The United Kingdom’s Post-Brexit Push for Deregulation in Global Data Governance

Javier Ruiz

June 2023
Executive Summary

The UK is using its post-Brexit role in global digital trade and data governance to promote economic growth and deregulation through free trade agreements and domestic data protection reforms.

The country wants to create a unique framework for international data transfers, liberalize data flows, and position the UK as the world’s most attractive data marketplace. This approach deviates from the EU’s focus on personal data protection as part of the right to privacy and aligns more with the US and Indo-Pacific region.

This strategic shift is cemented with accession to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). New agreements with countries in the region like Japan, Singapore and Australia prioritize digital trade and data flows. The UK is also pursuing deals with countries like India, focusing on digital trade. These deals face many challenges, from disagreements over India’s data localization policies to potential legal conflicts between the UK’s GDPR-based framework and India’s weaker privacy regulation.

Consumer rights advocates argue these trade deals could compromise data protection standards and limit transparency of algorithms. These trade deals would increase the risks of data exploitation and create difficulties to regulate digital technologies, such as AI, in the public interest, reducing the control people have over their data, and eroding consumer trust in the digital economy. The effect could be felt more widely if the UK government’s approach to digital trade reduces the potential for future global convergence of technology and data governance towards higher standards of consumer protection.

These international policies are coupled with domestic reforms that, in the name of growth, openly tilt the balance towards the needs of business by reducing consumer rights, potentially undermining privacy. The new Data Protection and Digital Information Bill (No. 2) will amend the UK GDPR to signal a departure from the EU approach in areas such as identifiable information, automated decisions, data rights, and business obligations. Proposed changes to the regulation of cross-border transfers of personal data would also make it easier for the UK to align with the data regimes of the CPTPP countries.

Critics argue that these changes could lead to hidden processing, fewer data subject rights, and increased complaints from data subjects. These changes could also jeopardise the existing arrangements for free flow of data between the UK and the EU, which would cause major economic turmoil.

As the UK moves forward, striking a balance between fostering economic growth and ensuring robust consumer and data protections will be crucial. The current bias towards traditional pro-business deregulation and unchecked free trade could cause problems for consumers and risks being out of step with the current geopolitical alignments and social concerns about technology.
Contents

The Importance of UK’s Role in Trade Justice and Global Data Governance ........................................ 3
The UK’s New Geopolitical Alignment and Digital Power ........................................................................ 4
Trade Policy: A Lack of Clarity and Coherence ...................................................................................... 5
Britain’s Digital Trade Objectives: Fostering Economic Growth ......................................................... 6
Trade Activities ..................................................................................................................................... 7
Continuity Deals ................................................................................................................................... 7
New Agreements ................................................................................................................................... 8
  UK-Japan Comprehensive Economic Partnership Agreement .......................................................... 8
  Australia .............................................................................................................................................. 9
  New Zealand ...................................................................................................................................... 10
  UK-Singapore Digital Economy Agreement ..................................................................................... 10
  Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) .............................................. 11
Priority Negotiations in 2023 ............................................................................................................. 12
  India .................................................................................................................................................. 12
  Ukraine ........................................................................................................................................... 13
Relationship with the EU ...................................................................................................................... 13
  Digital Trade in the EU-UK Agreement ............................................................................................ 13
  Data Protection and Regulatory Autonomy ..................................................................................... 14
Changes to the Domestic Data Protection Regime ............................................................................. 14
  A Domestic Data Regime That Pits Privacy Rights Against Growth ............................................. 15
International Data Transfers as Trade Instruments .......................................................................... 18
  Creating Practical Interoperability With Asia Pacific Data Regulations ..................................... 18
Challenges to independent data regulation ...................................................................................... 19
Risks to the EU Adequacy Decision .................................................................................................. 19
Conclusion ........................................................................................................................................... 20
The Importance of UK's Role in Trade Justice and Global Data Governance

Policymakers and advocates working on trade, digital governance, and human rights should be aware of the potential impact the United Kingdom has on the global governance of cross-border data flows. Due to historical and political factors, the UK significantly influences the global agenda on digital trade and technology regulation. Despite its medium-sized population, the UK remains a key player in the G7 group of leading economies, driven by its efforts to expand global trade agreements and prioritize data flow liberalization.

However, British digital trade agreements tend to be one-sided, promoting unrestricted cross-border data flows with limited provisions for public policy restrictions. These agreements often result in data traveling from jurisdictions with strong consumer protections to places where data can be exploited or misused.

Cross-border data flows are essential for the global economy, and the internet has brought countless benefits to people worldwide. However, growing concerns about online abuse, corporate surveillance, and new forms of control erode consumer trust in the digital economy.

Supporters of data liberalization argue against data localization policies that require companies to keep data within the country, e.g., health or financial records, for public policy or economic development. Supporters of data liberalization argue that localization limits access to global cloud infrastructure and hinders advancements in AI and other cutting-edge technologies.

There are many public policy reasons to keep data in a country, such as enabling access to regulators, controlling sensitive information, and promoting national digital innovation and economic growth. However, the effectiveness of data localization as an economic policy is unclear, and in many low- and middle-income countries additional developments in technology and infrastructure would be needed. At the systemic level, the concern is that if everyone were to implement data localization policies, the internet would fragment and the negative impacts of such global decoupling, or “balkanization of the Internet”, would undo any local economic gains.

Despite these risks, the current situation is not sustainable in the long term. The UN agency for trade and development, UNCTAD, has warned that “large power imbalances stalk the growing digital economy as major platforms reinforce their positions in the global data value chain.” Demands for data localization will continue if technological knowhow and infrastructure are unequally distributed.

From the point of view of human rights, while data localization may protect individuals from exploitation by foreign companies and spy agencies, it can also facilitate domestic state surveillance. This is clear in the case of China and other countries with authoritarian governments, but these policies are reproduced elsewhere.

The recent conflict of the US government with the company TikTok is the most high-profile example of data localization and evidence of the difficulties with squaring data flows with public policy. National security concerns over the potential surveillance of US TikTok users by the Chinese government led to US government measures. Facing the risk of being banned in the US, in 2022 TikTok placed all the data
of its US users in the cloud systems of US company Oracle, who are able to monitor and control its use, in what amounts to an escrow system.\textsuperscript{iv}

Critics of localization have expressed that “national security justifications for these mandates are often thinly veiled attempts at asserting greater control of the domestic digital domain”.\textsuperscript{v} For example, it is unclear whether US concerns over TikTok relate to evidenced Chinese surveillance, the potential loss of its own surveillance capabilities, or wider economic competition.

While the global internet provides many advantages, simply removing barriers to data flows without proper safeguards can harm consumers. The root of many negative perceptions about digital technologies lies in poor data governance, including data protection, privacy laws, and the positive use of data for economic development.\textsuperscript{[6]}

The best way to remove barriers to digital trade is by raising global standards for innovative data governance, increasing public participation\textsuperscript{[7]} and implementing effective and consistent enforcement of regulations in fair competition.

**The UK's New Geopolitical Alignment and Digital Power**

As an established mid-ranking digital power, the UK boasts accumulated wealth, advanced skills and education, and well-developed regulation, despite its aging infrastructure. The country sees a low level of business investment, including R&D, but has a high concentration of data centres. Notably, 81% of UK market revenues for public cloud infrastructure are generated by US firms like Amazon, Microsoft, and Google.\textsuperscript{[8]} After Brexit, the UK now finds itself navigating between the regulatory frameworks of the US, the EU, and China, much like other nations in a similar position, such as Japan or Canada.

The prospect of a comprehensive free trade deal with the US, which was central to the Brexit narrative, has not materialized as anticipated. Consequently, the UK continues to strive for stronger ties with the US while improving relations with the EU. However, both the EU and the US are preoccupied with strengthening their own connections and addressing issues such as Ukraine and China. This has left the UK with limited interest from both parties.

Instead, the UK government has shifted its foreign policy focus towards the Indo-Pacific region, emphasizing data and digital services in its trade strategy.\textsuperscript{[9]} New UK trade agreements feature digital trade rules that liberalize data flows and accept lower data protection standards. The country also actively participates in global digital governance spaces, such as the G7 and the WTO.

This foreign policy shift is accompanied by domestic legal reforms aligning specific data regulations with Pacific region countries, reducing privacy protections under a pro-growth data governance regime.\textsuperscript{[10]} These changes could complicate the UK's relationship with the EU, as the government aims to distance itself from the perceived lack of dynamism within the EU.\textsuperscript{[11]} At the same time, the UK recognizes the importance of maintaining existing data arrangements for both the UK and the EU economies and for collaboration over security issues ranging from police investigations to the war in Ukraine.\textsuperscript{[6]} Under the current arrangements within the EU adequacy regime, the EU currently treats the UK as if it were still part of the bloc for data transfer purposes, but this could change if divergence becomes too extreme.
Although restrictions to data transfers to the UK by the EU could be complicated by the Trade and Cooperation Agreement (TCA), which sets out a wide berth for regulatory autonomy on both sides, as we discuss elsewhere in this brief.

Ironically, the negative impacts of many Brexit-driven policies have diminished the UK’s status and ability to execute these new trade agreements and build economic relationships across the world effectively. The country's reputation hit rock bottom during Liz Truss's brief tenure as Prime Minister in 2022, as her policies to remove regulations and cut taxes threatened financial stability and caused confusion including over technology and trade.\[12\]

The confusion over policies continues, mainly stemming from internal divisions within the current Rishi Sunak’s government, as ministers have been pushing different agendas, including data reforms that diverge from the GDPR. A clear realignment on foreign policy may emerge amid these shifting priorities, which we discuss in more detail below.

**Trade Policy: A Lack of Clarity and Coherence**

British trade policy has faced criticism due to its lack of "clarity, strategy, and coherence... at a risk of pursuing trade deals for their own sake." \[13\] Despite the significant volume of negotiations and the diligent work of civil servants, concerns persist that the UK is driven by ideological priorities. \[14\] Many policymakers are eager to use the UK's newfound freedoms after Brexit to establish new trade agreements, \[15\] but these efforts have not yielded the expected benefits. \[16\] For example, the food related sections of the UK-Australia free trade agreement have been described as “not actually a very good deal for the UK” by the minister responsible for agriculture at the time.\[17\]

Rushing trade deals has also been criticized for overlooking human rights issues, as seen in India's handling of British citizen Jagtar Singh Johal \[18\] and the treatment of workers in UK priority countries for trade deals.\[19\]

**Weak Scrutiny and a Push for Transparency**

For years, UK trade policy was part of the EU, with local transparency and consultation gaps compensated for by MEPs and civil society scrutiny in Brussels, including British participation. However, since Brexit, the transfer of these capabilities has been sluggish, and scrutiny of UK trade deals has proven inadequate. Many civil society organizations and publications, including The Economist, have lamented the lack of information and transparency surrounding trade agreements. \[20\] Businesses have also struggled to stay informed, particularly on EU trade tariffs. \[21\]

The UK Trade Policy Observatory has recommended improvements to Parliament’s role, evidence quality, and a wider range of consultations, but the government has not changed its approach. \[22\]

**Rishi Sunak’s Government: Renewed Focus and Pragmatism**

The current government of Rishi Sunak has attempted to bring focus and pragmatism to EU relations while contending with MPs in its own party who remain staunchly opposed to the bloc. Reproachment with the EU, including a Northern Ireland deal to break the most serious impasse, have been balanced
with accession to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).\[^{23}\]

New Trade Secretary Kemi Badenoch is a vocal free trade advocate and opposes protectionism.\[^{24}\] While she champions the removal of trade barriers, her focus appears to be more on deal-making than the intricacies of data and digital policy. Badenoch aims to solidify the policy objectives of previous Conservative governments into a concrete target of growing UK exports in a Race to a Trillion – selling over a trillion pounds of goods and services worldwide annually by 2030.\[^{25}\] This goal represents a 20% increase from the current £800 billion, though some economists argue that inflation alone would achieve this figure.\[^{26}\]

**Britain's Digital Trade Objectives: Fostering Economic Growth**

The UK's Digital Trade Objectives centre on promoting economic growth. The UK seeks to achieve this by removing trade barriers, helping businesses acquire new customers, streamline logistics and processes, and connect with global workforces.\[^{27}\]

Most of the UK's digital trade objectives do not pose major issues of concern for consumers. For example, the goal of opening digital markets is uncontroversial and encompasses promoting market access for UK companies, net neutrality, and other fair competition measures. Similarly, the development of digital trading systems that facilitate administrative and logistical processes is a positive step for consumers.

While better international cooperation, global governance, and promoting consumer and business safeguards are positive in principle, the details are crucial. The UK has high consumer protection standards, both domestic and inherited from the EU, and some agreements could lead to lower protections.

From the perspective of digital rights and trade justice, the primary concern is the unabashed championing of international data flows. The plan outlined in the objectives document aims to "make the UK a world leader in developing a balanced approach to the trade in data, maximizing the benefits of cross-border data flows to consumers and businesses while maintaining and promoting high standards of protection for personal data." Although this sounds good in principle, the implementation is problematic.

The United Kingdom requires that its trade partners commit to establishing or maintaining domestic legal frameworks that safeguard personal data, while concurrently ensuring that personal data originating from the UK remains protected under its own domestic data protection legislation. A key issue with this policy is its lack of specificity concerning the quality of data protection legal frameworks required from trade partners. Furthermore, the policy does not address how the UK's domestic data protection legislation will secure data transferred to jurisdictions with weaker legal regimes. Combined with the data protection law reforms discussed earlier, this approach could potentially lead to diminished data protection standards compared to those currently in force.
Trade Activities

Since Brexit, the UK has pursued an ambitious trade agenda, finalizing deals with over 70 countries. However, most of these agreements are continuity deals, which extend existing EU arrangements. Japan is a notable exception, as the UK inherited a comprehensive agreement from the EU and supplemented it with novel commitments, particularly concerning digital trade. Similar digital provisions are featured in agreements with Australia and the CPTPP, while New Zealand sought tailored arrangements to safeguard the rights and interests of its Māori population. The new digital partnership with Singapore covers various regulatory aspects of digital technologies, including AI and digital identities. The UK's priority negotiations include South Korea and, more significantly, India, due to its vast English-speaking market. Additionally, the UK strategy involves advocating for the liberalization of digital trade and data governance within the World Trade Organisation and the G7.

Continuity Deals

Most of the recent UK trade agreements are continuity deals, with many being collective arrangements involving groups of countries such as the Caribbean community CARIFORUM or the Eastern and Southern Africa (ESA) trade bloc. These deals predominantly replicate prior arrangements established while the UK was an EU member and do not incorporate digital trade chapters. Some agreements do contain electronic commerce chapters, but none commit to data protection and cross-border data flow provisions. Certain renewed deals include clauses obligating parties to renegotiate within a specified timeframe, with digital trade likely to feature in future discussions.

Despite initial political alignment between the pro-Brexit UK government and the Trump administration, the interests of various groups including Irish American concerns over peace in Northern Ireland slowed the trade talks between the UK and the US.

Realizing a comprehensive trade agreement between the UK and the US is a challenging endeavour despite the intentions of the UK government. Integrating the UK into a close trading partnership with the US would mean dismantling a significant portion of the British regulatory framework inherited from the EU. The US government on behalf of its multinational corporations has argued that EU/UK regulations, including data protection rules, alongside food additives, hazardous chemicals, and industrial safety certifications, are unacceptable trade barriers.

While the British public have expressed abstract support for a US trade deal, they vehemently oppose specific regulatory changes, especially those concerning farming and food processing.

The geopolitical situation has changed since the Brexit vote, with the US concentrating on China and Pacific through the Indo-Pacific Economic Framework for Prosperity (IPEF).

The ongoing conflict in Ukraine has underscored the EU's significance to the US in its efforts to isolate Russia and made the UK less of a strategic priority, as evidenced by the joint EU-US Trade and Technology Council.

The Biden administration has repeatedly confirmed it has no plans for a trade agreement with the UK.
New Agreements

Digital trade and data flows provisions are a central element of the UK’s new and prospective free trade agreements that do not involve continuity from EU deals. These new agreements primarily target the Asia-Pacific region: CPTPP, Japan, Australia, New Zealand, and Singapore, with negotiations with India and South Korea.[34] The UK government sees that region as the centre of the global economy and future growth, in contrast to Europe, which it perceives as slow and resistant to change and innovation.

UK-Japan Comprehensive Economic Partnership Agreement

The UK-Japan Comprehensive Economic Partnership Agreement (CEPA) was signed in October of 2020 and entered into force at the end of that year. The treaty marked the first new free trade agreement independently signed by the UK, separate from the EU. While most of the agreement is based on the existing EU-Japan deal, important changes on digital trade have been introduced, particularly regarding data flow liberalization and algorithm disclosure restrictions.[35] These provisions mirror those in recent US agreements, such as the United States-Mexico-Canada Free Trade Agreement (USMCA) and the US-Japan Digital Trade agreement.[36]

The government has highlighted the agreement’s benefits, but many economists argue that the claimed advantages stem from the existing treaty with the EU.[37] Beyond a few economic sectors, such as gaming and connected cars, cultural barriers may limit the practical impact of the digital provisions. For example, the most popular social media in Japan is the app Line, originally from Korea and completely unknown in the UK.[38]

Nevertheless, this treaty is significant because both Japan and the UK are strong advocates for digital trade liberalization and will use this deal as a policy tool beyond its immediate economic effects. The UK-Japan CEPA has served as a springboard for the UK into the Pacific region. Japan is part of most regional agreements, and this alignment facilitated the UK’s application to the CPTPP.

The previous EU-Japan deal prohibited the forced disclosure of source code as a condition for exports, but CEPA goes further by also restricting access to algorithms associated with source code.[39] These technical disclosure prohibitions can limit the scrutiny and accountability of various digital systems.[40] The UK Digital Regulation Co-operation Forum (DRCF), composed of the main regulatory bodies on privacy, finance, competition and communications, has found that “there is a lack of visibility and transparency in algorithmic processing, which can undermine accountability”, and propose to increase “algorithmic assessment practices.”[7] These efforts could be hampered by such trade clauses.

The UK-Japan agreement also adds provisions to restrict forced disclosure and/or adoption of specific encryption technologies, like those in the CPTPP agreement (Annex 8-B)[41] and DEPA, the Digital Economic Partnership Agreement (explained in detail below), but even broader.[42]

These trade policies address long-standing industry complaints about countries like China and Vietnam using regulations requiring disclosure to steal proprietary information or mandating specific technologies to act as trade barriers.[43] Governments must protect consumer data and communication security, but trade rules should not hamper interventions to mandate higher standards. The impact of
restricting encryption disclosure remains unclear because security designs are not typically completely secret.\[44\]

**Data Protection in the UK and Japan deal**

CEPA requires the implementation of valid data protection frameworks and encourages developing the compatibility between the different data regimes. While Japan's legal privacy framework enables data transfers from the EU and the UK, Japan has also signed several digital trade agreements that mandate free data flow with countries with lower protections including the US. Research by the Digital Trade Alliance has shown that these arrangements could pose risks for onward data transfers.\[45\]

The agreement clarifies that valid data protection frameworks specifically include "laws that provide for the enforcement of voluntary undertakings," meaning that the privatized certification regimes popular in the Asia-Pacific region would be considered equivalent to the UK's GDPR-based system. However, it is highly questionable whether certification schemes would be enough to satisfy the strict safeguards and strong consumer protections required by the European model.\[46\]

**The New EU-Japan Digital Partnership**

The EU and Japan are forging closer ties, which may reduce the gap between them and also facilitate closer integration with the UK. In May 2022, the EU and Japan established a Digital Partnership, marking the first such agreement the EU has signed with a partner country.\[47\] Although the partnership is a relatively informal arrangement, it carries significant implications as it paves the way for Japan's integration into the highly valued EU Horizon 2020 research program, which currently excludes the UK.\[48\] Furthermore, the EU is considering updating its existing trade agreement with Japan to incorporate provisions on cross-border data flows.\[49\] This development reflects the growing importance of digital trade and data governance in international relations and the nexus between the EU, Japan, and the UK.

**Australia**

The UK and Australia signed a trade agreement in December 2021, serving as another springboard towards the Pacific but having limited short-term impact on actual digital trade between the countries.\[50][51\]

The UK deal with Japan was the first treaty post-Brexit, but most of it was inherited from the EU. Australia entered the first new UK trade deal negotiated from scratch. The treaty includes provisions on cross-border data flows, localization, encryption, and source code protection that closely resemble the UK-Japan agreement text. These data protection provisions replicate the problematic acceptance of lower standards (voluntary undertakings) found in other FTAs. The British government defended the clauses in its official impact assessment, claiming they do "not undermine the UK's domestic legislation on personal data protection" without providing a detailed analysis.\[52\] Since 2001, Australia has been unable to agree on free data flow with the EU due to differences in legal frameworks.\[53\] However, planned Australian privacy law reforms could change this situation.\[54\]

The impact assessment of the deal highlights that it includes "the first-ever dedicated innovation chapter of any FTA in the world." However, the actual text is somewhat underwhelming, with weak commitments to promoting governance frameworks and standards, and establishes a Strategic Innovation Dialogue of
unclear powers and outcomes. The new innovation chapter is among several novel commitments on
digital technologies that align UK policy more closely with the Digital Economic Partnership Agreement
(DEPA). These commitments include electronic invoicing, data innovation, and mutual recognition of
digital identities, even though the UK does not have a national digital identity system. The DEPA contains
interesting innovations, as discussed elsewhere, but at the same time it solidifies the CPTPP and similar
trade agreements.

The deal became a flashpoint for the conflict between Parliament and the executive over scrutinizing
trade deals.[55] Despite calls from several committees in the British Parliament to delay the process,[56]
the UK government eventually ratified the agreement without a parliamentary vote or debate.[57] This
event underscores the ongoing tension between branches of government regarding the oversight of
trade negotiations and the transparency of international agreements.viii

New Zealand

The UK and New Zealand have signed an agreement encompassing extensive digital trade commitments
but with notable differences from previous deals regarding data protection and source code.[58]

The first distinction is the absence of a clarification about voluntary undertakings and other lower data
protection standards. Unlike Australia, both the EU and the UK recognize New Zealand's privacy regime
as adequate, allowing free data flow. While this recognition means that the impact of this omission is
limited, it is a positive step that should be replicated in future UK trade deals.

The agreement adopts a different tone, emphasizing interoperability, consumer confidence, and digital
inclusion in its digital chapter objectives. However, most treaty provisions align with the UK deals
previously discussed, including data flows, localization, encryption, digital identities, and digital
innovation and emerging technologies. As a member of the DEPA, New Zealand's influence is evident in
some of these provisions.

This more progressive digital trade agreement is partly due to Māori organizations' long-term
involvement in trade policy. All FTAs New Zealand has signed in the past two decades include the Treaty
of Waitangi exception clause, which enables the Government to adopt policies fulfilling its obligations to
Māori communities under the Waitangi Tribunal.[59] This approach contrasts with the UK's approach to
the participation of stakeholders.

Māori community concerns led to the removal of the clause protecting source code (and algorithms)
found in other agreements. Concerns about data sovereignty previously raised in relation to CPTPP by
the Waitangi Tribunal led to this change.[60] The UK-NZ deal is small, and the changes will not have
significant practical consequences, but they demonstrate that alternative approaches to digital trade
agreements are possible.

UK-Singapore Digital Economy Agreement

The UK government described the Digital Economy Agreement signed with Singapore in February 2022
(UKSDEA) as "the world's most innovative trade agreement, covering the digitized trade in services and
goods across the whole economy."[61] The UKSDEA includes binding commitments on digital trade, such
as free data flow and a ban on localization, alongside cooperative elements in various emerging and innovative areas such as Artificial Intelligence, fintech, digital customs, digital identities, and legal technology.\[^{[62]}\]

The agreement is modelled on the DEPA originating in the Asia-Pacific region and other similar bilateral deals signed by Singapore.\[^{[63]}\] These agreements are described as the new frontier for trade. To emphasize this innovative aspect, New Zealand, Chile, and Singapore signed the world's first DEPA remotely in 2020 using electronic signatures.\[^{[64]}\]

DEAs differ from digital trade treaties by not emphasizing strong rules, compulsory commitments, and potential trade sanctions, although the texts mirror and expand the digital trade disciplines of CPTPP, which most countries signing these new deals have already agreed upon.\[^{[65]}\] Instead, DEAs promote cooperation towards "interoperability" of digital regulations and standards through optional "modules," ranging from cybersecurity to artificial intelligence, which can be used in other FTAs. The DEPA carrot may sit on top of the CPTPP stick, which the UK is hoping to join.

Current DEPA members include Chile, New Zealand, and Singapore, but South Korea and Canada have begun the application process for joining DEPA.\[^{[66]}\] China is also negotiating access (open to all WTO members),\[^{[67]}\] but it is widely perceived that the country's regulation of cross-border data flow and data storage may need changes.\[^{[68]}\] However, DEPA's modular nature could allow China to align on other areas instead.\[^{[69]}\] Given the increasing hostility between the US and China, this process may be challenging, as the US will undoubtedly apply diplomatic pressure on DEPA members despite not being formally part of the agreement. If China stays out of DEPA it will spare the UK a potential diplomatic headache.

Singapore has subsequently initiated a Digital Partnership with the European Union, characterized by more limited terms, and has begun discussions with the European Free Trade Association (EFTA).\[^{[70]}\] The EU agreement adopts the phrase "data free flow with trust," originating from the G20, G7, and World Economic Forum.\[^{[71]}\] This term signifies a commitment "towards ensuring trusted cross-border data flows in compliance with data protection rules and other public policy objectives, including public security and public order."\[^{[72]}\]

**Comprehensive and Progressive Trans-Pacific Partnership (CPTPP)**

In 2018, the UK surprised the global community by announcing its intention to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). The 11 CPTPP members include Asian economies like Japan and Singapore, Australia and New Zealand, and American countries such as Canada, Mexico, and Chile. Notably, the US withdrew from the agreement, despite initially being a major proponent.

Formal accession procedures began in summer 2021,\[^{[73]}\] and in March 2023, the CPTPP Accession Working Group (AWG) confirmed the UK's compliance with existing CPTPP rules and its provision of high-standard market access offers.\[^{[74]}\] Joining the CPTPP could have numerous effects on the UK economy, but the government has not thoroughly discussed the practical implications despite some limited consultations.\[^{[75]}\] China has also applied for membership but has not received a positive response like the UK.\[^{[ix]}\]
Fact checkers found the government exaggerated the benefits of the treaty. CPTPP will only add 0.08% to UK GDP over the next ten years but it may have more important effects on geopolitical alignment and British public policy than on hard economics. CPTPP sits alongside the new defence agreement with the US and Australia to provide the latter with nuclear submarines to counter the perceived threat of China. Brexit advocates celebrate CPTPP, openly and loudly claiming that this treaty makes Brexit irreversible by locking the UK into a separate regulatory regime. Technically, it will be possible for the UK to abandon the CPTPP, but in practice it will be difficult to disentangle any new regulations and standards.

The consequences of the treaty for the UK have only started to sink in after accession was announced. Trade campaigners warn that the UK has committed to Investor State Dispute Settlement (ISDS) clauses that allow companies to sue the government over regulations they deem are unfair breaches of the deal. The main headline issue is the news that the UK will have to relax current tariffs – inherited from the EU – designed to reduce imports of Malaysian palm oil, which is a major cause of deforestation. Besides being terrible news for the environment and climate change, this is one of the clearest examples of how divergence from the EU necessitates more controls at the border between the UK and the bloc. The EU will be keen to ensure that cheaper Malaysian palm oil does not enter the single market, undercutting its industry and undermining its environmental policies.

Digital trade provisions within the CPTPP resemble those in the UK-Japan agreement we discuss above. Similar commitments are found in over a dozen agreements in the Pacific region. There is not yet a similar debate about the impacts on digital regulation and privacy, but this is only a matter of time. Privacy scholars and advocacy groups have raised concerns about the potential negative effects of CPTPP on data protection, and the challenges it presents for UK regulations.

**Priority Negotiations in 2023**

**India**

India is a major trade priority for the UK due to its large market and English-speaking population, as well as its history as a British colony. Formal negotiations began in January 2022, initially focusing on goods such as automobiles and renewable energy, but also encompassing digital trade, intellectual property, and other issues. India seeks increased opportunities for its workers to travel to the UK. At the time of writing, the ninth round of trade negotiations was scheduled for May 2023, with roughly half of the 26 chapters in the agreement closed; digital is unlikely to be among the concluded chapters.

India is a major provider of digital services outsourcing, and this deal could expand that sector. UK companies might become a gateway for EU and other countries to access more affordable Indian ICT services, as these countries have stricter data transfer restrictions.

The UK’s strategic priorities include commitments to free and trusted cross-border data flows, preventing unjustified data localization, and maintaining high standards for personal data protection. India’s promotion of data localization policies to boost domestic digital innovation might pose a challenge in negotiations.
India currently lacks a comprehensive privacy law, but it is in the process of enacting one. The latest draft of India's Data Protection Bill, released at the end of 2022, has been called "business-friendly" and removes previously proposed controversial provisions to regulate "non-personal data." The new bill allows for transfers to certain countries under a regime like EU adequacy. However, human rights groups have criticized the bill for granting the government excessive power and potentially enabling surveillance, which could lead to legal challenges in any UK-India deal.

Business groups have proposed a digital trade chapter and specific legal reforms, but these remain uncertain. If India could elevate its data protection standards to meet the UK's, this could pave the way for a more extensive deal with the EU. However, it is more likely that the UK will lower its requirements instead.

Ukraine

The UK announced an Agreement in Principle for a digital trade agreement with Ukraine in November 2022. Ukraine is a signatory of the Council of Europe's Convention 108+ on data protection and is working on aligning its law with the GDPR. Although Ukraine has candidate status to join the EU, there are significant obstacles that may also pose problems for free data flows between Ukraine and the UK.

Relationship with the EU

The UK fully departed from the EU on December 31, 2020, following years of negotiations, transition periods, and delays. The comprehensive Trade and Cooperation Agreement (TCA) governs the relationship between the UK and the EU, covering various aspects of their economic relationship, from fisheries and nuclear energy to digital trade. The TCA sets out the terms for a level playing field of cooperation and competition. Though the TCA is the most extensive agreement the EU has signed, its terms differ significantly from full EU membership.

The TCA aims to maintain continuity in essential areas and establish parameters for future divergence. The UK's national strategy for foreign policy and defence emphasizes that the TCA safeguards the UK's regulatory autonomy while allowing for cooperation when appropriate.

Digital Trade in the EU-UK Agreement

The TCA includes a digital trade chapter that reflects standard EU policy but adds new data protection commitments not found in any other EU trade deal.

Other TCA provisions may impact digital trade, such as general exceptions, competition rules, health, cybersecurity, and finance. Spam and consumer protections are also present, albeit in more general terms than current shared regulations. The agreement excludes areas like audio-visual media, broadcasting, gambling, and certain regulated legal services.

The EU views data localization and data flows as separate policies, which can sometimes be difficult to distinguish. The EU considers GDPR as a system for enabling protected cross-border data flows and discourages mandatory data localization requirements. These include forcing the use of computing facilities in the territory and storage of data, but also mandating specific technical certification
The TCA does not contain a general prohibition on cross-border data flow restrictions, aligning with the EU's approach. Compared to the UK's treaties with Japan, Australia, and New Zealand, the TCA's digital provisions are less far-reaching. The TCA's practical impact on digital trade may become more evident as regulatory regimes diverge.

Data Protection and Regulatory Autonomy

The standard EU approach to data in trade deals has been to ring-fence its GDPR data protection regulatory regime to control cross-border data flows. This is achieved through "horizontal provisions for cross-border data flows and for personal data protection" in any EU FTA. These standard clauses feature anti-localization requirements, a weak commitment to cooperation on regulatory issues, and wording designed to protect EU data protection from legal challenges.

The TCA contains a more complex formulation, protecting the regulatory autonomy of the parties within certain conditions, in contrast to the older EU model text that directly safeguards personal data and privacy protection. The clause on data mirrors wider provisions elsewhere in the TCA on the right to regulate in a non-discriminatory manner as understood under trade.

The impacts on data protection regulation are unclear. The European consumer association BEUC has expressed concerns that this wording could leave EU data protection vulnerable to challenges by the UK. They argue that the TCA's public policy exception regime, modelled on World Trade Organization treaties, could pose a risk to the EU's data protection model. While it is theoretically possible for the UK to challenge the EU GDPR regime, it is more likely that the UK will use the new text to protect its regulatory autonomy from EU challenges.

Changes to the Domestic Data Protection Regime

The successive governments the country has had since Brexit have been working on a program of deregulation around data protection, intending to diverge from the EU GDPR model. Departing from GDPR would impact the privacy rights of people in the UK and possibly undermine the higher standards set by the EU. In March 2023, Rishi Sunak's government published a revised Data Protection and Digital Information Bill (No. 2) that extensively amends the UK GDPR and related legislation inherited from the EU.

The new legislation followed from the UK's National Data Strategy from 2020, which set out a vision for a data-driven society and economy, outlining changes to the UK GDPR and data protection framework in areas such as:

- reducing barriers to innovation and facilitating research,
- reducing burdens on businesses by removing compliance and accountability requirements,
- increasing the use of data in the delivery of public services, law enforcement and national security,
- transforming the national data authority – the Information Commissioner Office (ICO) – to focus more on growth,
- facilitating cross-border data flows to boost trade.
The Bill also addresses other data-related areas regulated separately from GDPR, such as digital identities, spam phone calls, cookie banners, and the national registration of births and deaths. Some proposed changes, like removing many GDPR compliance and accountability requirements, have been taken even further in the updated Bill.

The government claims that the new Bill was "co-designed with business from the start,"[105] but support is not universal among businesses. Some smaller companies worry that removing conditions for data processing for commercial scientific research will disproportionately benefit large tech companies with vast research labs and data.[106]

There are also concerns about the government's extensive powers to change the law without a full debate and approval by Parliament, which could undermine public confidence in UK data rules.[107]

Human rights organizations have called for the Bill to be scrapped due to concerns about the substance of the reforms and the lack of consultation with civil society. [108] The Bill arrives amid other legal reforms that threaten the right to privacy and the entire UK human rights framework.[109]

Changes to privacy law may be popular with many people who view GDPR as burdensome and complex while positive effects are more subtle.[110] The government has proposed removing requirements for consent for cookies, seeing it as a popular measure that can get support from tabloid press.[x] Proposals to replace cookie banners with browser controls to avoid “consumer fatigue” have been voiced by the Information Commissioner Office (ICO), the UK’s national data protection authority, for some time.[x] The draft law is problematic because it deals with the problem by simply removing the current need for consent, moving to an opt-out system that actually puts more responsibility on consumers under the guise of protecting them from annoying banners. Browser controls may or may not materialize at some point in the future. The consumer group Which? has carried out research that challenges the government’s view that consumers do not care about the use of cookies. They found that consumers wanted control over cookies but complained about the lack of standardisation in how cookies are explained and consent is presented.[xiii]

One proposal that is certain to garner broad support is bringing fines for nuisance calls and texts in line with GDPR’s strong penalties of up to 4% of global turnover.

**A Domestic Data Regime That Pits Privacy Rights Against Growth**

The proposed domestic data regime changes seem to prioritize business growth over consumer privacy rights. While the proposals acknowledge the need for consumer trust in the digital economy, they provide businesses with more opportunities to bypass consumer concerns. These changes would affect anyone whose data is handled in the UK, not just British citizens.

Many of the proposed changes address well-known data protection issues and areas of confusion or conflict. However, the bill tends to favour data users over those affected by data usage. Some of the changes may not be drastic, and certain new uses of data might already be possible within the existing regime, but the overall impact could undermine consumer privacy.
Controversial changes in the bill include:

**Identifiable Information and Anonymous Data**

The bill changes how any organisations processing data related to people in the UK handle situations where data may not directly identify an individual but could be indirectly used to identify them using other data. This is a known problem due to the increasing availability of third-party data for matching. For example, in 2014 a New York taxi company released data that had all identifiers of drivers and clients removed, but computer scientists could still identify many of the trips, including those of the actor Bradley Cooper.[111] High-profile incidents like this have created an awareness of the risks of data that is meant to be deidentified.

The Bill sets out that organisations only need to consider the immediate context when assessing the risk of depersonalized data identifying individuals. This is the narrowest approach possible, designed to promote the uses of big data and AI, but it increases the risks and could encourage a lack of care when organisations handle this kind of data.

**Automated Decisions, AI, and Profiling**

The bill addresses another long-standing data protection controversy in Europe: the rights of people in relation to decisions based solely on automated processing, including profiling, which produce legal effects concerning them or similarly significantly affect them. [112] This covers important decisions such as Human Resources processing, credit offers, and other impactful choices.

Under GDPR, people have the right not to be subject to certain decisions based solely on automated processing, except when it is necessary for a contract, it is required by law, or consent is provided. This is one of the areas of GDPR where we find divergent opinions. On one side are those who see the right as an absolute ban on certain types of fully automated decisions, requiring that a human is placed in the loop before a decision is made. [xiv] The other side, where the UK government is firmly placed, claims that this must be a right only to specific safeguards after the decision is made, rather than as a general prohibition on certain types of solely automated decision-making. This approach is seen as vital for the expansion of AI systems.[113]

The Bill removes any ambiguity in UK law, by deleting the relevant GDPR article that contains the right not to be subject to high-impact automated decisions without prior human intervention altogether. Instead, we find mandatory safeguards to inform affected people and allow them to contest the decision.

While highly symbolic, the short term may be limited, partly because the existing framework is not fully understood and enforced. Organizations already must inform individuals about automated processing and their right to object to it. Individuals also have the right to ask for human intervention and express their point of view after the automated decision has been made. Organisations must also ensure that they have appropriate measures in place to protect individuals’ rights, freedoms, and legitimate interests when engaging in automated decision-making. However, there is only a weak effort to ensure these safeguards work. In the medium term, this could create unforeseen risks for individuals from evolving AI technologies. The UK government has chosen to put these innovations before any protections for consumers, instead of finding a more balanced approach.
Restrictions on Data Rights
The bill proposes restrictions on existing data rights, allowing organisations to refuse "vexatious or excessive" requests from people to access or amend their data or object to certain practices. This change has garnered most attention, but while it lowers the bar for rejections, it may have limited impact since organizations already had the right to reject certain requests.

However, data litigation experts at AWO, a European digital policy consultancy, have found that the new rules and time limits for complaints could have very negative impact on consumers, who could face waiting 20 months or longer to resolve even basic breaches of their data rights that are supposed to be solved in weeks. [114]

This pro-business stance risks signalling to unscrupulous companies that abusing consumers is acceptable. It seems more like a political choice than a solid policy, as there is no evidence that data rights are being abused.

AWO also states that the Bill creates new grey areas where businesses will be free to interpret the law in the way most convenient to them by enabling new legal grounds to facilitate data processing and permissive rules on data reuse. In their view, “the net result will be more hidden processing, fewer data subject rights, and the need for more complaints and challenges from data subjects.”  [115]

Reducing Burdens on Businesses
The UK government initially considered proposals to replace the accountability framework under GDPR with a more flexible approach, like those in Canada, Australia, or Singapore, using "Privacy Management Programmes." [116] This would allow organizations to develop self-defined, risk-based policies. While Privacy Accountability Frameworks can work well in some situations, having each company create its own systems could lead to confusion for organizations that have already spent resources adapting to GDPR.

The Data Bill does not completely overhaul privacy requirements for companies, but it does remove many obligations, including transparency and consultation of risk assessments, and notification to the ICO of high-risk activities.

The Bill replaces the role of Data Protection Officer with a senior responsible individual and Data Protection Impact Assessments with "assessments of high-risk processing." These changes could be substantial or largely cosmetic, but they risk conveying the message that privacy is no longer important.

One significant change is the removal of the requirement to document how data is used. The Bill eliminates the obligation for organizations to keep records of personal data processing. Under the new regime, only organizations carrying out high-risk activities will have to comply with a simplified regime, as determined by the regulator. This may appear to be a minor change, but data records are the foundation for managing personal data in all organizations. Without these records, it is difficult to see how organizations will be able to comply with many duties.

Another change is the removal of the obligation for certain foreign organizations processing data of people in the UK to appoint a legal representative. This GDPR provision was not well understood and
caused complications after Brexit, as many organizations had to appoint a representative for the EU and another for the UK. However, removing the role altogether means that consumers and the regulator will not have a contact point if there is a problem.

International Data Transfers as Trade Instruments

The draft proposals to promote cross-border data flows could have a more significant impact on consumers outside of the UK than the domestic reforms. The consultation documents preceding the current data bill proposed to create a unique UK framework for data transfers, promote the liberalisation of data flows at the WTO and G7, and make the UK "the world's most attractive data marketplace." [117]

The framework for international data transfers positions data protection as a core aspect of economic policy, which is a major departure from the EU's approach (where personal data is primarily treated as part of the right to privacy) and aligns more with the perspective of the US and Indo-Pacific region. [118]

Under the current UK system, any cross-border transfers of personal data should not generate additional risks for the individuals whose data is being sent. The easiest mechanism for transfers is an adequacy decision, where the UK declares that the receiving jurisdiction provides essentially equivalent protections to the UK's. [119]

The UK plans to change the adequacy regime to make the process faster and more transparent, but it also wants to lower the bar for assessing protections in the receiving country. The new data protection test in the bill requires that protection standards are not materially lower than in the UK, instead of requiring those to be essentially equivalent. [120] The current Data Bill clarifies that any mechanisms for data transfers currently in place will remain valid under the new regime.

While policies to make adequacy decisions more transparent and systematic could lead to better and more consistent decisions if applied properly, [121][122] there is a risk that adequacy decisions could become mere tools for trade policy. The government has published a list of priority countries for new "data partnerships" that will be fast-tracked for adequacy decisions. [123] Except for South Korea and Brazil, none of these countries have high data protection standards. British ministers will also be able to create collective adequacy decisions for "groups of countries, regions, and multilateral frameworks" and remove statutory obligations to review decisions every four years, instead opting for ongoing monitoring. [124]

In practice, consumers will always have a harder time enforcing their rights against a rogue company that is located abroad and they need all the help they can get. Adequacy is not a magic bullet and requires vigilance and enforcement. Despite its limitations, adequacy is a very useful tool to provide trust for consumers and enormous advantages for businesses. Adequacy shifts the responsibility for the risk assessment of data transfers from consumers and organisations to the government, saving substantial legal costs.

Creating Practical Interoperability With Asia Pacific Data Regulations

The UK Data Bill allows for the creation of new private international data transfer mechanisms that the government could recognize in UK law. [125] This would enable the UK to join the Global Cross-Border
Privacy Rules (CBPR) regime, a US-led framework based on the Asia-Pacific Economic Cooperation organization (APEC-CBPR) rules.\textsuperscript{[126][127]} Open to countries worldwide, CBPR offers an alternative to GDPR and facilitates accession to the CPTPP and future data transfers to the US.

The UK formally applied to become a member of the CBPR in April 2023 while it hosted the international working group of the framework.\textsuperscript{xv} There are no details on the process or timeframe, but the CBPR has published its working documents, including a process for new members, and we should expect an acceleration of its development.\textsuperscript{xvi}

The CBPR regime is based on private business commitments and certification by commercial entities, underpinned by a legal regime enabling consumers to enforce certain breaches under private law. This provides a much lower level of consumer guarantees than the current UK framework.

**Challenges to Independent Data Regulation**

British organizations like the Open Rights Group have criticized the weak enforcement action of the Information Commissioner Office (ICO), the UK's national data protection authority.\textsuperscript{[128][129]}

The current proposals may not improve enforcement while forcing the regulator to adopt a pro-business stance. The UK data strategy proposes changing the ICO's role to introduce a statutory obligation to prioritize competition, innovation, and economic growth, aligning the ICO's international activities with the UK government's diplomatic and economic strategy.\textsuperscript{[130]} These changes may compromise the regulator's independence, a key legal requirement.\textsuperscript{[131]} Moreover, Privacy International (PI) has urged caution with regard to such duties imposed upon the ICO, "because of the risk that the ICO would be put under pressure to consider potential negative implications on competition of limiting data processing/enforcing data subject...\textsuperscript{[132]}

**Risks to the EU Adequacy Decision**

Data transfers between the EU and the UK are currently treated as internal transfers for regulatory purposes, under reciprocal adequacy decisions.\textsuperscript{[133]} However, concerns abound that radical changes to the UK's data regime could affect data flows with Europe, coming both from civil society and businesses.\textsuperscript{[134]} The situation is uncertain, with some legal scholars arguing that the current reforms are not radical enough and the UK will still be following the Convention 108+ of the Council of Europe, which could provide a basis for EU adequacy.\textsuperscript{[135]}

If the EU no longer considers the UK to provide essentially equivalent privacy protections, there could be significant economic implications.\textsuperscript{[136][137]} Adequacy is crucial for the continuity of many economic activities and services across the UK and EU. Estimates of the direct legal and administrative costs of
replacing adequacy range from £1.6 billion to £420 million. The UK government estimates wider costs at between £2.10 billion and £3.78 billion of lost trade in ten years, but this figure may be too low.

The key question is whether the UK government is willing to risk adequacy for regulatory autonomy and potential future trade, or if they believe the new regime is compatible with the EU. Many EU institutions have expressed misgivings about free data flows with the UK, exemplified by unique safeguards like the sunset clause in the UK adequacy decision,\[^{138}\] which expires after four years in June 2025 unless extended.\[^{139}\] However, there are enormous pressures to maintain the status quo, as any changes would also have huge costs for the EU economy and cause many problems for collaboration in other areas.

Even if the EU takes no action, privacy advocates may go to court to challenge the arrangements, as happened in the Schrems II case,\[^{140}\] where the legal mechanism to send data from the EU to the US was invalidated by the Court of Justice of the EU.\[^{141}\] The Schrems II judgement forced the EU and US governments to come up with a new framework, the European Union-US Data Privacy Framework, that provides additional safeguards,\[^{142}\] but it is already under pressure from the European Parliament because it “fails to create actual equivalence in the level of protection”.\[^{143}\]

**Conclusion**

The UK’s current agenda of unleashing data’s power across the economy and society, alongside expanding free trade across the Asia-Pacific region, is rooted in a deep deregulation ideology. This is driven by Brexit-related priorities to promote free trade, pro-business deregulation, and restriction of consumer rights while favouring the Indo-Pacific region, particularly English-speaking former colonies with shared cultural and ethnic heritage. Although a change in government may not result in a significant shift of priorities due to the contentious nature of EU-related discussions in the UK, the systemic transformations underway are worth considering.

While these policies currently coexist with the nominal policy to maintain the post-Brexit status quo with the EU, including data adequacy arrangements, ongoing conflicts over custom arrangements and finance persist. The UK risks further breakdowns with unpredictable consequences, potentially positioning itself as a data deregulation haven.

However, this approach may be on the wrong side of history, as global debates on data governance and the digital economy seem to shift towards increasing consumer privacy rights, platform regulation, and higher international standards. The UK could end up isolated as an unsafe destination for data, undermining global data standards.

A more constructive approach would be to avoid false equivalences on the interoperability of data regimes and focus on developing better international standards to embed in trade deals. While the current regime has its flaws, some proposals could create a more agile and flexible system. Nevertheless, there are risks, such as weakened public scrutiny and potential bias in decisions. The regulatory shift might facilitate trade agreements with the US and other countries, but it could also affect current trade with the EU, raising concerns for consumers and digital trade.
Endnotes


[52] Ibid.


[79] Briefings for Britain. (2023, March 31). Brexit is now irreversible!! Briefings For Britain. Retrieved from https://www.briefingsforbritain.co.uk/brexit


[95] @t_streinz. (2021, January 19.) "However, in line with previous practice, the Commission insisted on this being a separate issue. @Trade_EU explicitly lists it as an 'unilateral measure' that was not covered by the negotiations." [Tweet]. Twitter. Retrieved from https://twitter.com/t_streinz/status/1351558954405556225


[115] Ibid.


