce (2024), if it comes into force, would replace the AfCFTA Digital Trade Protocol as the geographically broadest provision. The most active jurisdictions are the UAE, Singapore, Australia, and Chile.

Data protection provisions have grown in parallel to domestic regulatory activity: Digital Policy Alert has tracked over 4,500 data governance policy and enforcement developments since January 2020. The jurisdictions with the most domestic data governance developments are the US, the EU, the UK, and Korea.

This domestic regulatory activity interacts with international data protection provisions in FTAs in two ways. On the one hand, data protection provisions primarily require governments to adopt or maintain data protection frameworks, suggesting that implementation is well underway. On the other hand, growing domestic regulatory activity creates demand for international alignment, as governments need to find common ground when regulating the same issue across borders.

Data innovation

Data innovation provisions represent an emerging element of digital trade agreements, with 13 provisions across 12 agreements between 70 jurisdictions, from 2020 to 2025. The provisions recognize that digitalization and data use promote economic growth and establish non-binding commitments to support data innovation through collaboration on data-sharing, cooperation on data mobility policies and standards, facilitation of knowledge exchange, and support for regulatory sandboxes. The trajectory and proliferation of provisions on this subject shows how digital trade agreements are and are perceived as a vector for policymakers to "future-proof" their economies.

Most recently, the Australia-UAE CEPA (2024) and the India-UK CETA (2025, yet to enter into force) incorporated data innovation provisions following the standard approach set by the Australia-Singapore DEA.

Components

Data innovation provisions contain a recognition of its importance and a non-binding cooperation commitment.

- All provisions recognize that digitalization and data use in digital trade or digital economy promote economic growth, and that creating enabling environments for experimentation and innovation supports data-driven innovation. With two exceptions, provisions further recognize that cross-border data flows and data sharing enable data-driven innovation, and that innovation may be enhanced within regulatory data sandboxes.

- All provisions further use "shall endeavor" language on efforts to support data innovation through specified activities, including 1) collaborating on data-sharing projects involving researchers, academics, and industry; 2) cooperating on development of policies and standards for data mobility including consumer data portability; 3) facilitating exchange of knowledge and best practices; and 4) developing data-sharing frameworks protecting personal data.

Evolution

Data innovation first emerged in 2020 in the DEPA and the Australia-Singapore DEA. The Australia-Singapore DEA established the template combining the recognition and non-binding commitment to collaboration, cooperation, and knowledge exchange. Subsequently, this approach was embedded into the Australia-UK FTA (2021), the Singapore-UK DEA (2022), the Korea-Singapore DPA (2022), the China-Ecuador FTA (2023), and the Ukraine-UK DEA (2023). The DEPA focused the recognition on cross-border data sharing and further recognized the value of data sharing to promote innovation and creativity, facilitate the diffusion of information, and foster competition. This language was adopted only in the Chile-Paraguay FTA (2021).

In 2024, the AfCFTA Digital Trade Protocol complemented a data innovation provision, following the standard template, with a dedicated provision on data for development. The latter established commitments to facilitate innovative ways to promote public benefits by sharing or using data to harness Africa's data for socioeconomic value in public sector decision-making, planning, monitoring, and evaluation; to support data capabilities to leverage data-reliant technologies for sustainable development; and to leverage data-driven business models fostering intra-African digital trade. It is yet to enter into force.

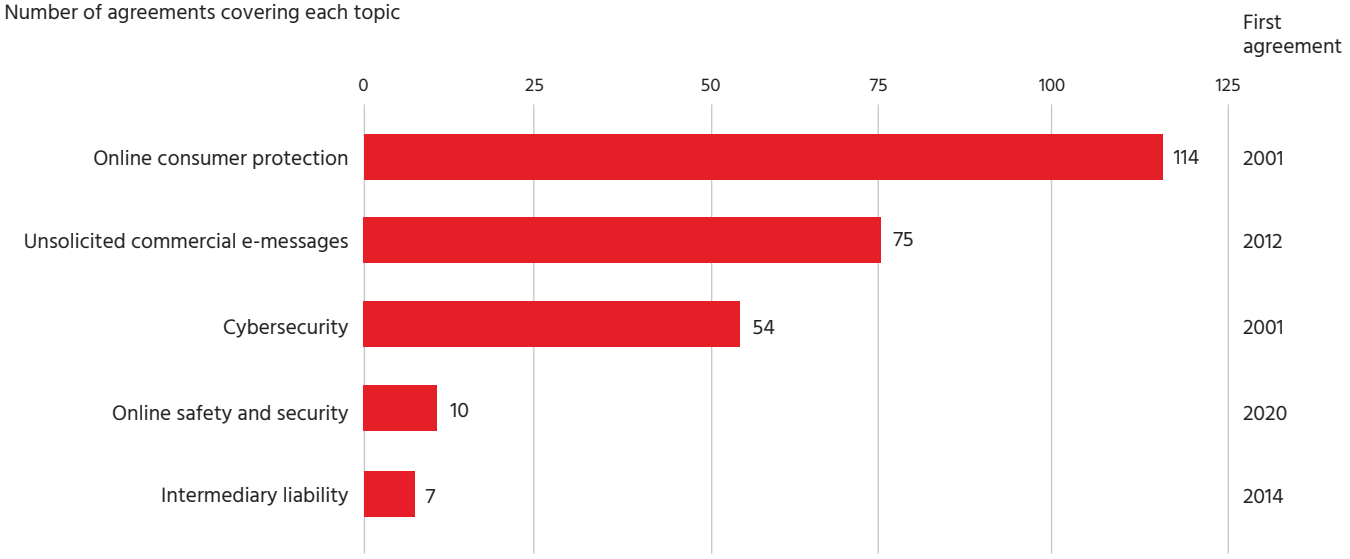
Most recently, the Australia-UAE CEPA (2024) and the India-UK CETA (2025, yet to enter into force) incorporated data innovation provisions following the standard approach set by the Australia-Singapore DEA. The EFTA-Singapore agreement (2025, yet to enter into force) included a distinct provision centered on distributed ledger technology and asset tokenization.

In total, the provisions cover 70 jurisdictions from the Asia-Pacific to the Americas, Europe, the Middle East, and Africa. Singapore participates in the most provisions, while the AfCFTA contains the geographically broadest commitment, covering 54 jurisdictions.

Section C: Consumer trust

Figure 6 – Trust commitments

Number of agreements covering each topic



Source: Digital Policy Alert

Online consumer protection provisions are one of the most widely and longest-established digital trade commitments, a reminder of the provenance of the concerns that drove the rise of international digital trade agreements.

Digital trade commitments on consumer trust include provisions on online consumer protection, unsolicited commercial electronic messages, online safety and security, intermediary liability, and cybersecurity. In view of the salience of consumer protection in digital trade agreements and domestic policy, we analyze these commitments in particular depth.

Online consumer protection

Online consumer protection provisions are one of the most widely and longest-established digital trade commitments, a reminder of the provenance of the concerns that drove the rise of international digital trade agreements. These now comprise 141 provisions across 114 agreements between 146 jurisdictions, spanning 2001 to 2026. The provisions recognize the importance of consumer protection since the advent of electronic commerce and require parties to adopt or maintain consumer protection laws applicable to electronic commerce and to cooperate on consumer protection matters.

Many online consumer protection provisions cover cooperation, committing consumer protection agencies to cooperate on matters of mutual concern, share information, and exchange best practices.

Components

Consumer protection provisions contain four core components:
1. a recognition of the importance of consumer protection;
2. a requirement to adopt or maintain consumer protection laws or measures;
3. a commitment to address prohibited commercial practices; and
4. provisions on cooperation and enforcement.

Provisions open with a recognition of the importance of consumer protection in digital trade. Basic formulations recognize "the importance of maintaining and adopting transparent and effective measures to protect consumers from fraudulent and deceptive commercial practices." More elaborate formulations encompass additional elements such as "measures conducive to the development of consumer confidence," measures that "enhance consumer trust," or references to "consumer welfare."

Recognitions are followed by the core commitment to adopt or maintain consumer protection laws or measures, typically including language that electronic commerce consumers should be protected equally to other consumers. In terms of binding-ness, 75 provisions use "shall adopt or maintain" language, while 12 provisions use "shall endeavor" language. Twenty-seven provisions merely "recognize" the importance of such measures without establishing a commitment. Regarding the scope and specificity, three variations are visible. The simplest formulation requires parties to adopt or maintain consumer protection laws "to proscribe fraudulent and deceptive commercial activities that cause harm" to consumers. The middle approach specifies what constitutes prohibited conduct in relatively concise language, requiring measures that "proscribe misleading, deceptive, and fraudulent commercial activities," with some provisions adding "unfair commercial practices" or "unconscionable conduct." The most detailed formulation specifies the measures "to ensure the effective protection of consumers" engaging in electronic commerce transactions, including transparency, information and withdrawal rights, and non-discrimination.

When provisions detail prohibited behavior, they target deceptive, fraudulent, and misleading commercial activities. Many provisions include explicit examples of what constitutes such activities, including making misrepresentations or false claims; failing to deliver products or provide services after consumers are charged; charging or debiting consumers' accounts without authorization; and advertising goods or services without intention or capability to supply.

Finally, many provisions cover cooperation, committing consumer protection agencies to cooperate on matters of mutual concern, share information, and exchange best practices. Some specify cooperation modalities such as notifications and consultations.

Evolution

Consumer protection provisions are among the oldest of digital trade commitments. The US was an early adopter: The US-Jordan Joint Statement on Electronic Commerce (2001) included a reference to consumer protection, followed by those in US FTAs with Australia (2004), Oman (2006), Peru (2006), and Korea (2007). The Australia-Singapore FTA (2003) included the first binding

Consumer protection provisions now cover 146 jurisdictions, including the US, the EU, China, and virtually all major economies participating in at least one consumer protection provision.

commitment. Consumer protection provisions subsequently spread across the Americas, with Canada, Chile, and Colombia being particularly active negotiators, as well as Asian governments as e-commerce took off in these regions.

In 2018, the CPTPP and USMCA consolidated a template requiring the adoption or maintenance of consumer protection laws covering online commercial activities and cooperation between enforcement agencies. This template was widely replicated across Asia-Pacific and the Americas' agreements, including the Brazil-Chile FTA (2018).

In 2020, the EU developed a more prescriptive approach in the EU-UK TCA. It introduced language on "consumer trust online," covering deceptive and misleading practices and the effective enforcement of consumer protection measures. This approach was followed in EU agreements with New Zealand (2023), Chile (2023), Singapore (2025), Korea (2025, yet to enter into force), Indonesia (2025, yet to enter into force), and Mercosur (2026, yet to enter into force).

From 2022 on, the UAE negotiated a series of consumer protection provisions, often formulating the commitment to adopt or maintain measures in non-binding "shall endeavor" language. This reflects the UAE's eagerness to enter into commitments as well as its flexibility in adapting to counterparts which prefer "endeavor" language.

In 2024, two regional agreements introduced detailed provisions on consumer protection:

- The Central European Free Trade Agreement (CEFTA) Decision on Facilitation of Electronic Commerce incorporated the most detailed consumer protection framework, with various provisions covering information requirements, withdrawal rights, delivery, digital content conformity, and trader liability.

- The AfCFTA Digital Trade Protocol, which is yet to enter into force, introduced multiple consumer protection provisions covering deceptive practices and online consumer protection.

Geographic patterns

Consumer protection provisions now cover 146 jurisdictions, including the US, the EU, China, and virtually all major economies participating in at least one consumer protection provision. The most active jurisdictions are the UAE, Singapore, Australia, and Chile. The seven CEFTA jurisdictions have negotiated over 20 provisions, all as part of the detailed CEFTA Decision on Facilitation of Electronic Commerce.

This level of international activity is matched by domestic regulation: Consumer protection is one of the most actively regulated policy areas on the Digital Policy Alert database, totaling over 1,500 policy and enforcement developments since January 2020. These developments mainly concern fair marketing and advertising requirements (530), quality of service requirements (286), age verification requirements (280), and user rights (268). Domestic regulators are increasingly developing and enforcing frameworks to protect electronic commerce users, as established by the core commitment of consumer protection provisions in digital trade agreements.

Provisions on unsolicited commercial electronic messages (spam) represent another rapidly emerging element of digital trade agreements, totaling 76 provisions across 75 agreements between 140 jurisdictions from 2012 to 2026.

Unsolicited commercial electronic messages

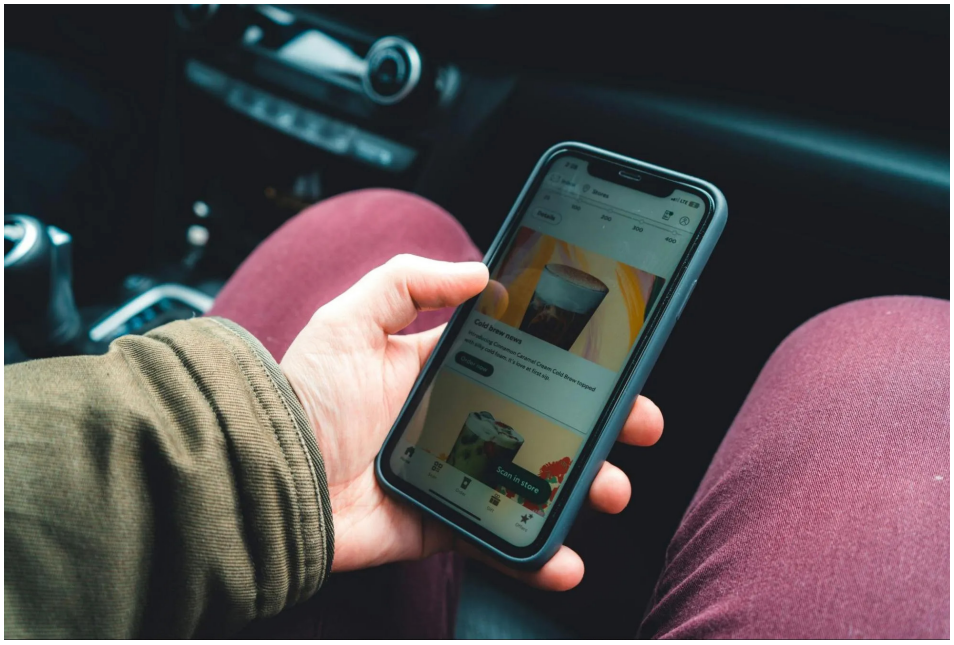
Provisions on unsolicited commercial electronic messages (spam) represent another rapidly emerging element of digital trade agreements, totaling 76 provisions across 75 agreements between 140 jurisdictions from 2012 to 2026. The provisions require parties to adopt or maintain measures regarding unsolicited commercial electronic messages, typically offering a choice between opt-out mechanisms, opt-in consent requirements, or minimization approaches. While early provisions used "shall endeavor" language focusing on minimization and cooperation, current provisions predominantly establish binding "shall adopt or maintain" obligations with mandatory recourse mechanisms. Most provisions incorporate cooperation commitments between parties on regulation of unsolicited messages.

Components

Spam provisions contain four core components:

1. requirement to adopt or maintain measures addressing spam;
2. specifications of such measures, including opt-out, opt-in, and minimization mechanisms;
3. details on recourse mechanisms; and
4. mechanisms for cooperation.

The core requirement obliges parties to adopt or maintain measures regarding spam. The high degree of international consensus on this issue is clear. Fifty-one provisions use binding "shall adopt or maintain" language, while nine use "shall endeavor" language. The requirement formulates measures "regarding" spam, rather than measures to prohibit or eliminate spam, to acknowledge that parties may adopt different regulatory approaches. Furthermore, 22 provisions demand



Provisions on unsolicited commercial electronic messages (spam) represent another rapidly emerging element of digital trade agreements.

The Australia-Malaysia FTA, signed in 2012, included the earliest spam provision, formulating both the core requirement and the cooperation in binding language, though with relatively little detail.

transparency, in both binding and non-binding language, namely that spam be clearly identifiable as such, disclose on whose behalf it is sent, and contain information enabling recipients to request cessation.

Most provisions then specify three alternative approaches for parties' measures regarding spam:

- opt-out mechanisms, requiring spam supplies to facilitate the ability of recipients to prevent or stop ongoing reception of spam.
- opt-in requirements, requiring either that messages be sent with the consent of the recipient or that senders indicate how consent was obtained.
- minimization mechanisms, demanding parties to otherwise provide for the minimization of spam.

To ensure that suppliers of spam comply with adopted measures, provisions then often require parties to provide affected users with recourse, redress, or remedies. This requirement applies to non-compliance with whichever alternative approach the party has adopted. Finally, most provisions commit parties to cooperate on addressing spam. Formulated either in binding "shall cooperate" or in "shall endeavor" language, these clauses specify mechanisms for relevant authorities to cooperate, including mutual consultation and information sharing. International organizations, including the International Telecommunication Union (ITU) and the OECD, provide fora and resources for such cooperation combating spam.

Evolution

The Australia-Malaysia FTA, signed in 2012, included the earliest spam provision, formulating both the core requirement and the cooperation in binding language, though with relatively little detail. The Australia-Korea FTA (2014) and the Japan-Mongolia EPA (2015) followed, both using "shall endeavor" language. Subsequently, the Chile-Uruguay FTA (2016) and the Argentina-Chile FTA (2017) adopted the brief and binding approach, both in Spanish.

In 2018, the CPTPP established the English-language template that is predominantly followed to date, including all the above-mentioned components: It included a binding core requirement, specified the opt-out, opt-in, and minimization mechanisms, and formulated the cooperation commitment in non-binding "shall endeavor" language. In the same year, the Peru-Australia FTA used the same formulation, while the USMCA went one step further, additionally specifying requirements for email spam, which must include either opt-out facilitation or opt-in consent requirements.

From 2019 to 2025, provisions proliferated rapidly across the globe, including a range of EU and UAE provisions. The EU uniquely required consent (opt-in), instead of proposing it as an alternative to opt-out and minimization, and formulated spam as "unsolicited direct marketing communications," with legal roots closer to data protection. The UAE adopted several provisions, including some binding and various non-binding "shall endeavor" formulations to address spam.

Online safety and security provisions are an emerging element of digital trade agreements, with only 10 provisions across six agreements between 61 jurisdictions, from 2020 to 2024.

Geographic patterns

Spam provisions now cover 140 jurisdictions across the globe, one of the broadest coverages in digital trade. The most active jurisdictions include the UAE, Singapore, Australia, and Chile. The geographically broadest provision is incorporated in the AfCFTA, although it is yet to enter into force. All major economies participate in spam provisions, signaling broad consensus on this subject.

Online safety and security

Online safety and security provisions are an emerging element of digital trade agreements, with only 10 provisions across six agreements between 61 jurisdictions, from 2020 to 2024. In this time period, the political salience of online harms grew substantially at the domestic and international level. The provisions recognize the importance of creating safe and secure online environments supporting digital trade and establish commitments to protect users from harmful content including terrorist and violent extremist content. Most provisions use non-binding language recognizing shared responsibility amongst governments, technology service providers, and users.

Components

Online safety provisions focus on cooperation and contain two core elements:

1. a recognition of the importance of a safe and secure online environment; and
2. a commitment to cooperate, share information, and exchange best practices on online safety matters.

The recognitions cover a range of topics, with all provisions stating that a safe and secure online environment supports the digital economy. Some further recognize the importance of a multi-stakeholder approach to addressing online safety and security issues, as well as its significant challenge to and shared responsibility between governments, providers, and users. These provisions also recognize the responsibility of industry to protect users.

The commitment obliges either cooperation between countries to develop solutions to global online safety and security issues or the creation and promotion of a safe online environment, where users are protected from harmful content and businesses can thrive. Cooperation commitments are typically formulated in non-binding "shall endeavor" language. The second type of commitment is generally binding and also mentions the role of international fora to create a safe online environment. It further specifies that parties "shall endeavor" to maintain an open, free, and secure internet when working to create a safe online environment.

Evolution

Online safety provisions emerged in 2020, as the DEPA and the Australia-Singapore DEA established two distinct approaches. The DEPA used a brief formulation, including the recognition and cooperation commitment. The Australia-Singapore DEA introduced a more detailed approach, including direct commitments to create a safe online environment and work together in international fora in pursuit of this goal. Subsequent agreements, including the

Major economies, including the US, the EU, China, India, and Japan have not entered into online safety commitments, as have major plurilateral frameworks including CPTPP and RCEP.

Singapore-UK DEA (2022), the Korea-Singapore DPA (2022) followed the DEPA approach while the Australia-UAE CEPA (2024) followed the Australia-Singapore DEA approach.

In 2024, the AfCFTA Digital Trade Protocol, which is yet to enter into force, diverged from this approach by establishing a comprehensive Annex on online safety and security. In the provision, parties agree to promote a safe and secure online environment that supports digital trade. The Annex then establishes a duty of care, requires parties to adopt or maintain laws fostering safe online environments, requires companies to comply with online safety regulations and publish their own safety and security policies, and requires parties to establish or designate competent online safety authorities. Finally, parties must harmonize their laws and regulations on online safety.

Sixty-one jurisdictions now participate in online safety provisions, 54 of which are AfCFTA signatories. Singapore is the most active jurisdiction, participating in four provisions. Major economies, including the US, the EU, China, India, and Japan have not entered into commitments, as have major plurilateral frameworks including CPTPP and RCEP. There is a reason for this, as we elaborate below.

Recent developments

Two factors contribute to the rarity of online safety commitments: Online safety is a novel, albeit rapidly growing, area of digital policy and not traditionally a trade subject.

Yet, domestically, online safety is one of the fastest-growing areas of digital policy. Digital Policy Alert has documented over 1,400 policy and enforcement developments focusing on online content moderation, a recent focus being AI-generated sexualized content on X. Governments are further imposing authorization, registration, and licensing regimes, totaling over 1,000 developments since January 2020. Such an increase in domestic regulatory activity is usually a driver of international alignment, such as digital trade commitments, to build common ground between governments pursuing the same regulatory objectives.

Two factors complicate such international alignment. First, online safety is an area where governments tend to prioritize the domestic perspective, as opposed to international alignment. Often, online safety issues fall into the realm of public morals and countries' sovereignty, where exception mechanisms allow governments to pursue domestic policies even if they contradict trade commitments. Second, the US government has strongly pushed back against foreign rules governing online content, especially the EU Digital Services Act and, less prominently, the UK Online Safety Act. Based on a "free speech" narrative, senior US officials and leaders have vocally countered online content rules, as well as enforcement actions against US companies, especially the EU's EUR 120 million fine against X in December 2025. Temporarily, the US government even issued travel visa restrictions against a Brazilian judge, due to his rulings that the US viewed as being online "censorship."

US intermediary liability provisions limit the liability of interactive computer services for third-party content, while European provisions establish safe harbors for intermediary service providers engaged in mere conduit, caching, and hosting activities, subject to specified conditions.

Ironically, online safety is one of the rare digital policy areas in which the US has adopted domestic regulation at the federal level. The President signed the TAKE IT DOWN Act in May 2025, including content moderation obligations for non-consensual intimate imagery, while the Senate passed the DEFIANCE Act in January 2026, introducing civil action rights for citizens affected by deepfakes. Online safety is also the focus of several enforcement actions pursued by the US administration, as well as a range of state-level laws and legislative proposals.

Intermediary liability

Intermediary liability provisions are rare, comprising 17 provisions across seven agreements between 35 jurisdictions, spanning from 2014 to 2020. The provisions limit the liability of online intermediaries such as service providers that transmit information, caching providers, or hosting service providers, based on two approaches: US provisions limit the liability of interactive computer services for third-party content, while European provisions establish safe harbors for intermediary service providers engaged in mere conduit, caching, and hosting activities, subject to specified conditions.

The US established its approach in the USMCA (2018), which was replicated by the US-Japan Digital Trade Agreement (2019). It first recognizes the importance of interactive computer services for digital trade growth. Then, it prohibits parties from adopting or maintaining measures that treat suppliers or users of interactive computer services as information content providers in determining liability for harms related to information stored, processed, transmitted, distributed, or made available by another information content provider. The provisions include exceptions permitting enforcement of laws relating to intellectual property rights and criminal law.

The European approach emerged from EU association agreements with Georgia (2014), Moldova (2014), and Armenia (2017), as well as agreements between the UK and Georgia and the UK and Moldova. These provisions distinguish between three types of intermediary services.

1. "Mere conduit" service providers that transmit information in communication networks or provide network access are not liable for transmitted information provided they do not initiate transmission, select receivers, or select or modify information, and provided they do not store information longer than reasonably necessary for transmission.

2. "Caching" service providers, automatically and temporarily storing information for efficient onward transmission, are not liable provided they do not modify information, comply with access conditions, comply with information update rules, do not interfere with the lawful use of technology, and act expeditiously to remove or disable access to cached information upon obtaining actual knowledge of removal or disabling at initial source or of court or administrative authority orders.

3. "Hosting" service providers, storing information provided by service recipients, are not liable provided they do not have actual knowledge of illegal activity or information and are not aware of facts or circumstances from which illegal activity is apparent, or upon obtaining such knowledge or awareness act expeditiously to remove or disable access to information.

Nearly all cybersecurity provisions include recognitions, typically acknowledging that threats to cybersecurity undermine confidence in digital trade.

The two approaches are grounded in their respective domestic regulatory frameworks. Section 230 of the US Communications Decency Act establishes that platforms generally are not liable for third-party content. The European approach stems from the EU's Electronic Commerce Directive, which serves as template for the EU Digital Services Act (see section on Online Safety and Security).

In total, 35 jurisdictions worldwide now participate in intermediary liability provisions, including the 27 EU member states separately. Major Asia-Pacific economies including Singapore, Australia, and China have not entered into such commitments, in contrast to their participation in numerous other digital trade commitments. Regional frameworks, including the CPTPP, the RCEP, the AfCFTA Digital Trade Protocol, and ASEAN frameworks all also do not include intermediary liability provisions. This limited diffusion reflects fundamental disagreements regarding intermediary liability: Western governments limited intermediary liability in the early days of the Internet, over 25 years ago, whereas the rest of the world's legal regimes are still emerging and evolving, hindering governments from entering into commitments on intermediary liability in FTAs.

Cybersecurity

Cybersecurity provisions are a well-established element of digital trade agreements, with 60 provisions across 54 agreements between 129 jurisdictions, spanning 2001 to 2026. This includes stand-alone cybersecurity provisions and cooperation provisions with dedicated language on cybersecurity. The provisions recognize the importance of building capabilities of national entities responsible for computer security incident response and using existing collaboration mechanisms to cooperate on cybersecurity matters. All provisions use non-binding language regarding cooperation, rather than binding obligations. This lack of binding language, even among closely aligned trading and security partners, signals how (cyber)security remains an area in which governments emphasize sovereign control over international alignment. Finally, most provisions include commitments regarding exchange of best practices, building incident response capabilities, and cooperation through existing mechanisms.

Components

Cybersecurity provisions combine a recognition of the importance of cybersecurity for digital trade with language on cooperation. Nearly all provisions include recognitions, typically acknowledging that threats to cybersecurity undermine confidence in digital trade. This recognition establishes the basis for the cooperation commitments.

The language on cooperation ranges from the mere recognition of the importance of cybersecurity cooperation, in 36 provisions, to non-binding "shall endeavor" cooperation commitments, in 14 provisions. Cooperation mechanisms include building the capabilities of national entities responsible for computer security incident response, through training and the exchange of best practices, as well as using existing collaboration mechanisms to cooperate on identifying and mitigating malicious intrusions and other cybersecurity matters. Less frequently, provisions mention workforce development and the mutual recognition of qualifications.

In 2018, the CPTPP and USMCA established two templates for cybersecurity provisions, with the CPTPP recognizing the importance of cooperation and the USMCA using "shall endeavor" language to commit parties to such cooperation.

Fourteen provisions additionally reference risk-based approaches to cybersecurity. They recognize that risk-based approaches may be more effective than prescriptive or compliance-based approaches, given the evolving nature of cybersecurity threats. Subsequently, these provisions establish non-binding commitments for parties to encourage companies to pursue such risk-based cybersecurity approaches. Only two provisions formulate these commitments in binding "shall" language.

Finally, AfCFTA contains several binding commitments, in "shall" language, to adopt or maintain cybersecurity measures. In addition, it contains "endeavor" commitments to build capabilities of national authorities, develop and strengthen collaboration mechanisms, and maintain dialogue on cybersecurity, among others. They are yet to enter into force.

Evolution

Cybersecurity was first mentioned in the Jordan-US Joint Statement on Electronic Commerce (2001), with a focus on critical infrastructure protection. In 2018, the CPTPP and USMCA established two templates for cybersecurity provisions. The CPTPP recognized the importance of cooperation, including building capabilities and using existing collaboration mechanisms to cooperate, without establishing a commitment. The USMCA used "shall endeavor" language to commit parties to such cooperation. It further included language recognizing the value of risk-based, as opposed to prescriptive, approaches to cybersecurity, including a non-binding commitment thereon.

In the subsequent surge of cybersecurity provisions, the CPTPP approach was used in 24 provisions, the USMCA approach was followed in nine provisions, and

The importance of cybersecurity for governments is visible in global regulatory activity as the incidence of cyberattacks increase globally.

The lack of more "intrusive" formulations signals how (cyber) security remains an area in which governments insist on sovereign control, as opposed to international alignment.

new approaches emerged. The UK, for instance, combined elements of both models with additional language on a shared vision to promote secure digital trade, in four provisions. The UAE entered into 18 cybersecurity commitments, in both standalone cybersecurity and broader cooperation provisions. The AfCFTA Digital Trade Protocol incorporated a cybersecurity provision and additionally addressed cybersecurity in the context of online safety and critical infrastructure: Its Annex requires parties to adopt or maintain laws for maintenance and protection of critical infrastructure from disruption, destruction, or interference, adopting risk-based approaches to identify critical infrastructure where cybersecurity incidents could result in catastrophic effects.

Geographic patterns

Cybersecurity provisions are widespread, covering 129 jurisdictions worldwide. The UAE participates in the most provisions, all negotiated after 2022, followed by Singapore. The geographically broadest provision, in the AfCFTA, covers 54 African jurisdictions. Notably, all major economic blocs participate in cybersecurity provision.

The spread of cybersecurity provisions can be explained by their "non-intrusive" language. Provisions focus on cooperation without imposing any obligations that affect domestic cybersecurity policy. By avoiding interference with delicate domestic rules, these provisions were thus able to proliferate across continents. The lack of more "intrusive" formulations signals how (cyber)security remains an area in which governments insist on sovereign control, as opposed to international alignment.

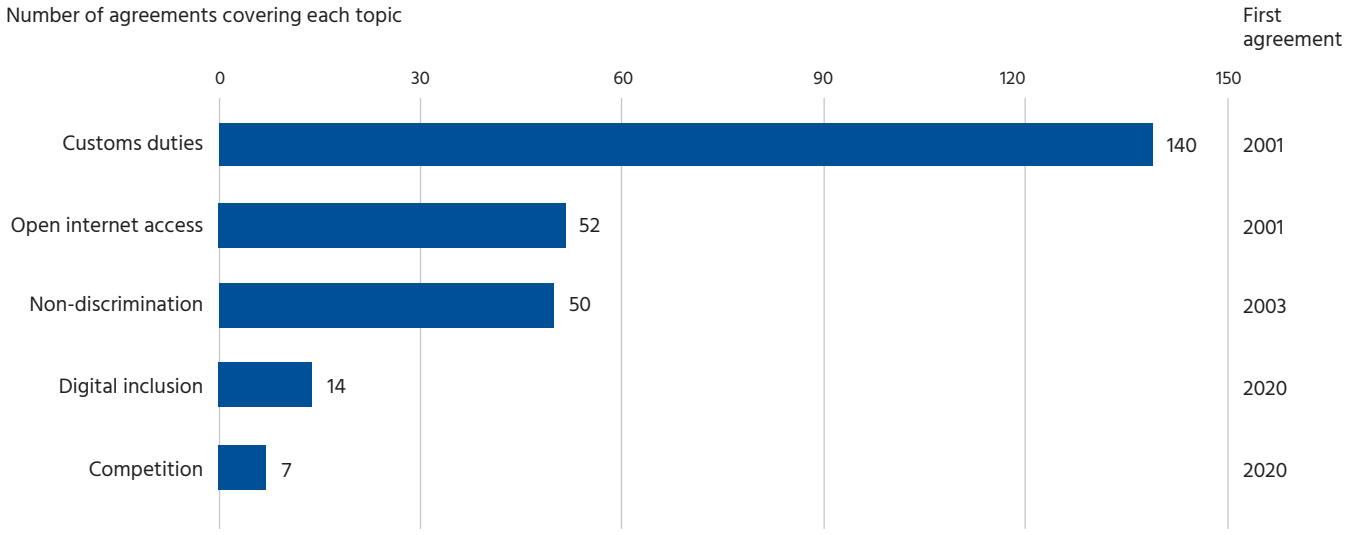
Recent developments

Yet the importance of cybersecurity for governments is visible in global regulatory activity as the incidence of cyberattacks increase globally: Digital Policy Alert has documented over 1,200 cybersecurity policy and enforcement developments since January 2020. The most active governments were the US, China, and the EU, while the most affected sectors include digital infrastructure and AI.

On the international stage, the "tariff deals" between the US and Argentina, Bangladesh, Cambodia, Taiwan, El Salvador, Guatemala, Indonesia, and Malaysia all include language on cybersecurity. Specifically, governments commit to collaborating with the US to "address cybersecurity challenges." The Malaysia-US Reciprocal Trade Agreement further provides specific examples of possible collaboration, including "exchanging information on threats and best practices, promoting the use of relevant international standards, and understanding capacity-building activities."

Section D: Market access

Figure 7 – Market access commitments



Source: Digital Policy Alert

Non-discrimination commitments for digital products are an established element of digital trade agreements, with 51 provisions across 50 agreements between 94 jurisdictions, spanning 2003 and 2025.

Digital trade commitments on market access include provisions on non-discrimination, customs duties on electronic transmissions, competition, open internet access, and digital inclusion. Given the prevalence of non-discrimination and customs duties in digital trade agreements, we analyze these commitments in depth. For competition policy, we also address recent international tensions and domestic developments.

Non-discrimination

Non-discrimination commitments for digital products are an established element of digital trade agreements, with 51 provisions across 50 agreements between 94 jurisdictions, spanning 2003 and 2025. The provisions establish non-discrimination obligations combining "most-favoured-nation" (MFN) and national treatment principles, typically through a unified approach that prohibits discrimination based on both the territorial origin of digital products and the nationality of their creators. Exceptions, particularly for subsidies and broadcasting, and refinements in scope and definitions have evolved over time.

Non-discrimination provisions for digital products first emerged in 2003 with the US-Chile FTA and the Singapore-US FTA, establishing the template that would persist throughout the following two decades: a unified non-discrimination obligation combining national treatment and MFN commitments.

Components

The non-discrimination commitments are the main element of these provisions:

- The national treatment obligation prohibits parties from according less favorable treatment to digital products of another party than to domestic like digital products. Forty-nine provisions include this obligation. The formulation typically states that no party shall accord less favorable treatment to a digital product "created, produced, published, contracted for, commissioned, or first made available on commercial terms" in the territory of another party, or to a digital product of which the "author, performer, producer, developer, or owner" is a person of another party.

- The MFN obligation prohibits parties from according less favorable treatment to digital products of another party than to like digital products of any other country. Forty provisions include this obligation, preventing preferential arrangements that would discriminate against one trading partner in favor of another. Provisions typically include a clarification extending the MFN treatment to digital products from non-parties. This establishes a global non-discrimination standard rather than one limited to products from other parties, though the MFN principle is now under intense global policy debate as major economies seek to reinterpret the bedrock trading principle.

Exceptions carve out specific policy areas from these non-discrimination commitments, including:

- subsidies, grants, government-supported loans, and guarantees.
- broadcasting, typically defined with reference to scheduled transmission of series of content over which consumers have no choice regarding scheduling.
- measures inconsistent with intellectual property chapters.

Evolution

Non-discrimination provisions for digital products first emerged in 2003 with the US-Chile FTA and the Singapore-US FTA. These initial provisions established the template that would persist throughout the following two decades: a unified non-discrimination obligation combining national treatment and MFN commitments. The US-Chile FTA adopted a more streamlined approach focusing on the core unified obligation. The Singapore-US FTA included a more elaborate structure with separate paragraphs for national treatment and MFN treatment alongside the unified obligation, as well as extensive clarifications regarding the extension of MFN treatment to non-parties and a broadcasting exception.

Non-discrimination provisions continued emerging between 2004 to 2010, totaling 15. Between 2011 and 2017, only five provisions were negotiated, but expanded to new regions including through the Central America-Mexico FTA (2011) and several Japanese agreements.

In 2018, non-discrimination provisions experienced renewed momentum as mega-regional FTAs took off. The CPTPP established non-discrimination across 11 parties spanning the Asia-Pacific and Americas. The CPTPP provision evolved into a new reference template for subsequent regional agreements. Also in 2018, the USMCA

Controversy remains that the US priority appears to be on foreign digital policies it deems to discriminate against US companies, rather the broader traditional sensibilities of the MFN principle as embodied in GATT and WTO rules.

incorporated a streamlined formulation, without broadcasting and intellectual property carve-outs. This template was included in the US-Japan Digital Trade Agreement (2019).

Since then, non-discrimination provisions have spread rapidly, including through extensive negotiations by the UAE totaling 11 commitments. In 2024, the AfCFTA Digital Trade Protocol incorporated extensive language on non-discrimination, including a standard provision as well as references to non-discrimination in Annexes on data and emerging technologies, among others. It is yet to enter into force.

Geographic patterns and recent developments

Non-discrimination provisions now cover 94 jurisdictions across the globe, with the US and Singapore participating in the most provisions. The AfCFTA represents the most expansive provision, covering 54 jurisdictions. Since both China and the EU do not participate in any non-discrimination provisions, among major economic blocs, non-discrimination is seemingly a US priority. Yet controversy remains that the US priority appears to be on foreign digital policies it deems to discriminate against US companies, rather the broader traditional sensibilities of the MFN principle as embodied in GATT and WTO rules.

The US government's emphasis on non-discrimination is visible in recent "tariff deals" with Argentina, Taiwan, Bangladesh, Cambodia, El Salvador, Guatemala, Indonesia, and Malaysia. In its joint statement, India committed to negotiate robust digital trade rules that address discriminatory or practices.

The US government has pushed back on various foreign digital policies it deems to discriminate against US companies. It prominently opposes digital services taxes, including in its "tariff deals" requirements for counterparts not to "impose digital services taxes, or similar taxes, that discriminate against U.S. companies in law or in fact." Furthermore, the US government vehemently opposes the EU Digital Services Act and Digital Markets Act, as well as Korea's proposed digital competition rules (see section on Competition), due to perceived discrimination against US companies.

Customs duties

Customs duties provisions represent another of the most established and widely adopted digital trade commitments, with 158 provisions across 140 agreements between 157 jurisdictions, from 2001 to 2026. The provisions prohibit parties from imposing customs duties on electronic transmissions, with clarifications preserving internal taxation authority. The provisions chronologically evolved from non-binding, to mixed, to binding commitments.

Components

Provisions contain two elements: the prohibition of customs duties on electronic transmissions and clarifications regarding scope and preserved regulatory authority.

Customs duties provisions emerge from the WTO's Work Programme on electronic commerce and the 1998 WTO ministerial declaration establishing a practice of not imposing customs duties on electronic transmissions.

The core prohibition has only minimal variations in binding-ness: 108 provisions use "shall not impose" and equivalent binding language prohibiting parties from imposing customs duties on electronic transmissions. In 24 provisions, parties commit to maintain their current practice of not imposing customs duties on electronic transmissions, while in five provisions they merely confirm current adherence to this practice. Two provisions including Jordan as a party contain less binding language ("seek to refrain from imposing").

The scope of the prohibition is defined in different terms: the majority of provisions limit the prohibition to customs duties on "electronic transmissions," while some provisions mention "digital products." A common clarification, found in some provisions, specifies that "content transmitted electronically" is covered by the prohibition. The "electronic transmissions" formulation focuses on the transmission method rather than the content, avoiding classification debates regarding whether digitally delivered content constitutes goods, services, or intellectual property. The "digital products" formulation explicitly addresses the product being transmitted rather than the transmission itself.

Regarding regulatory authority, a large part of provisions clarify that the prohibition does not preclude parties from imposing internal taxes, fees, or other charges on electronic transmissions, content transmitted electronically, or digital products, provided such internal measures are imposed consistently with the agreement. This clarification preserves parties' fiscal sovereignty to apply value-added taxes, sales taxes, and other internal taxation to digitally delivered products, distinguishing at-the-border measures from behind-the-border measures.

Additional passages often explicitly reference WTO ministerial decisions on the WTO's Work Programme on electronic commerce, linking the bilateral commitment to the multilateral context and preserving parties' rights to adjust practice in accordance with future WTO decisions. Others specify rules for customs valuation of physical carrier media bearing digital content.

Evolution over time

Customs duties provisions emerge from the WTO's Work Programme on electronic commerce and the 1998 WTO ministerial declaration establishing a practice of not imposing customs duties on electronic transmissions. This multilateral practice has been consistently renewed at subsequent ministerial conferences through extensions of a global moratorium on customs duties. In digital trade agreements, customs duties provisions first appeared in the Jordan-US FTA (2001), stating that parties will "seek to refrain" from deviating from existing practice of not imposing customs duties on electronic transmissions, without establishing a binding prohibition.

From 2003 to 2007, provisions proliferated through various FTAs spanning across continents. The Singapore-US FTA incorporated the first binding prohibition, focused on digital products, including the clarification regarding internal taxes. The Australia-Singapore and Australia-Thailand FTAs adopted "maintain current practice" language. From 2008 to 2017, provisions continued using diverse formulations without clear convergence.

Indonesia's turnaround on its longstanding support for customs duties on electronic transmissions under its US "tariff deal" represents how US pressure can be an effective vector for precipitating far-reaching changes in a country's digital trade policy.

One common approach, found in numerous Chinese agreements, referenced a WTO ministerial decision on the Work Programme on electronic commerce and added a passage that "each party may adjust its practice" in accordance with any further WTO ministerial decisions. In 2018, the CPTPP and the USMCA established the most frequently used template, combining all the components outlined above.

From 2021 to 2026, 95 provisions incorporated customs duty prohibitions, mostly following either the CPTPP or the RCEP approach. In European agreements, parties agree that electronic transmissions shall be considered as the provision of services, which cannot be subject to customs duties. The AfCFTA Digital Trade Protocol followed the CPTPP approach but additionally incorporated a comprehensive Annex on rules of origin. It is yet to enter into force.

Geographic patterns and recent developments

The provisions cover 157 jurisdictions across the world, including all major economies. Singapore and the UAE participate in the most provisions. The AfCFTA Digital Trade Protocol is currently the geographically broadest agreement. The WTO Agreement on Electronic Commerce, which is yet to enter into force, would provide broader coverage.

Beyond digital trade agreements, customs duties are currently at the center of two sets of contentious international negotiations. At the multilateral level, the WTO members decided at the 13th Ministerial Conference in 2024 that the moratorium on customs duties would expire at the 14th Ministerial Conference in March 2026. This occurred due to growing concerns from developing countries regarding the erosion of their potential tariff revenue base. If the moratorium is not prolonged, the importance of bilateral commitments on customs duties rise substantially.

Secondly, the US government is incorporating commitments on customs duties in its "tariff deals," with Argentina, Bangladesh, Cambodia, Taiwan, El Salvador, Guatemala, Indonesia, and Malaysia. All deals contain identical commitments that parties "shall not impose customs duties on electronic transmissions, including content transmitted electronically." All agreements further include commitments to support the multilateral adoption of a permanent moratorium on customs duties. For Argentina, Cambodia, and Indonesia, this commitment is explicitly immediate and unconditional.

Notably, the reciprocal trade agreement between the US and Indonesia includes additional commitments by Indonesia to eliminate existing tariff lines on "intangible products" and suspend related requirements on import declarations. Indonesia was long a leading proponent of customs duties on electronic transmission and laid the groundwork for their imposition at the domestic level, without actually imposing them. In 2006, Indonesia clarified that imports and exports by electronic means are covered by its customs regime. In 2018, Indonesia specified the types of intangible products covered by its customs regime by expanding its import tariffs book with a chapter on software and other digital goods. In 2023, Indonesia implemented an import declaration procedure for software and other digital products, requiring an import declaration within 30 days of payment. Indonesia's turnaround on this issue under its US "tariff deal" represents how US pressure can be an effective vector for precipitating far-reaching changes in a country's digital trade policy.

Competition provisions are an emerging element of digital trade agreements, comprising only eight provisions across seven agreements between 65 jurisdictions, spanning from 2020 to 2025.

Domestically, governments are gravitating to other means of raising tax revenue from the digital economy. Rather than border measures, such as customs duties, governments are focusing on internal taxes, including direct digital services taxes and indirect sales tax and value-added-tax regimes. Internal taxes are explicitly carved out from customs duties provisions and thus consistent with digital trade commitments. US "tariff deals", however, all contain commitments to not impose digital services taxes, or similar taxes, that discriminate against US companies in law or in fact.

Competition

Competition provisions are an emerging element of digital trade agreements, comprising only eight provisions across seven agreements between 65 jurisdictions, spanning from 2020 to 2025. The provisions establish frameworks for collaborative enforcement of competition law and joint development of regulatory approaches to address challenges arising from digital markets. They first articulate a shared recognition of benefits from cooperation and list potential technical cooperation activities, and then commit parties to cooperate on enforcement matters in binding or non-binding language.

Components

Competition provisions, including provisions on "competition and innovation" and on "cooperation on competition policy," are structured into two paragraphs. They begin with a recognition of the importance of cooperation and a list of cooperation mechanisms, then commitments.

Provisions recognize that parties can benefit by sharing experiences in enforcing competition law and developing competition policies to address digital economy challenges. Building on this recognition, provisions address specific cooperation activities parties shall consider or endeavor to undertake:

- exchanging information and experiences on competition policy development for digital markets;
- sharing best practices on competition law enforcement and competition promotion in digital environments;
- providing advice or training, including through official exchanges, to build capacity for competition policy development and enforcement; and
- undertaking other mutually agreed forms of technical cooperation.

Provisions then require parties to cooperate on competition law enforcement issues in digital markets through notification, consultation, and information exchange mechanisms. This commitment is formulated in either binding "shall" or non-binding "shall endeavor" language.

Beyond these core components, provisions incorporate qualifying language that provides implementation flexibility. The most common qualifiers include "where practicable," "subject to available resources," "in accordance with respective laws and regulations," "as appropriate," and "in areas of mutual interest." Several provisions include explicit clauses stating that cooperation must be compatible with each party's domestic law and important interests, and occur within reasonably available resources.

Sixty-five jurisdictions now participate in competition policy provisions, of which 54 through the AfCFTA Digital Trade Protocol, which is yet to enter into force.

Evolution

Competition policy provisions first emerged in 2020, in the Australia-Singapore DEA and the DEPA. The Australia-Singapore DEA introduced an "endeavor" template, using "shall consider" language for technical cooperation activities, and "shall endeavor" for cooperation. The DEPA established a more binding template, using "shall" language for cooperation, while maintaining "shall consider" in the first section.

Subsequent competition provisions in the Singapore-UK DEA (2022), the Ukraine-UK agreement (2023), and the EFTA-Singapore agreement (2025, yet to enter into force) adopted the "endeavor" approach. The Korea-Singapore DPA (2022) followed the DEPA approach. The AfCFTA Digital Trade Protocol (2024, yet to enter into force) includes provisions on competition and innovation in its Annexes on cross-border digital payments and on financial technology.

Geographic patterns and recent developments

Sixty-five jurisdictions now participate in competition policy provisions, of which 54 through the AfCFTA Digital Trade Protocol, which is yet to enter into force. Singapore participates in the most provisions. The major economic blocs, including the US, the EU, China, and India have not incorporated competition provisions.

Beyond the novelty of digital competition, two reasons could contribute to the limited diffusion of these provisions. First, longstanding tensions persist between domestic competition regulators and international trade negotiators, rendering competition a difficult subject matter for trade agreements. Second, governments are developing widely diverging regulatory approaches to digital competition: Competition is one of the digital policy areas in which governments

Longstanding tensions persist between domestic competition regulators and international trade negotiators, rendering competition a difficult subject matter for trade agreements.

Internet access provisions represent an established element of digital trade agreements, with 55 provisions across 52 agreements between 128 jurisdictions, spanning 2001 to 2025.

most frequently adopt policies and pursue enforcement: Digital Policy Alert has documented over 1,100 policy and enforcement developments in digital competition. This regulatory activity complicates international alignment, especially with the US government.

The US government continuously counters foreign competition regimes for digital markets that it perceives to discriminate against US companies. In the past year, the US government has focused on the EU Digital Markets Act as well as Korean digital competition proposals. Beyond countering policy developments, the US has protested against enforcement developments: A US official said that EU fines against Apple and Meta under the Digital Markets Act (of EUR 500 million and EUR 200 million respectively) are a "novel form of economic extortion" that "will not be tolerated."

This pressure has resulted in a formal commitment by Cambodia, in its "tariff deal" with the US, not to introduce a digital competition regime that "unreasonably or unjustifiably restricts U.S. commerce." Further, documents related to ongoing negotiations with Korea and China include references to competition. Although the deal is yet to be finalized, the statement with Korea mentions a commitment by Korea to ensure that US companies do not face unnecessary barriers in terms of "laws and policies concerning digital services, including online platform regulations," which refers to proposed digital competition rules. The US government's fact sheet on negotiations with China, states that China will terminate antitrust and anti-monopoly investigations targeting US companies in the semiconductor supply chain. Although this commitment was not confirmed by China, it reportedly dropped a competition investigation into Google during negotiations, but it is by no means certain that any such commitment may eventually change during the course of negotiations.

Open internet access

Internet access provisions represent an established element of digital trade agreements, with 55 provisions across 52 agreements between 128 jurisdictions, spanning 2001 to 2025. The provisions recognize the benefits of users having the ability to access and use services and applications of their choice available on the internet, connect end-user devices to the internet, and access information on network management practices. Provisions use non-binding language rather than binding obligations, with few exceptions.

Components

Internet access provisions contain three core components:
1. a recognition of principles on access to and use of the internet;
2. a commitment regarding the openness of the internet for digital trade; and
3. clarifications on the scope limitations of the commitment.

Provisions establish internet access frameworks through a recognition of benefits and specification of user abilities subject to regulatory authority. Twenty-seven provisions explicitly use "recognize the benefits" language, while other provisions implicitly recognize principles by stating that parties affirm, acknowledge, or commit to principles regarding internet access.

Distinct approaches to internet access provisions emerged in Europe, with EU and UK agreements placing emphasis on non-discriminatory treatment of internet traffic, while EFTA provisions introduced binding "shall" language.

The provisions then establish a commitment regarding open internet access, with various degrees of binding-ness. Only two provisions, both including EFTA as a party, use binding "shall" language. Five provisions use "shall endeavor" language, and two provisions use "should," while recognitions are predominant.

Commitments concern three matters:

- the ability to access and use services and applications of choice available on the internet, subject to reasonable network management. This encompasses accessing content, services, and applications without discriminatory blocking or throttling based on commercial considerations;
- the ability to connect end-user devices of choice to the internet, provided devices do not harm the network. This establishes device neutrality preventing internet service providers from restricting device choices; and
- the ability to access information on network management practices, ensuring transparency regarding internet service providers' policies.

Beyond these three core elements, some provisions include a fourth element allowing consumers to "run services and applications of their choice, subject to the party's law, including the needs of legal and regulatory enforcement activities."

Provisions provide limitations on these commitments, with three common qualifications:

- "reasonable network management," permitting network operators to engage in practices necessary for network integrity, security, and performance without violating open internet principles;
- net neutrality, explicitly addressing blocking, slowing down, or discrimination of traffic, typically qualifying that reasonable network management does not include blocking or slowing traffic based on commercial reasons; and
- "applicable policies, laws and regulations," establishing that recognized principles apply within parties' existing regulatory frameworks rather than constraining regulatory authority.

Evolution across time and regions and geographic patterns

Internet access provisions first emerged in the Jordan-US Joint Statement on Electronic Commerce (2001), followed by the US-Korea FTA (2007). The provisions gained momentum from 2018 onwards, when the CPTPP established a template comprising the elements outlined above that was subsequently widely adopted, including in the USMCA (2018).

From 2019 to 2025, 50 provisions adopted variations of this provision. Distinct approaches emerged in Europe, with EU and UK agreements placing emphasis on non-discriminatory treatment of internet traffic, while EFTA provisions introduced binding "shall" language.

Digital inclusion provisions contain two core components: a recognition of the importance of digital inclusion and the need to address barriers to participation and a commitment to cooperate on digital inclusion, targeting specific groups.

Internet access provisions span 128 jurisdictions, including the US, the EU, and India, but not China. The UAE is the most active jurisdiction, with a total of 19 internet access provisions, all negotiated between 2022 and 2025. The AfCFTA Digital Trade Protocol, yet to enter into force, has the broadest geographical span.

Digital inclusion

Digital inclusion provisions are rare, comprising 14 provisions across 14 agreements between 106 jurisdictions, spanning 2021 to 2025. Provisions recognize the importance of ensuring that all people and businesses, including marginalized groups and small- and medium-sized enterprises (SMEs), can participate in, contribute to, and benefit from digital trade. With slight variations in binding-ness, the provisions pursue cooperation toward these goals.

Components

Digital inclusion provisions contain two core components: a recognition of the importance of digital inclusion and the need to address barriers to participation and a commitment to cooperate on digital inclusion, targeting specific groups.

Thirteen provisions open with a recognition that digital inclusion matters for digital trade and that expanding opportunities may require tailored approaches developed in consultation with groups that disproportionately face barriers. Some provisions explicitly name the groups concerned, including women, persons with disabilities, rural populations, and indigenous peoples.

The provisions then commit parties to cooperate on digital inclusion. Cooperation activities include sharing best practices and experiences, identifying and

Digital inclusion provisions recognize the importance of ensuring that all people and businesses can participate in, contribute to, and benefit from digital trade.

Digital inclusion provisions now cover 106 jurisdictions, including 54 AfCFTA signatories and 27 EU member states, as well as China, with Singapore and New Zealand participating in the most provisions.

addressing barriers to digital trade, improving digital skills and access to online business tools, sharing methods for collecting disaggregated data on participation, and promoting inclusive economic growth. The basic commitment to cooperate typically uses binding language ("shall"), while specific cooperative activities use "may include" language.

Five provisions include specific references to SME participation in digital trade, recognizing the role of SMEs in economic growth and job creation, and committing parties to foster cooperation. Four provisions additionally recognize the digital divide between developed and developing countries and commit parties to cooperate to promote developing country participation.

Evolution and geographical patterns

The DEPA (2020) established the first digital inclusion provision, followed by the Chile-Paraguay FTA (2021), the UK-New Zealand FTA (2022), and the Singapore-UK DEA (2022). The UK-New Zealand provision provided particular detail, including naming the Māori population as target beneficiaries.

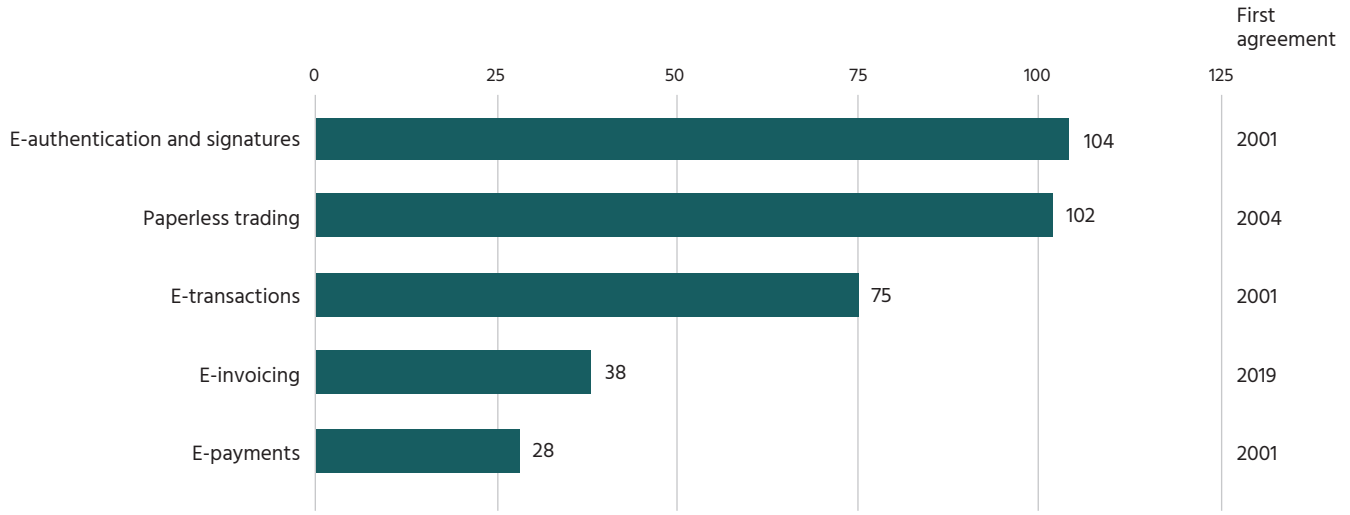
From 2024 onwards, the number of digital inclusion provisions rapidly grew, across continents, maintaining the same approach. One exception is the AfCFTA Digital Trade Protocol, adopted in 2024 but yet to enter into force, which formulates the core commitment obligation, to promote and facilitate the inclusion and participation, in binding "shall" language and then lists specific cooperation activities. This is perhaps unsurprising given Africa's large number of Least Developed Countries (LDCs) and underserved segments of the global population.

Digital inclusion provisions now cover 106 jurisdictions, including 54 AfCFTA signatories and 27 EU member states, as well as China. Singapore and New Zealand participate in the most provisions. The US has not entered into digital inclusion commitments.

Section E: Digital business

Figure 8 – Digital business commitments

Number of agreements covering each topic



Source: Digital Policy Alert

Electronic transactions provisions comprise 76 provisions across 75 agreements, covering 136 jurisdictions, with the core commitment requiring parties to adopt or maintain a domestic legal framework governing electronic transactions.

Digital business provisions include provisions on electronic transactions, electronic authentication and signatures, electronic invoicing, and paperless trade. As these are established commitments, on which governments have more ease in finding common ground, we provide a brief overview of the prevalence and spread for each of these commitments.

Electronic transactions

Electronic transactions provisions comprise 76 provisions across 75 agreements, covering 136 jurisdictions. The core commitment requires parties to adopt or maintain a domestic legal framework governing electronic transactions. Forty-one provisions use binding language, such as "shall maintain" or "shall adopt or maintain" with regard to the core commitment. Eighteen provisions use softer endeavor language, predominantly in UAE bilateral agreements, again signaling its desire to participate in provisions and flexibility in adapting formulations to trading partners.

Two templates have emerged around this core commitment. The most commonly used CPTPP template requires consistency with the principles of the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996) and adds commitments to avoid unnecessary

The majority of electronic payments provisions follow a template recognizing the growth of non-bank and fintech payment providers and committing parties to encourage the adoption of internationally accepted standards, promote the interoperability of payment infrastructures, and encourage innovation and competition.

regulatory burden and to facilitate stakeholder input. The other approach focuses on the contents of the legal framework, specifying that parties shall not deny the legal effect, validity, or enforceability of transactions, including contracts, solely because of their electronic form and that parties should not arbitrarily discriminate between different forms of electronic transactions.

The Jordan-US Joint Statement (2001) included the earliest reference. The CPTPP (2018) codified the predominant template, widely adopted across Asia-Pacific and Latin American agreements. The EU consolidated its contractual-validity approach in agreements with Singapore, Korea, Indonesia, and Mercosur. The agreements with Korea, Indonesia, and Mercosur are yet to enter into force. All major economies participate in electronic transactions provisions, including the US, the EU, China, and India.

Electronic authentication and electronic signatures

Electronic authentication provisions comprise 106 provisions across 104 agreements, including 143 jurisdictions. The core commitment prohibits parties from denying the legal validity of a signature solely because it is in electronic form. Seventy agreements use "shall" language with regard to the core commitment, while seven agreements use "may" and one uses "should." Provisions further address the freedom of transaction parties to determine appropriate authentication methods, exceptions for performance standards, and interoperability of authentication systems.

The most common template, used in CPTPP and previous Latin American agreements, combines the prohibition on denying validity with detailed rules on authentication methods and interoperability. Fewer agreements use a leaner formulation, limited to the core commitment prohibition and encouragement of interoperability. The US, the EU, China, and India all participate in at least one electronic authentication and signature provision.

Electronic payments

Electronic payments provisions comprise 37 provisions across 28 agreements, covering 116 jurisdictions. Provisions commit parties to support efficient, safe, and secure cross-border electronic payments. The majority of provisions follow a template recognizing the growth of non-bank and fintech payment providers and committing parties to encourage the adoption of internationally accepted standards, promote the interoperability of payment infrastructures, and encourage innovation and competition. Only six provisions apply partially binding language regarding these commitments, while 22 provisions use endeavor and/or recognition language without establishing binding commitments. The AfCFTA Digital Trade Protocol (2024, yet to enter into force) stands apart given its dedicated Annex on electronic payments, covering competition, interoperability, access, consumer protection, and settlement systems.

While the Jordan-US Joint Statement (2001) included an early reference to electronic payments, the Australia-Singapore DEA (2020) established the first comprehensive provision. The UK-Singapore DEA (2022) introduced the most detailed formulation, covering regulatory transparency, open access, and standards. UAE bilateral agreements contributed significantly from 2022 onward.

The WTO Agreement on Electronic Commerce, which is yet to enter into force, includes binding language regarding paperless trading for the customs authority and non-binding language for other authorities.

The US has not adopted a dedicated electronic payments provision beyond the early Jordan-US reference, while China and the EU entered into their first electronic payments provisions in 2025.

Electronic invoicing

Electronic invoicing provisions comprise 38 provisions across 38 agreements, negotiated since 2019 and covering 126 jurisdictions. Provisions recognize the importance of electronic invoicing for the efficiency and reliability of commercial transactions and commit parties to promote cross-border interoperability of electronic invoicing systems. Eighteen provisions use at least one binding language element, combined with endeavors. Specifically, 11 agreements use binding "shall ensure" language regarding the interoperability commitment, while 18 provisions are limited to endeavor/consider language, commonly following a UAE-originated formulation. Two agreements only contain a recognition.

The New Zealand-Singapore CEP Upgrade (2019) established the first electronic invoicing provision. The Australia-Singapore DEA (2020) introduced the recognition-interoperability-cooperation structure that has become a common template. The AfCFTA Digital Trade Protocol (2024, yet to enter into force) extended coverage to 54 African jurisdictions. The US has not adopted any electronic invoicing provisions, while China entered into its first electronic invoicing commitment in 2025, through the ASEAN-China FTA 3.0, which is yet to enter into force.

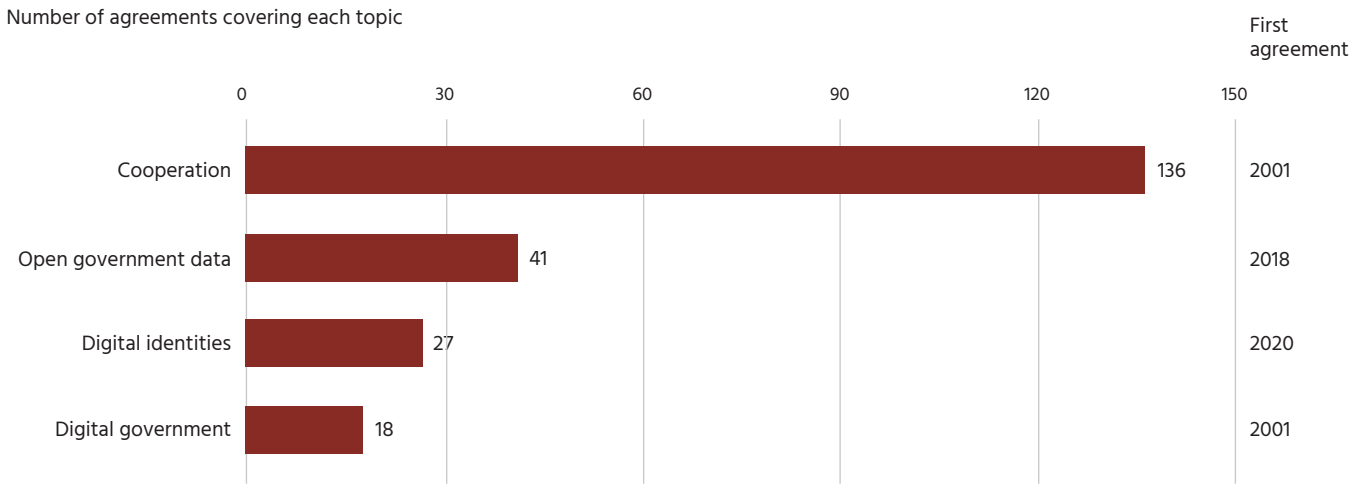
Paperless trading

Paperless trading or trade facilitation with digital means provisions comprise 116 provisions across 102 agreements, covering 142 jurisdictions. The core commitment requires parties to accept trade administration documents submitted electronically as the legal equivalent of their paper versions. Seventy-three provisions use endeavor language, while 24 provisions establish a binding "shall" commitment. Notably, the WTO Agreement on Electronic Commerce, which is yet to enter into force, includes binding language regarding paperless trading for the customs authority and non-binding language for other authorities. In addition, several provisions commit parties to make trade administration documents available in electronic form, with some mentioning single windows and electronic records.

The Australia-Singapore FTA (2003) established the first paperless trading provision, while the Australia-Singapore DEA (2020) introduced a detailed approach with electronic records and single-window commitments. The CPTPP (2018) codified the "endeavor to accept" template which is widely followed to date. The US, the EU, China, and India all participate in at least one provision and the AfCFTA extended coverage to 54 African jurisdictions in 2024 (yet to enter into force).

Section F: Digital government

Figure 9 – Digital government commitments



Source: Digital Policy Alert

Cooperation provisions comprise 177 provisions across 136 agreements, covering 163 jurisdictions — the broadest coverage of any digital trade commitment.

Digital government provisions include provisions on cooperation, open government data, digital government, cooperation, and digital identities. These provisions are novel, with the exception of cooperation, but governments find common ground on them with more ease.

Cooperation

Cooperation provisions comprise 177 provisions across 136 agreements, covering 163 jurisdictions — the broadest coverage of any digital trade commitment. They commit parties to cooperate on digital trade matters through information exchange, capacity building, dialogue, and joint activities. The subject matters of cooperation spans all areas of digital trade: The most frequently addressed topics are consumer protection, unsolicited commercial electronic messages, cybersecurity, and electronic authentication, among others. Formulations range from “shall cooperate” and “shall endeavor” to softer “shall consider” and “may cooperate” language.

The Jordan-US Joint Statement on Electronic Commerce (2001) established the first cooperation provision. Over time, cooperation articles evolved from broad, omnibus clauses to increasingly specialized provisions dedicated to specific topics. The CPTPP (2018) introduced the dual-article approach, combining a general cooperation provision with a dedicated cybersecurity article focused on

The AfCFTA Digital Trade Protocol (2024, yet to enter into force) includes a unique open government data provision focused on "data for development", aiming to foster Africa's data ecosystem to drive development and growth across the continent.

cooperation, which is widely replicated to date. All major economies participate in at least one cooperation provision.

Open government data

Open government data provisions comprise 43 provisions across 41 agreements, covering 124 jurisdictions. Provisions recognize that facilitating public access to government information fosters economic and social development, and commit parties to make government data available in machine-readable and open formats. Provisions often additionally commit parties to cooperate on expanding access with a view to generating business opportunities for SMEs. Eleven provisions follow an expanded formulation requiring parties to endeavor to avoid imposing conditions that prevent reproduction, redistribution, or commercial reuse of data. Several additionally include a cost commitment (no or reasonable charge to users), and two add a formal definition of metadata. EU agreements further require that use conditions be non-discriminatory and that data be made available in compliance with personal data protection rules.

The USMCA (2018) established the first open government data provision, replicated in the US-Japan Digital Trade Agreement (2019). UAE bilateral agreements proliferated from 2022 onwards, currently comprising 17 provisions. The AfCFTA Digital Trade Protocol (2024, yet to enter into force) includes a unique provision focused on "data for development", aiming to foster Africa's data ecosystem to drive development and growth across the continent. China has not adopted open government data provisions.

Open government data provisions recognize that facilitating public access to government information fosters economic and social development.

To date, the commitment to develop and implement digital transformation strategies is driven overwhelmingly by the UAE, which participates in 15 of 18 provisions.

Digital government

Digital government provisions comprise 18 provisions across 18 agreements, covering 28 jurisdictions. Provisions recognize that technology enables more efficient government operations and commit parties to develop strategies for digital transformation, including through open government processes, emerging technologies, digital platforms, and digital skills. Several provisions also address data governance and the use of AI in public service delivery. Alongside the commitments to develop strategies for digital transformation, most provisions include a dedicated cooperation framework covering the exchange of best practices, information sharing, and capacity building through training and exchange of officials. The core commitment is formulated in binding "shall endeavor" language to develop and implement digital transformation strategies.

To date, the commitment is driven overwhelmingly by the UAE, which participates in 15 of 18 provisions. The India-UAE CEPA (2022) established the modern template. The Jordan-US Joint Statement on Electronic Commerce (2001) included the earliest reference to such digital government. However, the US has not adopted dedicated digital government provisions beyond this early reference. The EU and China have entered no digital government commitments.

Digital identities

Digital identities provisions comprise 33 provisions across 27 agreements, covering 89 jurisdictions. They recognize the importance of digital identities for regional and global connectivity, acknowledge the diversity of legal and technical approaches, and commit parties to promote compatibility and interoperability between digital identity regimes. Twenty provisions use the India-UAE CEPA (2022) template, incorporating "shall endeavor" language to pursue compatibility mechanisms and including cooperation sub-paragraphs on frameworks, standards, mutual recognition, and knowledge exchange. Four other provisions follow the Australia-Singapore DEA (2020) template, focused on developing mechanisms for compatibility.

The Australia-Singapore DEA and DEPA (2020) established the first digital identities provision. The AfCFTA Digital Trade Protocol (2024, yet to enter into force) includes the most comprehensive framework, with a dedicated Annex on digital identities covering definitions, principles, standards, trust services, cross-border recognition, and competent authorities. The spread of these commitments is driven primarily by the UAE's bilateral negotiations, totaling 14, and the AfCFTA, 54-member breadth. The US has not adopted dedicated digital identities provisions, while China entered into its first digital identities commitment in 2025.

Methodological note

This note explains the scope of our analysis, as well as our heuristics in creating counts.

Our scope includes FTAs with dedicated electronic commerce chapters as well as stand-alone digital economy/trade/partnership agreements.[9] This includes:

- 20 agreements that are yet to enter into force, as long as their text was publicly available at the time of writing.[10] In the introduction, we count all provisions, to provide historical context. In Sections A–F, we include only the newest version for counts, but mention formulations in previous versions, when they are relevant for "evolution" sections.

- Four agreements that insert or amend digital trade chapters in existing FTAs between the same parties. We include these agreements in all counts, but clarify that they are yet to enter into force when they are mentioned in " evolution" sections.

We provide four types of counts throughout the report: provisions, agreements, jurisdictions, and formulations.

- We differentiate between the number of provisions and the number of agreements, since one agreement may contain more than one provision on a given topic. In Sections A–F, we open each topical section with counts for both provisions and agreements, then we focus on provision counts.

- When counting jurisdictions, we do not include the WTO E-Commerce Agreement, since it is not yet clear which governments will participate. As of December 2025, 72 governments co-sponsor the agreement, but this figure is dynamic and has fallen from the initial 91 negotiating governments. For the AfCFTA Digital Trade Protocol, we count 54 jurisdictions, reflecting the absence of Eritrea.[11]

- When providing counts for formulations, we strike a balance between simplicity and comprehensiveness: The sum of our formulation counts does not add up to the total provision count by design. Rather than describing every single idiosyncratic formulation, we outline and count the mainly used formulations, and provide a comprehensive Annex.

The Annex provides the full dataset underlying Sections A–F of this report, including the full text of all relevant provisions. Please contact the Digital Policy Alert team for further discussions on its available resources and analysis.

Author bios: Tommaso Giardini and Vladislav Alifirov

Tommaso Giardini is the Associate Director of the Digital Policy Alert, the world's largest open-access database on digital policy developments. The Digital Policy Alert provides daily updates on government regulation of the digital economy, including AI, social media, and e-commerce, across 50 countries. Tommaso's research compares how governments implement international commitments, including digital trade commitments and the OECD AI Principles.

Vladislav Alifirov is a Trade Policy Analyst at Global Trade Alert (GTA), a publicly accessible, independent, fact-based record that tracks trade and industrial policy developments in more than 60 markets. The GTA is an initiative of the Swiss-based St.Gallen Endowment for Prosperity Through Trade, a neutral, not-for-profit organization dedicated to increasing transparency of global policies affecting the digital economy, trade, and investment.

Endnotes

1. In this report, “trade agreements” includes both FTAs with dedicated electronic commerce chapters and stand-alone digital economy/trade/partnership agreements. To ease reading flow, we use the term FTAs to encompass all these forms of agreements.

2. The Annex provides the dataset underlying Sections A-F of this report, including the full text of all relevant provisions. Readers that wish to deepen their analysis can contact Digital Policy Alert, including for access to the Clairk tool.

3. Digital Policy Alert was established in 2021 by the St.Gallen Endowment for Prosperity Through Trade. It complements the Endowment’s Global Trade Alert, which has monitored state interventions affecting global commerce since 2009.

4. Not all topics follow this simplified lifecycle: In some, such as source code, provisions used binding language from the start, while in others, such as cybersecurity, language remains non-binding to date.

5. Going forward, we refer to “shall” language as “binding commitment”, “shall endeavor” language as “non-binding commitment”, and “recognition” language as such “recognition.”

6. AI commitments are also found in broader provisions on emerging technologies, digital government, and cooperation, which we do not analyze in this section.

7. Some provisions define terms, specifically cryptography (principles for transforming data to hide content or prevent unauthorized use through secret parameters); encryption (conversion of plaintext to ciphertext); cryptographic algorithm or cipher (mathematical procedures combining keys with plaintext); and key (parameters determining algorithm operations).

8. We do not analyze provisions focusing specifically on financial services. They oblige parties not to require financial service suppliers to use or locate computing facilities in their territory as a condition for conducting business, so long as the party’s financial regulatory authorities have access to information on computing facilities located outside the territory.

9. Provisions on artificial intelligence located outside electronic commerce chapters, such as Art. 20.4 of the Australia-UK FTA, are not analyzed. See the TAPED dataset for systematic information on digital trade commitments outside electronic commerce chapters.

10. The text for various Comprehensive Economic Partnership Agreements between the UAE and trading partners, especially in Africa, is not yet available and they are thus not included in the analysis.

11. The Digital Trade Protocol, adopted in February 2024, and its Annexes, adopted in February 2025, are yet to enter into force, while the AfCFTA itself has reached the threshold for ratifications.

hinrich foundation

advancing sustainable global trade

The Hinrich Foundation is an Asia-based philanthropic organization dedicated to advancing mutually beneficial and sustainable global trade.

We believe that global trade – when mutually beneficial and sustainable – is a powerful force for shared prosperity, technological progress, sustainability and peaceful international cooperation.

Our work is grounded in independent, fact-based research and the development of innovative trade education programs.

CONTACT US

There are many ways you can help advance sustainable global trade. Share our research, participate in our events or partner with us in our programs.

inquiry@hinrichfoundation.com

Subscribe to our newsletter for the latest global trade research

hinrichfoundation.com

hinrich foundation
hinrichfdn
hinrichfoundation
hinrichfoundation

Disclaimer:

The Hinrich Foundation is a philanthropic organization that works to advance mutually beneficial and sustainable global trade through original research and education programs that build understanding and leadership in global trade. The Foundation does not accept external funding and operates a 501(c)(3) corporation in the US and a company in Singapore exclusively for charitable and educational purposes.
 All statements of fact and the views, conclusions and recommendations expressed in the publications of the Foundation are the sole responsibility of the author(s).