



**TRADE JUSTICE
MOVEMENT**



The price of the deal:

Potential implications for UK technology regulation from a UK-US digital trade agreement

October 2026

Daniel Rangel Jurado



Contents

Executive summary	3
1. Introduction	5
2. Overview of US-style digital trade provisions	7
2.1. Non-discrimination for digital products and services – and the arrival of explicit DST bans	8
2.2. Source code and algorithm secrecy protections	10
2.3. Data localisation and cross-border transfer requirements	12
2.4. Key takeaways	14
3. Implications of US-style digital trade provisions for UK technology regulation	15
3.1. The Digital Services Tax	15
3.2. Digital competition regulation: the DMCCA	17
3.3. AI governance	18
3.4. The Online Safety Act	20
3.5. The UK GDPR and the protection of personal data	21
3.6. Child protection: the under-16 ban, nudification tools, and AI-generated CSAM	22
Conclusion	24
List of acronyms	25
References	26

Front cover photo: President Donald J. Trump hosts a luncheon on Super Intelligence (AI) in the East Room of the White House, Tuesday, September 29, 2026. (Official White House Photo by Daniel Torok)

Executive summary

The United Kingdom has spent the past half-decade building a regulatory architecture for the digital economy: a digital services tax, a bespoke digital competition regime under the Digital Markets, Competition and Consumers Act (DMCCA), the Online Safety Act's platform accountability system, data protections that follow personal information across borders, newly enacted offences targeting AI-enabled abuse, and an emerging framework for governing artificial intelligence. At the same time, previous UK governments pursued a digital trade agreement with a United States administration that has made the dismantling of foreign technology regulation an explicit objective of its trade policy. Those negotiations stalled in late 2025; whether the Burnham government resumes them is an open question. This report examines what is at stake if it does.

The report's central argument is that US-style digital trade provisions – non-discrimination rules for digital products and services, source code and algorithm secrecy protections, and disciplines on data localisation and cross-border data transfers – could significantly undercut the policy space the UK requires to regulate digital markets and technologies. The UK has already accepted versions of these provisions through the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and several bilateral agreements. But an agreement with the United States would be categorically different: US firms dominate the regulated markets, so even formally reciprocal commitments would in practice bind only the UK. Moreover, recent US agreements covering digital trade are more aggressive than anything the UK has yet signed; and the United States today acts as rule-maker, judge, and enforcer at once, leaving no independent tribunal between a commitment and its enforcement.

The report's key findings are as follows:

- **Digital trade provisions have grown steadily more expansive.** Across three generations of texts – CPTPP, US-Mexico-Canada Agreement (USMCA), and the second Trump administration's "agreements on reciprocal trade" (ARTs) – definitional limits have been dropped, triggers widened from the sale of products to the conduct of business, public policy exceptions narrowed or removed, and subject matter extended into taxation. The ARTs abandon even the appearance of mutuality, placing obligations only on the US's trading partners.
- **The Digital Services Tax is the most immediately exposed measure.** The ART template includes an express prohibition on DSTs "or similar taxes" that discriminate "in law or in fact". Even without an express ban, the DST's exposure would turn on whether the agreement included non-discrimination obligations covering US digital goods and services. Canada's experience, having rescinded its DST under tariff threat, shows that without a tribunal, the commitment can mean whatever Washington says it means.

- **The DMCCA's designation regime supplies the starting point for a discrimination claim.** The two firms designated to date with strategic market status are American. That reflects the structure of the markets. But under a de facto discrimination standard following the US template, the composition of the register could be presented as evidence of targeting, while conduct requirements on defaults, rankings, and data access could be characterised as according “less favourable treatment” to US products.
- **AI legislation would be constrained before it is written.** Proposals under discussion – mandatory pre-deployment testing, third-party audits, explainability duties – would operate ex ante, across a class of developers, and require access to algorithmic information. Each feature places them outside the case-specific regulatory exception that runs through every US-model digital trade agreement text, which permits compelled access only for “a specific investigation, inspection, examination, enforcement action, or judicial proceeding”.
- **The Online Safety Act's supervisory model sits on the wrong side of that same line.** Ofcom's audit powers expressly reach “algorithms of a specified description” and can be exercised to assess risk without any suspicion of a breach. The statute's proactive design premise – continuous supervision rather than reactive enforcement – and its authorisation to engage external evaluators are at odds with source code and algorithm secrecy provisions in modern digital trade agreements.
- **Data transfer regulation would be constrained at its core.** The ART model replaces negative disciplines with a positive undertaking: partners such as Indonesia and Argentina have committed to recognise the United States as an adequate jurisdiction under their own data privacy law. An equivalent UK commitment would pre-empt the Secretary of State's statutory assessment required before approving personal data transfers to any jurisdiction and freeze that judgement against future changes in US law and practice. Significantly, it could also place at risk the UK's own adequacy status under EU law.
- **Even child protection measures could depend on US forbearance.** No trade provision targets the under-16 social media restrictions or the Crime and Policing Act 2026's new offences specifically. But the dominance of US firms in digital markets facilitates claims of discrimination against policies that particularly affect their business models.

The report concludes that a UK-US digital trade agreement resembling the current US templates would convert the UK's technology statutes from sovereign choices into matters of ongoing US sufferance, and that entering such a negotiation is too risky under present conditions. It identifies the provisions that would do most damage – non-discrimination obligations covering digital products and services, source code and algorithm secrecy protections, and commitments to recognise the United States as an adequate jurisdiction for data transfers – and argues that the more useful course is to revisit the digital trade commitments the UK has already made rather than to add to them.



1. Introduction

The defining regulatory challenge of the coming decade is how democratic governments respond to the concentration of economic and social power in a handful of digital firms. The United Kingdom has begun to assemble its response: a Digital Services Tax to address the mismatch between where digital revenues are earned and where they are taxed; the Digital Markets, Competition and Consumers Act to constrain the market power of the largest platforms; the Online Safety Act to hold digital services accountable for harms to their users; personal data protections that should not expire once information is transferred to servers abroad; and an ongoing debate over binding rules for artificial intelligence, age limits for social media, and the misuse of generative AI tools.

Yet just as this regulatory architecture takes shape – and just as Prime Minister Andy Burnham’s new government takes office, having promised “strong public control” over industry, including AI¹ – the UK is emerging from a period in which successive governments were adamant about adopting so-called digital trade rules, whose purpose is to demarcate what governments can and cannot do in regulating digital markets and technologies. The previous government, moreover, actively pursued a digital trade agreement with the United States specifically,² even as the current US administration has made the dismantling of technology regulation by its trading partners an explicit objective of its trade policy.

This report argues that digital trade rules as a category – particularly, provisions on non-discrimination for digital products and services, source code and algorithm secrecy protections, and disciplines on data localisation and cross-border data flows – could significantly undercut the policy space governments require to regulate markets and technologies in the digital era. These provisions are typically drafted so broadly as to reach far beyond their purported purpose of preventing protectionism, and the UK has already signed up to versions of them through its accession to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the conclusion of several other trade agreements with digital trade or e-commerce chapters. But undertaking such commitments with the United States is a categorically different proposition, for two reasons. First, US firms dominate the markets targeted by these regulations, meaning they would be the principal regulated entities under any UK digital tax, online competition regime, or AI governance framework. As a result, any trade provision limiting regulation of the digital sector would, even if formally applicable to both the UK and the US, in practice primarily constrain the UK. Second, the US-style provisions now on offer are more aggressive than anything the UK has previously signed, including explicit prohibitions on digital services taxes. Trade agreements are never drafted from tabula rasa. They are often based on previous agreements concluded by the parties, and typically the party with greater economic clout has greater influence over the negotiating agenda and the resulting text. This is why the trend under the second Trump administration of expanding the scope of digital trade rules while making them applicable only to its trading partners should raise serious concerns for the UK.

However, the danger today is not primarily that the UK could lose disputes decided by an independent tribunal, as trade disputes have traditionally been resolved. Rather, the main risk presently is that these commitments would operate before any dispute arises, chilling regulatory ambition as UK policymakers pre-emptively narrow, weaken, or shelve measures to avoid confrontation – or as Washington uses the rules to bolster unilateral efforts to undermine tech regulation initiatives.

The report proceeds in two main parts. Section 2 provides an overview of US-style digital trade provisions – non-discrimination rules for digital products and services (including explicit bans on digital services taxes), source code and algorithm secrecy protections, and rules on data localisation and cross-border data transfers – comparing traditional free trade agreement language with the more aggressive model advanced in the second Trump administration’s “Agreements on Reciprocal Trade”. Section 3 examines how these provisions could be leveraged against existing and prospective UK policies across six areas: the Digital Services Tax; digital competition regulation under the Digital Markets, Competition and Consumers Act; AI governance; the Online Safety Act’s platform-accountability enforcement system; the cross-border data-transfer regime under the UK General Data Protection Regulation; and restrictions on under-16 social media use, nudification apps, and AI-generated child sexual abuse material. Throughout, the report situates these risks within the current enforcement environment, arguing that the concentration of rule-making, adjudication and punishment in the Office of the US Trade Representative – template drafter, judge of compliance and enforcer through unilateral tariffs – means that any digital trade commitment made to the United States today is a commitment made without the safeguards of independent adjudication on which the trading system has traditionally relied. A concluding section draws out the implications for UK policymakers.

2. Overview of US-style digital trade provisions

Digital trade chapters are conventionally presented as a set of trade facilitation measures: rules that keep data moving, reduce regulatory burdens for electronic transactions, and stop governments from favouring domestic suppliers. While some rules included in digital trade agreements³ aim to facilitate commerce by, for instance, harmonising requirements for electronic documents or signatures, the most consequential provisions in these agreements have considerably more far-reaching implications. In practice, three families of provisions pose the most acute risks to states' regulatory independence: non-discrimination rules for digital products and services; protections for source code and algorithms against disclosure requirements; and disciplines governing data localisation and cross-border data transfers. This section examines each in turn, comparing the language the United Kingdom has already accepted through its CPTPP accession, the high-water mark of current US free trade agreement practice in the US-Mexico-Canada Agreement (USMCA), and the model advanced by the second Trump administration through its Agreements on Reciprocal Trade (ARTs).

Before turning to the comparison, it is worth contextualising the emergence of ARTs in international trade dealmaking. By imposing a set of global tariffs under the International Emergency Economic Powers Act (IEEPA) in April 2025, the Trump administration was able to bring many countries to the negotiating table to sign a new type of agreement. Unlike free trade agreements (FTAs), Agreements on Reciprocal Trade do not require reciprocal trade liberalisation between the parties, nor do they establish regulatory frameworks that apply equally to all signatories. Instead, ARTs memorialise predominantly unilateral commitments by US trading partners, many of which reflect longstanding deregulatory priorities of US corporate interests. Another key difference is that traditional FTAs include a dispute settlement chapter that typically provides for an independent panel of trade experts to adjudicate disputes between the parties. Where a panel finds a violation, the prevailing party is normally authorised to suspend concessions, including by imposing tariffs on the non-conforming party's exports. By contrast, the ARTs promoted by the second Trump administration contain a single "Enforcement" article that authorises unilateral action under domestic law where one party considers that the other has failed to comply with its obligations under the agreement.

This provision must be read in light of the recent active use by the US government of Section 301 of the Trade Act of 1974. Section 301 empowers the United States to unilaterally suspend or withdraw benefits under trade agreements or impose duties or other import restrictions on foreign goods and services where the US Trade Representative determines that measures adopted by another state violate its trade commitments, are unjustifiable or discriminatory, and burden or restrict US commerce. In this context, signing an ART serves to embolden the US

government to pressure and unilaterally sanction countries, rather than taking action via traditional dispute settlement mechanisms.

So far, 10 countries have signed this type of agreement with the United States.⁴

2.1 Non-discrimination for digital products and services – and the arrival of explicit DST bans

Non-discrimination is one of the oldest ideas in international trade law: a government may regulate as it wishes, so long as it does not treat foreign products worse than their domestic or third-country equivalents. The principle underlying this rule is that countries want to ensure that their liberalisation commitments are not undermined by policies that ultimately favour domestic or third-country products. However, when applied to digital trade, this commitment carries far greater weight than this familiar framing suggests, because discrimination in contemporary trade law is not confined to measures that expressly distinguish between foreign and domestic firms or products, or that constitute disguised protectionism. Unless a specific provision clarifies that a finding of discrimination requires protectionist intent, a facially neutral measure may nevertheless be considered discriminatory if it modifies the conditions of competition to the detriment of the other party's products or suppliers. This is known in international trade law as *de facto* discrimination.

In digital markets, where a handful of US firms hold dominant positions across search, social media, operating systems, app stores, cloud services, and AI, this doctrine has a structural consequence: almost any regulation aimed at market power, scale, or systemic risk will, in practice, fall most heavily on those firms. Revenue thresholds, user-number thresholds, gatekeeper designations and tiered obligations – the standard tools legislatures use to focus obligations on the largest actors and spare smaller ones – all tend to place the greatest regulatory burden on US firms that can be characterised as *de facto* discrimination. Thus, when a country binds itself to non-discrimination obligations covering digital markets with the United States, market dominance itself can become a legal shield for large, concentrated firms: the more concentrated the market, the harder it becomes to regulate it without providing grounds for a trade claim.

The only agreement the UK has entered into that contains non-discrimination obligations covering digital products is the CPTPP,⁵ whose text had already been negotiated before the UK's accession. Beyond that agreement, the UK government has deliberately declined to include such provisions in its other digital trade agreements. It even explicitly told Japan, in the context of a meeting of the Committee on Trade in Services, Investment Liberalisation and Electronic Commerce under the Comprehensive Economic Partnership Agreement between Japan and the United Kingdom (UK-Japan CEPA), that it did not intend to include non-discrimination provisions for digital products in its bilateral agreements.⁶

Yet it is unclear whether the UK could resist US demands to include such a clause in a potential UK-US digital trade agreement. During the first Trump administration, the US government negotiated two agreements containing digital trade rules: the USMCA and the US–Japan Digital Trade Agreement, which had almost identical formulations of non-discrimination rules for digital products.⁷ Perhaps more importantly, the ARTs promoted by the second Trump administration have so far all included non-discrimination obligations covering digital markets, which go even further than these precedents.

The table below compares the CPTPP and USMCA templates with the ART model for digital non-discrimination provisions:⁸

Table 1. Digital Non-Discrimination: treaty language compared

	CPTPP Art. 14.4: Non-Discriminatory Treatment of Digital Products	USMCA Art. 19.4: Non-Discriminatory Treatment of Digital Products	US-Argentina ART Art. 3.2.1: Facilitation of Digital Trade
Core prohibition	“No Party shall accord less favourable treatment to digital products created, produced, published, contracted for, commissioned or first made available on commercial terms in the territory of another Party, or to digital products of which the author, performer, producer, developer or owner is a person of another Party, than it accords to other like digital products”. (para. 1)	“No Party shall accord less favourable treatment to digital products created, produced, published, contracted for, commissioned or first made available on commercial terms in the territory of another Party, or to digital products of which the author, performer, producer, developer or owner is a person of another Party, than it accords to other like digital products”. (para. 1)	“Argentina shall facilitate digital trade with the United States, including by refraining from measures that discriminate against US digital services or products distributed digitally. The Parties shall collaborate to address cybersecurity challenges”. (para. 1)

The non-discrimination provisions for digital products in CPTPP and USMCA are closely related – unsurprisingly, since both descend from language the United States developed.⁹ Each imposes a general obligation to treat digital products of the other parties no less favourably than comparable domestic ones, and each extends, on standard non-discrimination reasoning, to measures that discriminate in effect as well as on their face. Notably, unlike older formulations of non-discrimination obligations, CPTPP and USMCA do not require determining whether an origin-neutral policy – that is, one that does not differentiate based on origin but may have a disparate effect – was adopted with the objective of protecting domestic competitors.¹⁰ By contrast, simply showing that a challenged policy negatively affects the conditions of competition for foreign products relative to like domestic or third-country products could be sufficient to establish a violation. In this respect, the CPTPP and USMCA are equally expansive.

There is, however, an important difference between them. CPTPP Article 14.4 obliges each Party to accord no less favourable treatment to “digital products created, produced, published, contracted for, commissioned or first made available

on commercial terms in the territory of another Party”; USMCA Article 19.4 uses the same formula but in the singular – “a digital product”. Legal scholar Simon Lester noticed the switch, framing it as a question about policy space rather than drafting tidiness.¹¹ The plural wording suggests a comparison between groups: to establish a breach, a complaining government would need to show that foreign digital products as a class fare worse than comparable domestic ones. The singular wording lowers that bar considerably, since a claim can rest on a single product treated less favourably than a single comparable product.

Now, the ART model is even more expansive: the obligation is recast to cover discrimination against US digital services as well as products distributed digitally, without any definitional limits or carve-outs. This means that the United States could more easily argue that the provision covers not only the content carried by online platforms, but the platforms themselves. Moreover, the ART model gives no guidance on the comparator against which discrimination is to be assessed. CPTPP and USMCA at least specify one: treatment no less favourable than that accorded “other like digital products”. The ART text supplies nothing equivalent. The partner simply undertakes to refrain “from measures that discriminate against US digital services or products distributed digitally” – without indicating whether the benchmark is domestic suppliers, suppliers of third countries, or neither. Discrimination is a relational concept, and a prohibition that never identifies the relation leaves ample room for the United States to determine what counts as discriminatory.

Additionally, the ARTs promoted by the second Trump administration force a commitment on the trading partner “not to impose digital services taxes, or similar taxes, that discriminate against US companies in law or in fact”.¹² This means that a facially neutral measure that captures predominantly US firms – as revenue-threshold digital tax regimes generally do – would be immediately exposed to challenge.

In sum, the steady expansion of non-discrimination rules – from digital products to digital services, from facially discriminatory measures and those adopted with protectionist intent to measures discriminatory in effect, and now into taxation – severely narrows the scope for governments to regulate an industry whose leading firms are overwhelmingly American. The more effectively a measure targets concentrated market power, the more readily it can be characterised as discrimination.

2.2 Source code and algorithm secrecy protections

Source code provisions prohibit governments from requiring a firm to hand over, or give access to, the underlying code of its software – and, in later versions, the algorithms that code expresses – as a condition of selling or operating in the market. Presented as a defence against forced technology transfer, they are in fact a restriction on the central instrument of technology regulation. Nearly every regulatory approach to algorithmic systems, from AI frameworks to platform

accountability regimes and algorithmic auditing, depends at some point on a public authority being able to look inside the system. Trade secrecy is already protected multilaterally under the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS);¹³ what these provisions add is a limit on what democratically enacted regulation may require of firms operating lawfully in the jurisdiction.

The obligation has widened with each generation of text, and the widening is best seen in the language itself.

Table 2. Source code and algorithm provisions: treaty language compared

	CPTPP, Art. 14.17: Source Code	USMCA, Art. 19.16: Source Code	US-Argentina ART Art. 3.2
Core prohibition	"No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory". (para. 1)	"No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory". (para. 1)	"Argentina shall not impose any condition or enforce any undertaking requiring US persons to transfer or provide access to a particular technology, production process, source code, or other proprietary knowledge, or to purchase, utilize, or accord a preference to a particular technology, as a condition for doing business in its territory". (para. 2)
Limitation on covered software	"For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure". (para. 2)	None.	None.
Regulatory access	No express provision. Para. 3(b) preserves only "a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement".	"This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure". (para. 2)	Identical wording to USMCA para. 2, applied to "a person of the other Party".

Three shifts are visible across the columns. First, the limits on covered software disappear: CPTPP confines the prohibition to mass-market software and excludes software used for critical infrastructure, preserving the ability to inspect code running power grids and payment systems; neither of the later texts does so. Second, the trigger widens. CPTPP and USMCA apply to conditions imposed on the import, distribution, sale, or use of software, whereas the ART formulation applies to any condition for doing business in the territory, which could be interpreted as a more catch-all formulation. Third, the protected subject matter expands, from source code alone in CPTPP, to algorithms expressed in source code in USMCA, to the broader and vaguer category of “a particular technology, production process, source code, or other proprietary knowledge” in the newer ART model.

Regarding the regulatory access exception, notably, CPTPP does not contemplate the possibility that regulatory authorities may need access to source code to perform their functions. USMCA and the ART texts do include such a guarantee, but only in very limited terms. Disclosure may be required only for “a specific investigation, inspection, examination, enforcement action, or judicial proceeding” – a backward-looking, particularised exception that applies only once a regulator is pursuing an identified matter involving an identified firm. That is not how emerging AI regulation regimes are structured. Their characteristic instruments are prospective and systemic: standing transparency obligations imposed on a class of providers, external testing before deployment, periodic sector-wide audits, and mandated researcher access.¹⁴ None of these fits comfortably within the category of a specific investigation or enforcement action.

2.3 Data localisation and cross-border transfer requirements

Data provisions in digital trade agreements typically have two objectives: they oblige governments to allow data to move across borders for business purposes, and they prohibit requiring firms to store or process data on local servers as a condition of operating in the market. Obligations of this kind carry significant implications for data privacy legislation. Privacy regimes restrict cross-border transfers not to protect domestic industry but because data protection is only as strong as the weakest jurisdiction the data reaches. Adequacy assessments, standard contractual clauses and transfer impact assessments all exist to keep protections attached to data as it moves.¹⁵ Localisation rules also serve interests well beyond privacy, including enabling financial supervisors and tax authorities to access records, as well as addressing national security and resilience concerns that lead states to keep certain workloads onshore.¹⁶

As shown in the table below, the obligations in the CPTPP and USMCA are broadly similar. What distinguishes them is the room they leave for competing public policy objectives. The ART model, exemplified here by the US–Indonesia ART, adopts an altogether different structure.¹⁷

Table 3. Cross-border data flows and localisation: treaty language compared

	CPTPP, Art. 14.11: Cross-Border Transfer of Information by Electronic Means and Art. 14.13: Location of Computing Facilities	USMCA, Art. 19.11: Cross-Border Transfer of Information by Electronic Means and Art. 19.12: Location of Computing Facilities	US–Indonesia ART, Art. 3.2: Facilitation of Digital Trade and Annex III, Article 3.2: Data Transfers
Cross-border transfers	“Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person”. (Art. 14.11(2))	“No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person”. (Art. 19.11(1))	“Indonesia shall facilitate digital trade with the United States, including by [...] ensuring the transfer of data by electronic means across trusted borders with appropriate protection for the conduct of business”. (Art. 3.2(b)) “Indonesia shall provide certainty regarding the ability to move personal data out of its territory to the United States by recognizing the United States as a country or jurisdiction that provides adequate data protection under Indonesia’s law”. (Annex III, Art. 3.2)
Localisation	“No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory”. (Art. 14.13(2))	“No Party shall require a covered person to use or locate computing facilities in that Party’s territory as a condition for conducting business in that territory”. (Art. 19.12, in full)	No general provision. Sector-specific instead: e.g. “Indonesia shall refrain from imposing requirements to process data onshore, particularly in the financial space, provided the country’s authorities have, for regulatory and supervisory purposes, immediate, direct, complete, and ongoing access to the information processed or stored outside Indonesia’s territory” (Annex III, Art. 2.29(1))

Regarding the data-transfer obligations in these agreements, it is worth noting that the CPTPP adopts a positive obligation: each Party “shall allow” the cross-border transfer of information, including personal information, when carried out for the conduct of business. The USMCA turns that formulation around: no Party “shall prohibit or restrict” such transfers. The USMCA obligation is arguably broader. A duty to allow transfers applies to measures that block them; a prohibition on restricting transfers reaches any measure that makes transfers more difficult,

potentially bringing conditions and procedural requirements that fall well short of an outright block within its scope.¹⁸ The US–Indonesia ART returns to a positive formulation – although, like most commitments in the ART model, a non-reciprocal one – obliging Indonesia to “ensure the transfer of data by electronic means across trusted borders with appropriate protection for the conduct of business”. This is closer in form to the CPTPP provision, although key terms remain undefined.

Additionally, both CPTPP and USMCA ban data localisation requirements, including policies that require data to be processed onshore. The US–Indonesia ART, instead of containing a general data-localisation provision, identifies specific sectors, such as financial services, in which Indonesia is required to refrain from imposing onshore data-processing requirements.

Finally, it is worth noting that CPTPP subjects both disciplines to a legitimate public policy objective exception with a proportionality test. The USMCA retains that exception for data transfers but removes it entirely for data localisation. The US–Indonesia ART contains no equivalent exception. In any event, limiting conditions such as the proportionality test, or the requirement to demonstrate that a challenged measure is neither a means of arbitrary or unjustifiable discrimination nor a disguised restriction on trade, substantially constrain the potential effectiveness of the exceptions in both the CPTPP and USMCA.¹⁹

Beyond these textual differences, the objective of these provisions is broadly the same: to facilitate unfettered cross-border data transfers and limit the regulatory capacity of states to impose conditions or restrictions on such transfers. Moreover, rules on cross-border data flows and localisation can subordinate data privacy regimes to the commercial imperatives of trade agreements. The US–Indonesia text makes this particularly clear by obliging Indonesia to recognise the United States as providing an adequate level of data protection under its own law.

2.4 Key takeaways

Taken together, these three families of digital trade provisions show a consistent trajectory. Definitional limits have been dropped, triggers widened from the sale of products to the conduct of business, exceptions narrowed or removed, and subject matter extended into taxation and, through the adequacy undertakings, into positive commitments about how a partner exercises its own regulatory judgement. The Agreements on Reciprocal Trade complete the pattern by abandoning even the appearance of mutuality: their obligations are drafted as duties owed by the partner to the United States, unaccompanied by schedules, reservations or the public policy exceptions that qualified the earlier texts. Having traced that evolution, the report turns to what it would mean in practice for the UK to negotiate and sign a digital trade agreement with the United States and, more broadly, to the tensions between digital trade rules and domestic regulatory priorities.

3. Implications of US-style digital trade provisions for UK technology regulation

The UK and US have been engaged in “discussions toward a transformative technology partnership”²⁰ since at least May 2025. This section applies the provisions examined in Section 2 to six areas of UK technology policy: the Digital Services Tax, digital competition regulation under the DMCCA, AI governance, the Online Safety Act, personal data transfer rules, and the emerging framework of child protection measures. For each area, it identifies the measure at issue, the treaty language that could be invoked against it, and the way pressure could be applied in practice.

A preliminary point applies to all six areas. The question examined below is not whether the UK would lose a formal dispute brought by the US via the framework of an eventual UK-US agreement. If the UK were to sign anything similar to the ARTs promoted by the second Trump administration, Britain would not have access to an independent tribunal: currently, the United States assesses compliance itself and acts under its own law. The relevant question is therefore whether a UK measure can plausibly be characterised as inconsistent with the commitments. A plausible characterisation is sufficient to support a US tariff threat, or a demand for amendment – and the anticipation of such a characterisation influences what policymakers and regulators are willing to propose in the first place. Nor does this dynamic begin with a US agreement. The commitments the UK has already accepted – particularly on source code and algorithms through its CPTPP accession and a handful of bilateral agreements – can produce the same anticipatory effect: a department preparing legislation, or a regulator designing how to use its powers, must take advice on whether a proposal is consistent with the UK’s treaty obligations, and language that makes a measure arguable rather than clearly permitted enters that process as a reason for caution, whether or not any treaty partner ever objects. The analysis that follows therefore assesses exposure, not how a neutral adjudicator would rule.

3.1 The Digital Services Tax

The DST is a 2% tax on the revenues that search engines, social media services, and online marketplaces derive from UK users, applying only to groups whose digital services revenues exceed £500 million globally and £25 million from UK users.²¹ It is the UK measure with the longest history of US pressure, and the only one that has already been the subject of formal trade action under Section 301 of the Trade Act of 1974. USTR’s Section 301 investigation against the UK concluded in January 2021 that the DST discriminates against US companies. Notably, the report claimed that the tax’s revenue thresholds and its selection of covered activities were discriminatory because companies which meet the DST’s thresholds

were expected to be exclusively, or predominantly, US companies.²² Retaliatory tariffs were announced and then suspended under the October 2021 transitional compromise, in which the UK undertook to withdraw the DST once the OECD's Pillar One solution entered into force.²³

Pillar One has not entered into force, and the second Trump administration has renewed the pressure. A February 2025 presidential memorandum directs USTR to resume Section 301 scrutiny of digital services taxes generally;²⁴ the Trump administration's own account of the US-UK Economic Prosperity Deal records its disappointment that the UK would not "fully address" the DST;²⁵ and press reporting during 2025 indicated that the Starmer government considered reducing the rate in exchange for tariff concessions.²⁶ That episode is an example of regulatory chill operating on a measure already in force, before any treaty obligation existed.

As previously noted, several of the ARTs promoted by the second Trump administration provide that the partner "shall not impose digital services taxes, or similar taxes, that discriminate against US companies in law or in fact". By incorporating the possibility of de facto discrimination, without any requirement to assess the objective of the measure, the thresholds that confine DSTs to the largest firms would become the evidence of discriminatory treatment.

It is important to note that the DST would be exposed even under a UK-US agreement that contained no express DST prohibition. An unqualified non-discrimination commitment covering digital products and services, drafted based on the CPTPP or USMCA terms, would itself strengthen the US case. The Section 301 report's central argument – that the DST discriminates in effect against US firms – currently rests on US domestic law alone. A treaty obligation not to discriminate against US digital products and services would give that argument a basis in an international instrument to which the UK is a party, particularly if the text does not require a showing of protectionist intent, as is the case under the non-discrimination obligations in the digital trade chapters of the CPTPP and USMCA. This would allow the United States to present any pressure on the DST as the enforcement of an agreed commitment rather than as a unilateral demand. It is worth noting that the CPTPP and USMCA include taxation carve-outs that could cover DSTs.²⁷ However, the second Trump administration has been reluctant to include such exceptions and carve-outs in the agreements it has negotiated since returning to office, and the ART texts contain no equivalent carve-out.

Whereas the meaning of such commitments and carve-outs was once determined primarily through a mutually agreed legal process, in practice today it is often determined by the party with the power to enforce them. For instance, when the Trump administration ramped up pressure on Canada's DST, the Canadian government could have argued that its tax was not discriminatory or that it was covered by the USMCA's taxation carve-out.²⁸ However, faced with a tariff threat, Canada rescinded its DST outright in June 2025.²⁹ This means that, even if a UK-US agreement left the DST in place, its continuation would depend on how Washington chose to apply the clause at any given moment.

3.2 Digital competition regulation: the DMCCA

The Digital Markets, Competition and Consumers Act (DMCCA) created the UK's regime for digital competition. Under the DMCCA, the Competition and Markets Authority (CMA) may designate a firm as having strategic market status in a digital activity where the firm has UK turnover above £1 billion or global turnover above £25 billion and holds substantial and entrenched market power and a position of strategic significance. Designated firms become subject to tailored conduct requirements and, potentially, pro-competition interventions, with penalties of up to 10% of global turnover.³⁰ The regime is now in operation: the CMA designated Google in relation to general search in October 2025.³¹ Later that month, the CMA designated Apple and Google in relation to their mobile platforms.³² In January 2026, the CMA proposed its first conduct requirements for Google's general search services, including allowing publishers to opt out of having their content used to power AI features and introducing choice screens on the Chrome browser.³³ And, in June 2026, the CMA began consultations on steering requirements for Apple and Google's mobile platforms.³⁴

Evidently, both firms designated to date are American. That reflects the structure of the markets rather than any underlying discrimination within the Act. However, under an agreement prohibiting measures that discriminate against US digital products and services in fact, the composition of the designation register itself could provide the starting point for a claim. Under non-discrimination obligations covering digital products modelled on the USMCA or CPTPP, US firms would need only to argue that, in practice, the DMCCA has a disproportionate impact on them relative to UK or third-country like digital products. As discussed in Section 2, under USMCA-style language, a claim could rest on the treatment of a single product. This means that the United States could claim that a violation exists if, for instance, Google receives less favourable treatment than a single non-US competitor. The DMCCA's conduct requirements operate directly on how designated firms' products are distributed and displayed, through measures such as choice screens, restrictions on defaults, and obligations to give rival services parity or prominence. A requirement that a designated US firm's search application or app store be displayed alongside, or ranked no higher than, competing services could therefore be characterised as according that product less favourable treatment than like products.

Even more significantly, under the ART language the Trump administration has been imposing on its trading partners, it would not even be necessary to demonstrate that a domestic or third-country product receives more favourable treatment. The language broadly proscribes discrimination against US digital services or products distributed digitally without further elaboration. Without specific evidentiary standards and given the US's ability to initiate Section 301 proceedings to unilaterally determine whether a country has violated its agreements with the United States, a UK-US digital trade agreement following the ART model for digital trade provisions would leave the DMCCA vulnerable to direct challenges by the US government.

The United States has already treated foreign digital competition regimes as discriminatory trade barriers. The February 2025 memorandum states as policy that the United States will respond to foreign regulations that are “more burdensome and restrictive on United States companies than their own domestic companies”.³⁵ US industry associations and members of Congress have campaigned against the EU’s Digital Markets Act on the grounds that its designation thresholds capture US firms almost exclusively.³⁶ Most recently, President Trump threatened the EU with tariffs after the European Commission announced an €890 million fine against Google for violations of the DMA.³⁷

The DMCCA has attracted less attention than the DMA mainly because its enforcement began later. Yet its structure presents the same profile: quantitative thresholds that only the largest firms cross, designation without any finding of wrongdoing, and obligations that fall, in practice, entirely on US companies. Thus, it is likely that as the DMCCA enforcement efforts advance, the UK will face more pressure and threats from the current US administration. A UK-US digital trade agreement that binds the UK to refrain from discriminating against US digital products and/or services in vague and open-ended terms would give Washington greater leverage to undermine the UK’s flagship digital competition policy.

3.3 AI governance

The UK has not yet adopted a cross-sector AI statute, so the exposure in this area concerns future legislation. That does not make it less significant. The direction of UK policy has been consistent under both Labour and Conservative governments: toward greater transparency and external scrutiny of AI systems. At the same time, increased awareness of the possibilities and risks of AI is leading to a public clamour for greater regulation in the UK.³⁸

The 2023 white paper, issued by the Sunak Conservative government as part of its light-touch approach, nevertheless made transparency and explainability core principles. It called for regulators to have “sufficient information about AI systems and their associated inputs and outputs” and for parties affected by an AI system to be able to “access sufficient information” to enforce their rights.³⁹ The 2024 Labour manifesto committed to binding regulation on the companies developing the most powerful AI models.⁴⁰

The Burnham government has moved further: it has appointed the UK’s first dedicated Minister for AI, who has stated that the government rejects “tech boosterism” and will act through regulation to address the material risks of AI.⁴¹ More recently, the UK Minister for AI stated that “Britain would consider regulating advanced AI models if its current voluntary system for testing them before deployment no longer proved sufficient to protect the public.”⁴² His comments followed widespread reporting that frontier AI models had behaved unpredictably and compromised third-party systems, raising questions about whether voluntary pre-deployment testing is sufficient to identify emerging risks. The UK AI Security Institute currently receives pre-release access to frontier

models from the major developers under voluntary agreements. However, the recent reports are renewing interest in legislation establishing mandatory pre-deployment external testing and third-party audits.

A statutory regime of that kind would likely have some or all of three features that matter in the context of digital trade rules: it would operate before a system reaches the market; apply to a class of developers defined by capability rather than to any identified wrongdoer; and require access to detailed algorithmic information, including model weights and, in some formulations, source code. Regarding its digital trade implications, the first two elements would place such a regime outside the regulatory exception in the source code and algorithm provisions advanced by the US government, which permits compelled access only for “specific investigation, inspection, examination, enforcement action, or judicial proceeding”. The third element would bring the regime squarely within the protected subject matter of those provisions, as it would require access to software information that could be characterised as algorithms and, potentially, to source code. It is worth noting that some of these elements already appear in federal legislative proposals and in state-level AI laws that have been enacted in the United States.⁴³

However, if a UK statute were to convert voluntary access into a mandatory precondition, a UK-US digital trade agreement containing source code and algorithm secrecy protections could be leveraged to challenge or undermine such a policy, particularly because most of the firms likely to be subject to its requirements are US corporations.

That said, the UK’s existing trade agreements contain versions of source code and algorithm secrecy rules that could already undermine any future efforts to regulate AI. The UK has signed trade agreements with source code and algorithm secrecy provisions – albeit some of them do not extend to algorithms – with the CPTPP countries,⁴⁴ EU,⁴⁵ Japan,⁴⁶ Singapore,⁴⁷ Australia,⁴⁸ Ukraine,⁴⁹ and India.⁵⁰

It is worth noting that some of the UK’s more recent agreements allow “designated conformity assessment bodies” to require that source code and algorithms be preserved and made available. While this addition to the standard exception language found in agreements such as the USMCA is a positive development, the exception retains a case-by-case formulation that would likely leave little room for the kind of ongoing monitoring contemplated by recent AI regulation proposals. Thus, policies imposing a standing obligation on developers of advanced AI systems to disclose model weights, training data or architecture to a public authority or accredited auditor, without tying that disclosure to the assessment of an identified system, would not be covered even by the exception as currently formulated in agreements such as those the UK has signed with Singapore or India.

To that extent, existing UK trade agreements already create tensions with the government’s apparent plans to regulate AI. A UK-US digital trade agreement would entrench an existing obstacle to AI regulation and potentially make it more difficult for the UK to adopt stronger rules in the future.

3.4 The Online Safety Act

The Online Safety Act (OSA) was passed in 2023, establishing a set of rules aimed at protecting children and adults online. It imposes statutory duties of care on social media and search services, requiring them to assess the risks their services pose and take proportionate steps to mitigate the risk of users encountering illegal content and to protect children from material that is legal but harmful to them, with additional duties applying to the largest services once categorised.⁵¹ The Office of Communications (Ofcom) is the regulator responsible for enforcing the OSA. Accordingly, it produces the codes of practice and guidance that set out how providers are to meet their duties, monitors compliance through information-gathering, audit and transparency-reporting powers, and takes enforcement action against providers that fall short. Penalties can reach £18 million or 10% of a provider's qualifying worldwide revenue, whichever is greater. In the most serious cases, Ofcom can also seek court orders imposing business disruption measures, including requiring third parties to withdraw services from a non-compliant provider.⁵²

The OSA is the existing UK statute whose structure conflicts most directly with digital trade obligations, because its supervisory model relies on instruments that the source-code and algorithm-secrecy provisions effectively prohibit and, in some cases, that the specific exception does not cover.

Section 100 of the OSA empowers Ofcom to require any regulated provider to supply information for the purpose of “exercising, or deciding whether to exercise” its online safety functions – a formulation that covers ongoing supervision as well as enforcement in response to an identified breach. Moreover, Section 100(3)(a) expressly allows Ofcom to require a service provider “to take steps so that a person authorised by OFCOM is able to view remotely (...) information demonstrating in real time the operation of systems, processes or features, **including functionalities and algorithms**, used by a service” (emphasis added). In investigations into the death of a child that could be connected to the use of social media, search engines or other covered services, Section 101 similarly empowers Ofcom to require the relevant service provider to provide the authorities “with information about the use of a regulated service by the child whose death is under investigation, including, in particular—(a) content encountered by the child by means of the service, (b) how the content came to be encountered by the child (**including the role of algorithms or particular functionalities**)...” (emphasis added). Lastly, Section 107 establishes Ofcom's authority to conduct on-site audits. Schedule 12 sets out the process for such audits, clarifying that, during an audit, Ofcom may require a provider to assist an authorised person in viewing, in real time, “information demonstrating (...) the operation of systems, processes or features of a specified description, **including functionalities or algorithms of a specified description**” (emphasis added). These broad powers to require access to algorithms are in clear tension with the UK's commitments to refrain from requiring source code and algorithm disclosure, particularly under agreements that lack an exception for specific investigations such as CPTPP or the EU-UK Trade and Cooperation Agreement.

Yet other elements of the OSA could create broader conflicts with source code and algorithm secrecy provisions in trade agreements. Section 104(1) allows Ofcom to appoint a “skilled person” to assist in identifying and assessing an actual or potential failure by a provider of a regulated service to comply with a relevant requirement, assessing the nature and level of the risk of such a failure, and identifying ways to mitigate that risk. According to Section 101(7), the relevant provider must give the skilled person all such assistance as it may reasonably require in preparing the report. Such an obligation could easily entail granting access to detailed algorithmic information and, potentially, source code to an external examiner. It is unclear whether “skilled persons” in the context of the OSA would qualify under the notion of “designated conformity assessment bodies” used in some of the most recent agreements signed by the UK, meaning that this aspect of the legislation could be vulnerable under existing digital trade agreements to which the UK is a party.

Signing a UK-US digital trade agreement would increase the vulnerabilities of this statute, particularly because the firms most affected by the OSA are American, giving them an additional tool to challenge Ofcom’s enforcement of the law. Moreover, the OSA’s categorisation structure creates a second, independent source of exposure. Duties escalate by category, and the thresholds – based on user numbers and functionality – produce a Category 1 register composed overwhelmingly of US-owned platforms.⁵³ As with the DMCCA, that composition reflects the structure of the market. But under broad, open-ended non-discrimination obligations covering digital products and services, the composition of the register could provide a basis for a de facto discrimination claim based on differential treatment for US firms.

3.5 The UK GDPR and the protection of personal data

A UK-US digital trade agreement could constrain personal data transfer regulation. Under the UK General Data Protection Regulation (GDPR), personal data may leave the country only on conditions designed to keep protection attached to it: adequacy regulations made by the Secretary of State, standard contractual clauses, and transfer risk assessments.⁵⁴ An adequacy finding is a judgement about the current state of another country’s law and practice and whether it confers a “not materially lower standard of the protection”. Such a finding is kept under review and withdrawable if the receiving state’s surveillance practices or redress mechanisms deteriorate.

US-style digital trade provisions target this architecture from two directions. Cross-border data flows provisions impose a general obligation to permit international transfers, or to refrain from restricting them. Such an obligation is qualified by a public policy objective exception, but as mentioned in Section 2.3, the ability of these exceptions to safeguard data transfer regulation has been questioned.

Yet the agreements now promoted by the US government go further: countries like Indonesia and Argentina have each expressly committed to recognise the United States as a jurisdiction providing adequate data protection under their own law. That converts a domestic regulatory determination into a treaty obligation.

For the UK, an equivalent commitment would pre-empt the statutory assessment that the Secretary of State is required to make before approving transfers to any jurisdiction. It would effectively lock that assessment in place, preventing the UK from revisiting its adequacy determination in response to material changes in US law or practice. For instance, EU digital rights experts have called for the revocation of the EU-US data-transfer arrangement following the US Supreme Court's decision that the US Federal Trade Commission – the agency responsible for enforcing protections for personal data under the arrangement – is not an independent agency.⁵⁵ If the UK wanted to review its own arrangements for UK-US data transfers, a trade-law commitment to deem the United States adequate could significantly obstruct any reconsideration. Moreover, such a commitment would create a direct tension with the UK's own adequacy status under EU law, which depends on the European Commission's continuing assessment of UK data protection, including protection against onward transfers to third countries. A UK bound by treaty to treat the United States as adequate could jeopardise the UK's own adequacy status in the EU if the Commission were to determine that US data-protection safeguards are insufficient to protect Europeans' personal data. This would likely erect significant barriers for UK firms seeking to operate in the EU, as the EU rightly takes measures to protect the privacy of its citizens.

3.6 Child protection: the under-16 ban, nudification tools, and AI-generated CSAM

The agenda to protect children from technology-related harms has moved quickly in the UK, and part of it is now law. The Crime and Policing Act 2026 criminalises the making, adapting, supplying and offering of tools that generate purported intimate images of a person – so-called nudification tools – and creates a new offence of adapting, possessing, supplying or offering a child sexual abuse image generator, meaning an AI model optimised to produce indecent images of children.⁵⁶ The Children's Wellbeing and Schools Act 2026 inserts a power into the OSA for the Secretary of State to restrict children's access to specified services.⁵⁷ Under that power, the UK government announced that it intends to bar social media platforms from serving under-16s, with regulations expected before the end of 2026 and protections in force from spring 2027.⁵⁸

It should be said plainly that no digital trade provision targets these measures specifically, and no trade challenge to comparable measures elsewhere has been brought. The exposure nonetheless follows the same de facto logic as the preceding subsections. For instance, an under-16 prohibition is a measure applied to social media services, which are overwhelmingly US-owned. The burdens of compliance – including age-assurance infrastructure, the loss of a user cohort and enforcement risks – would therefore fall almost entirely on US firms, a fact that

could ultimately be used to construct a de facto discrimination claim under broad, open-ended non-discrimination rules covering digital products and services, if the UK were to negotiate a digital trade agreement with the United States. Notably, the Trump administration has already expressed its opposition to a UK ban on social media use by under-16s, claiming that the policy would “impose a disproportionate burden on US tech companies”.⁵⁹

Conclusion

The pattern across the six policy areas analysed in this report is consistent. The measures most exposed are those that reach the largest firms – which, given the structure of digital markets, means US firms – and the treaty language converts that reach into legal vulnerability. Whether any of the characterisations described above would persuade a neutral adjudicator cannot be tested, because the ART model provides for no such adjudicator; instead, Washington currently doles out reward and punishment without relying on pre-established legal processes. When the party that drafts the template also assesses compliance and imposes the consequences, the meaning of every commitment is whatever that party needs it to mean at a given moment – as the fate of the Canadian digital services tax already demonstrates.

On that basis, negotiating a digital trade agreement with the United States is too risky at present for the UK. The risk is not only that the UK could strike a poor bargain on the substance; it is also that the substance would not be settled by the bargain at all. Commitments would be interpreted and enforced by one party, under its own law, against a partner whose principal regulatory targets are that party's own firms – and at a moment when the current US administration has made the dismantling of foreign technology regulation an explicit objective. Whatever such an agreement said on paper, it would function as a standing licence for the United States to apply pressure on the UK's technology statutes.

Certain provisions would be more damaging than others. A non-discrimination obligation covering digital products or services would supply the legal foundation the United States has so far lacked to build cases against the DST, the DMCCA's designation regime, and the Online Safety Act's categorisation thresholds alike. Source code and algorithm provisions drafted on the US model would sit directly across the pre-deployment, class-based oversight on which prospective AI legislation could depend, as well as Ofcom's powers to enforce the OSA. And a commitment to recognise the United States as an adequate jurisdiction would convert a revisable regulatory judgement into a treaty obligation, with consequences for the UK's own standing under EU law and the prospects of a meaningful reset in UK-EU relations.

The tensions documented here do not, in any case, begin with a US agreement. The source code and algorithm secrecy clauses in CPTPP and the UK's agreements with a handful of trading partners already sit uneasily with the powers Parliament has given Ofcom and with any future AI legislation. The more useful course is therefore not to add new commitments but to revisit the existing ones: to seek amendment of the provisions that most constrain domestic policy space.

A government has taken office promising stronger public control over the technologies reshaping British economic and social life, including through potential regulation of AI. The choice it faces is not between a digital trade agreement and none, but between regulatory capacity held as a right and regulatory capacity held on sufferance.

List of acronyms

AI	Artificial intelligence
ART	Agreement on Reciprocal Trade
CEPA	Comprehensive Economic Partnership Agreement (UK-Japan)
CMA	Competition and Markets Authority
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CSAM	Child sexual abuse material
DMA	Digital Markets Act (EU)
DMCCA	Digital Markets, Competition and Consumers Act 2024
DST	Digital Services Tax
EU	European Union
FTA	Free trade agreement
GDPR	General Data Protection Regulation
IEEPA	International Emergency Economic Powers Act
OECD	Organisation for Economic Co-operation and Development
Ofcom	Office of Communications
OSA	Online Safety Act 2023
TPP	Trans-Pacific Partnership
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
UK	United Kingdom
US	United States
USMCA	US-Mexico-Canada Agreement
USTR	Office of the US Trade Representative

References

- 1 Chloe Taylor, “‘You can’t just leave it to the market’: Frontrunner to replace UK PM Starmer calls for ‘strong public control’ over industry and AI”, CNBC, 28 May 2026, <https://www.cnbc.com/2026/05/29/andy-burnham-makerfield-byelection-keir-starmer-tony-blair-ai.html>.
- 2 Office of the US Trade Representative, “Fact Sheet: US-UK Reach Historic Trade Deal”, accessed 9 August 2026, <https://ustr.gov/about/policy-offices/press-office/fact-sheets/2025/may/fact-sheet-us-uk-reach-historic-trade-deal>.
- 3 For brevity, this report uses the term “digital trade agreements” to refer to both standalone digital trade agreements and digital trade or e-commerce chapters contained in broader trade agreements.
- 4 The texts of these agreements are available here: Office of the US Trade Representative, “Agreements on Reciprocal Trade”, accessed 5 September 2026, <https://ustr.gov/trade-agreements/agreements-reciprocal-trade>.
- 5 CPTPP Art. 14.1.
- 6 UK Department for Business & Trade, “1 November 2021: UK-Japan CEPA Committee on Trade in Services, Investment Liberalisation and Electronic Commerce – joint minutes”, 1 November 2021, <https://www.gov.uk/government/publications/uk-japan-cepa-documents/01-november-2021-joint-minutes-of-the-first-meeting-of-the-committee-on-trade-in-services-investment-liberalisation-and-electronic-commerce>.
- 7 USMCA Art. 19.4; US-Japan Digital Trade Agreement Art. 8.
- 8 As an example of the “ART model”, this analysis uses the Agreement between the United States of America and Argentina on Reciprocal Trade and Investment (US-Argentina ART). However, the language across the 10 ARTs signed by the second Trump administration to date is strikingly similar, suggesting that the countries that have accepted these agreements have had limited ability to modify the template proposed by USTR through negotiations.
- 9 The Trans-Pacific Partnership (TPP) was signed in Auckland on 4 February 2016 by twelve countries including the United States. After the US withdrawal in January 2017, the remaining eleven concluded the CPTPP in Santiago on 8 March 2018, incorporating the TPP text by reference subject to twenty-two suspended provisions, mostly US priorities in intellectual property and investor–state dispute settlement. The electronic commerce chapter, largely built on US proposals, was not among them and survived unchanged apart from the removal of references to the United States. The UK acceded on 15 December 2024.
- 10 Daniel Rangel and Lori Wallach, “International Preemption by ‘Trade’ Agreement: Big Tech’s Ploy to Undermine Privacy, AI Accountability, and Anti-Monopoly Policies”, Rethink Trade, March 2023, <https://rethinktrade.org/wp-content/uploads/2023/03/International-Preemption-by-Trade-Agreement.pdf>, pp. 25–27.
- 11 Simon Lester, “Non-Discrimination Provisions in Digital Trade Chapters/Agreements: ‘A Digital Product’ vs. ‘Digital Products’, and the Impact on Policy Space”, International Economic Law and Policy Blog, 3 March 2021, <https://ielp.worldtradelaw.net/2021/03/non-discrimination-provisions-in-digital-trade-chaptersagreements/>.
- 12 See, for instance, US-Argentina Article 3.1.
- 13 TRIPS Art. 39 (protection of undisclosed information); Art. 10.1 (computer programs, whether in source or object code, protected as literary works under the Berne Convention).
- 14 Kristina Irion, “Algorithms Off-limits? If Digital Trade Law Restricts Access to Source Code of Software then Accountability Will Suffer”, in Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency (New York: Association for Computing Machinery, 2022), 1561–70, <https://doi.org/10.1145/3531146.3533212>.
- 15 Regulation (EU) 2016/679 (General Data Protection Regulation), Art. 44 (general principle for transfers), Art. 45 (transfers on the basis of an adequacy decision) and Art. 46 (transfers subject to appropriate safeguards, including standard contractual clauses). On transfer impact assessments, see Case C-311/18, Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II), EU:C:2020:559, and European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. For the UK, see UK GDPR Arts. 44–46 and Data Protection Act 2018, Part 2 Chapter 5.
- 16 Daniel Rangel, Jai Vipra and Lori Wallach, “The Digital Trade Data Heist”, Rethink Trade, February 2025, https://rethinktrade.org/wp-content/uploads/2025/05/Digital_Heist_report_updated.pdf.
- 17 On data localisation and cross-border transfers we use the US–Indonesia agreement rather than the US–Argentina agreement, because the Argentine text is atypical of the ART class. Both contain the same adequacy undertaking, requiring the partner to recognise the United States as a jurisdiction providing adequate data protection under its own law. But Article 3.2 of the Indonesian agreement, like Article 3.2(b) of the Malaysian one, also obliges the partner to ensure the transfer of data by electronic means “across trusted borders with appropriate protection for the conduct of business”. The Indonesian agreement is therefore the more representative example. Either way the objective is the same: removing the case-by-case regulatory assessment that transfer regimes ordinarily require before personal data may leave the jurisdiction.

- 18 For a detailed explanation see: Daniel Rangel, Jai Vipra and Lori Wallach, “The Digital Trade Data Heist”, p. 35.
- 19 For a detailed explanation see: Daniel Rangel, Jai Vipra and Lori Wallach, “The Digital Trade Data Heist”, pp. 26–27.
- 20 See: ‘General Terms for the United States of America and the United Kingdom of Great Britain and Northern Ireland Economic Prosperity Deal’, May 2025.
- 21 Finance Act 2020, Part 2 (Digital Services Tax).
- 22 USTR, Section 301 Investigation: Report on the United Kingdom’s Digital Services Tax, 13 January 2021, <https://ustr.gov/sites/default/files/files/Press/Releases/UKDSTSection301Report.pdf>.
- 23 US Department of the Treasury, “Joint Statement from the United States, Austria, France, Italy, Spain and the United Kingdom Regarding a Compromise on a Transitional Approach to Existing Unilateral Measures”, 21 October 2021, <https://home.treasury.gov/news/press-releases/jy0419>.
- 24 The White House, “Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties”, Presidential Memorandum, 21 February 2025, <https://www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/>.
- 25 USTR, “Fact Sheet: US-UK Reach Historic Trade Deal”, May 2025, <https://ustr.gov/about/policy-offices/press-office/fact-sheets/2025/may/fact-sheet-us-uk-reach-historic-trade-deal>.
- 26 See, e.g., Philip Aldrick and Nour Al Ali, “Starmer Holds ‘Productive’ Talks With Trump Ahead of Tariff Hit”, Bloomberg, 30 March 2025, <https://www.bloomberg.com/news/articles/2025-03-30/uk-s-starmer-in-productive-talks-with-trump-before-crunch-week>; Pippa Crerar, Heather Stewart and Richard Partington, “Starmer offers big US tech firms tax cuts in return for lower Trump tariffs”, The Guardian, 1 April 2025, <https://www.theguardian.com/us-news/2025/apr/01/starmer-offered-big-us-tech-firms-tax-cuts-in-return-for-lower-trump-tariffs>.
- 27 Both CPTPP and USMCA contain general taxation carve-outs that limit the application of most obligations to tax measures (CPTPP Art. 29.4; USMCA Art. 32.3).
- 28 Allison Christians, “Can Canada Tax Digital Services if the United States Disagrees?” Perspectives on Tax Law & Policy, Volume 4, Number 2 (June 2023), <https://www.ctf.ca/EN/EN/Newsletters/Perspectives/2023/2/230205.aspx>.
- 29 Department of Finance Canada, “Canada Rescinds Digital Services Tax to Advance Broader Trade Negotiations”, 29 June 2025, <https://www.canada.ca/en/department-finance/news/2025/06/canada-rescinds-digital-services-tax-to-advance-broader-trade-negotiations-with-the-united-states.html>.
- 30 Digital Markets, Competition and Consumers Act 2024, Part 1.
- 31 Competition and Markets Authority, “NOTICE UNDER SECTION 14(2) OF THE DIGITAL MARKETS, COMPETITION AND CONSUMERS ACT 2024 (THE ACT)”, 10 October 2025, <https://www.gov.uk/cma-cases/googles-general-search-and-search-advertising-services>.
- 32 Competition and Markets Authority, “CMA confirms Apple and Google have strategic market status in mobile platforms”, 22 October 2025, <https://www.gov.uk/government/news/cma-confirms-apple-and-google-have-strategic-market-status-in-mobile-platforms>.
- 33 Competition and Markets Authority, “CMA proposes package of measures to improve Google search services in UK”, 28 January 2026, <https://www.gov.uk/government/news/cma-proposes-package-of-measures-to-improve-google-search-services-in-uk>.
- 34 Competition and Markets Authority, “CONSULTATION: STEERING CONDUCT REQUIREMENT – Apple’s Mobile Platform”, 30 June 2026, <https://connect.cma.gov.uk/consultations/proposed-steering-cr-apple/supporting-documents/consultation-document-apple-steeringpdf>; Competition and Markets Authority, “CONSULTATION: STEERING CONDUCT REQUIREMENT – Google’s Mobile Platform”, 30 June 2026, https://assets.publishing.service.gov.uk/media/6a4359d2db380b085e94ab73/Consultation_document_Google_steering.pdf.
- 35 White House, Defending American Companies Memorandum, Sec. 3(c).
- 36 For instance, see: Computer & Communications Industry Association, “Comments for the 2026 USTR National Trade Estimate Report on Foreign Trade Barriers”, 30 October 2025, <https://ccianet.org/library/ccia-comments-for-the-2026-ustr-nte-report/>, p. 82; Office of Rep. Darin LaHood, “LaHood, DelBene Lead Bipartisan Lawmakers to Urge President Biden to Demand Changes to Discriminatory EU Digital Markets Act”, 23 February 2022, <https://lahood.house.gov/2022/2/lahood-delbene-lead-bipartisan-lawmakers-to-urge-president-biden-to-demand-changes-to-discriminatory-eu-digital-markets-act>.
- 37 Gaya Gupta, “Trump threatens EU with ‘substantial’ tariffs over fines of US tech giants”, The Guardian, 24 July 2026, <https://www.theguardian.com/us-news/2026/jul/24/trump-european-union-tariffs>.
- 38 Ada Lovelace Institute, “Nearly 9 in 10 people in the UK support independent regulation of AI”, 4 December 2025, <https://www.adalovelaceinstitute.org/press-release/nearly-9-in-10-people-in-the-uk-support-independent-regulation-of-ai/>.
- 39 Department for Science, Innovation and Technology, “A Pro-Innovation Approach to AI Regulation”, 3 August 2023, <https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper>.

- 40 The Labour Party, “Change: Labour Party Manifesto 2024”, <https://labour.org.uk/wp-content/uploads/2024/06/Labour-Party-manifesto-2024.pdf>.
- 41 Chris Smyth and Anna Gross, “Chips and drones to be at heart of Andy Burnham’s push to ‘reindustrialise’, AI minister says”, Financial Times, 26 July 2026, <https://www.ft.com/content/5b789a38-c9ca-4b23-8e61-8f9e2e589396?syn-25a6b1a6=1>.
- 42 Paul Sandle, “Britain says it is open to AI regulation if voluntary safeguards fall short”, Reuters, 3 August 2026, <https://www.reuters.com/business/media-telecom/britain-says-it-is-open-ai-regulation-if-voluntary-safeguards-fall-short-2026-08-03/>.
- 43 US House of Representatives, Frontier Risk Oversight, National Transparency, Independent Evaluation and Reporting Act, H.R. 9925, 119th Congress, 2nd sess., introduced 23 July 2026, <https://www.congress.gov/bill/119th-congress/house-bill/9925/text>; Illinois General Assembly, Artificial Intelligence Safety Measures Act, SB0315, 104th General Assembly, <https://www.ilga.gov/Legislation/BillStatus/FullText?GAID=18&DocNum=315&DocTypeID=SB&LegId=0&SessionID=114>.
- 44 CPTPP Art. 14.17.
- 45 EU–UK Trade and Cooperation Agreement Art. 207.
- 46 UK–Japan Comprehensive Economic Partnership Agreement Art. 8.73.
- 47 UK–Singapore Digital Economy Agreement Art. 8.61–K.
- 48 Australia–UK Free Trade Agreement Art. 14.18.
- 49 UK–Ukraine Digital Trade Agreement Art. 132–P.
- 50 UK–India Comprehensive Economic and Trade Agreement Art. 12.15.
- 51 Online Safety Act 2023, Parts 3–4 (duties of care for user-to-user and search services).
- 52 Online Safety Act 2023, Part 7 (Ofcom’s powers of information-gathering, enforcement and business disruption).
- 53 According to Ofcom, the current Category 1 services are Facebook, Instagram, Pinterest, Quora, Reddit, Roblox, Snapchat, TikTok, WhatsApp, X and YouTube, all but one of which are US firms. See: Ofcom, “Online Safety: Register of categorised services and list of emerging Category 1 services”, last updated 14 August 2026, <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/register-of-categorised-services-and-list-emerging-category-1-services>.
- 54 UK GDPR, Chapter V (Arts. 44–49).
- 55 Noyb, “US Supreme Court just blew up EU–US Data Transfers”, 29 June 2026, <https://noyb.eu/en/us-supreme-court-just-blew-eu-us-data-transfers>.
- 56 Crime and Policing Act 2026, Secs. 99 and 74.
- 57 Children’s Wellbeing and Schools Act 2026, inserting Sec. 214A into the 2023 Online Safety Act.
- 58 Department for Science, Innovation and Technology, “Fact sheet: New rules to protect children online”, 17 July 2026, <https://www.gov.uk/government/publications/fact-sheet-new-rules-to-protect-children-online/fact-sheet-new-rules-to-protect-children-online>.
- 59 Dan Milmo, “White House urges UK not to ban social media for under-16s”, The Guardian, 9 June 2026, <https://www.theguardian.com/uk-news/2026/jun/09/white-house-urges-uk-not-ban-social-media-under-16s>.



Author: Daniel Rangel Jurado

Daniel Rangel Jurado is the Director of Research and International Advocacy of the Rethink Trade programme at the American Economic Liberties Project. Daniel holds a master's degree in International Economic Policy from the Paris School of International Affairs at Sciences Po and an LL.M. in International Legal Studies from Georgetown University Law Center. He also holds Law and Political Science degrees from Universidad de los Andes in Bogotá, Colombia. The views expressed in this policy brief are personal and do not represent the organisation.

The Trade Justice Movement is a network of 45 organisations, including trade unions, environmental groups and justice campaigns, which push for trade policy that works for people and planet.



**TRADE JUSTICE
MOVEMENT**

 www.tjm.org.uk

 [@tradejusticemov.bsky.social](https://bsky.app/profile/tradejusticemov.bsky.social)

 [trade-justice-movement](https://www.linkedin.com/company/trade-justice-movement)