THE EU AS A DIGITAL TRADE ACTOR – THE CHALLENGE OF BEING A GLOBAL LEADER IN STANDARD-SETTING

Elaine Fahey*

Abstract:
The EU's ambitious and far-reaching efforts at de facto and de jure regulation of high data standards is increasingly expressed as a global standard. It is mostly in the area of protection of privacy standards where the EU has innovated but which raise complexities for the place of standards more broadly in digital trade. The challenge remains for the EU to upload its standards to multilateral agreements. However, developments as a digital services tax show the significance of the regulation of the digital matters outside of trade agreements
Keywords: digital trade, data privacy, European Union, global actor, WTO

Overview

There is no universal formula for data related issues in a trade agreement, which may cross-cut everything from cybersecurity, intellectual property, transparency to frictionless movement of tech workers. It is also complex to capture digital services in statistics as to their precise importance to the economy, because of the difficulty of defining digital services and business. Nonetheless, it is a truth universally acknowledged that every ambitious twenty-first century trade agreement is in want of a holistic and robust chapter on electronic commerce (e-commerce mainly hereafter).[1] Governments and organisations are learning how to engage in this complex new field. Whereas most Regional Trade Agreements (RTAs) treat e-commerce as its own standalone chapter, a few embed e-commerce provisions as part of a broader chapter.[2] Yet, tech sectors are predominantly services-based sectors and increasingly perceive Free Trade Agreements (FTAs) to be ineffective for their needs. The framework of FTAs has observed the insertion of specific provisions such as a ban on encryption or rules on intermediaries' liability becoming part of the agreements through concerted efforts of lobbying rather than as an evolution of a holistic solution attempt to a complex multi-dimensional problem of digital trade.[3] FTAs are easily said then to exacerbate rule fragmentation and even the values of multilateral venues and the role of international law in general.[4]

The EU's Digital Strategy published in early 2020 indicates in unequivocal terms that the institutional, regulatory and international dimension of the EU as a global digital player is synonymous with its policy evolution.[5] The EU's ambitious and far-reaching efforts at de facto and de jure regulation of high data standards is increasingly expressed as a global standard, with a rising number of mimics, adopters and transposers of its GDPR.[6] The EU has had data transfer regimes and flows which have counted as some of the largest in the globe (e.g. EU-US Privacy Shield 2016-2020 covering over one billion citizens, EU-Japan Data Adequacy Decision, relating to the world's third

* Professor of Law, Institute for the Study of European Law, City Law School, City, University of London. Email: elaine.fahey.1@city.ac.uk
[1] Richard Wolfe, "Learning about Digital Trade: Privacy and E-Commerce in CETA and TPP" (2019) 18(S1) World Trade Review 63.
[2] Mark Wu, "Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System" (2017) RTA Exchange International Centre for Trade and Sustainable Development and Inter-American Development Bank, 8.
[3] Mirra Burri, "The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation" (2017) 51 University of California Davis Law Review 65, 130.
[4] Ibid, 127.
[5] European Commission, "Shaping Europe's digital future: Commission presents strategies for data and Artificial Intelligence" (February 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273> accessed 15 December 2020.
[6] European Commission, "Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World" COM (2017) 07 final.

largest free trade agreement).[7] The EU has tended to conclude RTAs with a chapter dedicated to Trade in Services Establishment and Electronic Commerce.[8] It has historically adopted a somewhat inconsistent approach to e-commerce, which it tends to merge with Trade in services, establishment and electronic commerce, i.e. rather than giving e-commerce (or indeed digital trade) a standalone chapter. In more contemporary agreements such as the EU-Canada Comprehensive Economic and Trade Agreement (CETA), a standalone e-commerce chapter is found. By contrast, the EU-Japan Economic Partnership Agreement (EPA) has a broad chapter that covers trade in services, investment liberalisation and e-commerce. However, in more recent negotiations with Australia, Mexico and the UK, digital trade has become a standalone text, where it shifts the nomenclature thereto. Advanced economies connected closely to the EU such as the EEA have not necessarily sought historically a broad e-commerce chapter either.[9] The latest US-China Phase One Trade Agreement does not address emerging issues such as privacy protection and data regulation relating to digital trade, despite the significance of US-Sino relations for ICT and tech issues. National security issues relating to Huawei, Wechat, Tiktok and the sales of 5G equipment are also left unaddressed by the agreement. There are thus striking inconsistencies even across some of the largest scale trade agreements as to how to formulate digital trade.

The transformations of the Internet have also been associated with new measures that inhibit digital trade, such as "data localisation" measures, e.g. requiring localisation of data servers and providers, local content policies, or discrimination against digital services or providers not locally based, to gain jurisdictional control. However, there are important regulatory gaps emerging as to such issues. Against the backdrop of pre-Internet World Trade Organisation (WTO) law, many of these disruptive changes have demanded regulatory solutions outside the multilateral trade forum and States around the world have used in particular the venue of Preferential Trade Agreements (PTAs) to fill in the gaps of the WTO framework.[10]

There is no settled definition of "digital trade" or "electronic commerce", and so characterisations differ greatly.[11] The WTO is currently seeking, through its Joint Statement Initiative (JSI) on Electronic Commerce, to negotiate a plurilateral agreement on trade-related aspects of electronic commerce, ideally eliminating tariffs and discrimination on data flows, preventing data localisation and providing security for digital transactions. However, progress appears limited for now. Here, digital trade is said to be understood in two fashions—narrow and broad.[12] As to the narrow understanding: digital trade is equated to commerce in products and services delivered via the Internet. The second fashion is much broader and relates to enabling innovation and the free flow of information in the digital networked environment. This distinction is far from academic and has profound policy implications. For instance, the US approach tends to focus more on the "digital" nature of digital trade, while the Chinese approach prefers to address the issue from the traditional "trade" perspective. While the EU has arguably shifted "mid-way" between these two positions, its resting position remains perhaps more curious and convoluted than this. As a result, the framework that now regulates contemporary digital trade is not coherent and is highly fragmented.[13] It has arguably left a significant and fragmented gap that the EU has directly and indirectly filled. It is

[7] On the status of the EU-US Privacy Shield: Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (*Schrems II*) [2020] EU:C:2020:559; Kenneth Propp and Peter Swire, "After Schrems II: A Proposal to Meet the Individual Redress Challenge" (*Lawfare*, 13 August 2020) <https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge> accessed 15 December 2020.

[8] Wu, "Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System" (n 2) 8.

[9] Ibid, 8.

[10] Mira Burri and Rodrigo Polanco, "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset" (2020) 23 Journal of International Economic Law 187; Henry Gao, "The Regulation of Digital Trade in the TPP: Trade Rules for the Digital Age" in Julien Chaisse, Henry Gao and Chang-fa Lo (eds), *Paradigm Shift in International Economic Law Rule-Making* (Springer 2017) 345.

[11] Andrew D Mitchell, "Towards Compatibility: The Future of Electronic Commerce within the Global Trading System" (2001) 4 Journal of International Economic Law 685.

[12] Ibid, 703-704.

[13] Burri and Polanco, "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset" (n 10).

mostly in the area of protection of privacy standards where the EU has innovated but which raise complexities for the place of standards more broadly therein and beyond. The EU has sought to upload its standards recently to multilateral fora, beginning with the WTO, as will be developed below. The challenge remains to achieve technical agreement for high standards. Beyond this, significant EU regulatory dpushes outside of trade agreements e.g. digital service taxes may suggest that the future of digital trade is dictated to outside of trade agreements. The EU will also face a complex task to implement increasingly strict CJEU caselaw on privacy.

This article thus examines: 1) the emerging relationship of RTAs with data protection and privacy, 2) the EU horizontal strategy on data flows, 3) the EU-Japan Economic partnership Agreement (EPA) as a study of EU best practice in digital trade, 4) recent EU negotiation objectives on digital trade, followed by Conclusions.

1) Complex emerging relationship of RTAs with data protection and data privacy: the EU's innovations

While approximately 80 or more Preferential Trade Agreements (PTAs) include provisions on privacy, many are non-binding and even in the most large-scale formulation of trade agreements, such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and United States–Mexico–Canada Agreement (USMCA), data has been overlooked as to a robust and precise relationship to privacy, where more economic rationalisations of privacy rights have prevailed. This reflects the highly variable position of the major actors and tensions between the regulatory goals of data innovation and data protection. Thus, while many new generation trade agreements have provisions on digital trade, they are neither consistent, coherent nor cohesive.

A shift took place evident in EU agreements on enhancing the security of personal data at international level, attempting to raise the level of privacy protection in electronic communications and avoid obstacles to trade requiring transfers of data.[14] It has amounted to a revolutionary shift in the formulation thereof.[15] Many activities such as sharing information on regulation, laws and programmes on data protection, domestic regimes for the protection of personal data, technical assistance in the form of exchange of information and experts, research and training activities, joint programmes, dialogues, consultations on data protection, etc. constitute activities warranting cooperation relating to data.[16] In a small number of treaties, parties commit to publish information on personal data protection to users of e-commerce, including how individuals can pursue remedies and how businesses can comply with any legal requirements.[17] Trade agreements increasingly deal with personal data protection with reference to the adoption of domestic standards, making the EU position less isolated. Some agreements merely recognise the importance or benefits of protecting personal information online. Yet increasingly treaties commit to adopt or maintain legislation and regulations that protect the personal data or privacy of users. These protections relate to the processing and dissemination of data, including administrative measures or the adoption of non-disciplinary practices. EU agreements include qualifications to these standards e.g. to give the parties the right to define and regulate their own levels of protection of personal data in pursuit of public policy objectives and not to be required to disclose confidential or sensitive information or data.[18] EU FTAs have pioneered that in the development of online personal data standards each party shall take into account existing international standards.[19] Other FTAs tend to emphasise the criteria or guidelines

[14] Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and the Republic of Moldova, of the other part [2014] OJ L260/4, art 13.1 and art 99(d).
[15] Svetlana Yakovleva and Kristina Irion, "Pitching trade against privacy: reconciling EU governance of personal data flows with external trade" (2020) 10(3) International Data Privacy Law 201.
[16] Burri and Polanco, "Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset" (n 10).
[17] Ibid. See also Yakovleva and Irion, "Pitching trade against privacy: reconciling EU governance of personal data flows with external trade" (n 15).
[18] Agreement between the European Union and Japan for an Economic Partnership (EU-Japan EPA) [2018] OJ L 330/3, art 18.1.2.h and art 18.16.7.
[19] Free Trade Agreement Between the European Union and the Republic of Singapore [2019] OJ L 294/2, art 8.57.4; Comprehensive and Enhanced Partnership Agreement between the European Union and the European Atomic Energy

of relevant international organisations or bodies e.g. APEC Privacy Framework, OECD Recommendations of the Council concerning Guidelines governing the protection of privacy and transborder flows of data (2013).[20] USMCA explicitly recognises the APEC Cross Border privacy rules system as a valid mechanism to facilitate cross-border information transfers while protecting personal information. TPP made one more step, because it has specific and hard obligation. TPP (Article 14.8) states that Each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce.

More recently, USMCA has a chapter (Ch. 19) on digital trade and not e-commerce unlike CPTPP (Ch. 14) and so distinct differences between two major agreements exist as to international privacy regimes cited, data localisation, interactive computer services and so on. It is thus not clear what precise implications these agreements have for the prevention of algorithmic bias, protection of critical infrastructure or the protection of national security as between the agreements, which appears a missed opportunity and concern, given their scale.[21] The EU has pioneered special chapters on the protection of personal data including discrete principles' such as purpose limitation, data quality, proportionality, transparency, security, right to access, rectification and opposition, restrictions on onwards transfers, protection of sensitive data, enforcement mechanisms, coherence with international commitments and cooperation between the parties to ensure an adequate level of protection of personal data.[22]

One of the most progressive of EU trade deals, the EU-Canada Comprehensive Economic and Trade Agreement (CETA), has numerous provisions cross-cutting data yet without regulating its flow or positively providing protections to personal data.[23]

2) Best practice in EU Digital Trade to date? EU-Japan EPA Digital Trade Provisions

The EU's recent Economic Partnership Agreement (EPA) with Japan is a useful study of best contemporary modern practice in next generation EU trade agreements with a developed economy. The e-commerce chapter of the EU–Japan FTA is much more substantial than that in EU–Korea and EU–Canada FTAs.[24] Some suggest that the e-commerce chapter in EU–Japan FTA is almost comparable to that of TPP except that the former does not have provisions on computing facilities, and its requirements on consumer and data protection are soft.[25] The request of source code is prohibited by the EU–Japan FTA, while the location of computing facility is not covered. Key provisions of the EPA (in Ch. 8 thereof) are outlined here by way of example.[26]

Community and their Member States, of the one part, and the Republic of Armenia, of the other part [2018] OJ L23/4, art 197.2; Economic Partnership Agreement between the CARIFORUM States, of the one part, and the European Community and its Member States, of the other part [2008] OJ L289/3, art 119.2; Agreement establishing an association between the European Community and its Member States, of the one part, and the Republic of Chile, of the other part [2002] OJ 359/3, art 202.

[20] Agreement between the United States of America, the United Mexican States, and Canada 12/13/19, art 19.8.2.

[21] See Patrick Leblond, "Digital Trade at the WTO- The CPTPP and CUSMA Pose Challenges to Canadian Data Regulation" (2019) CIGI Papers No 227 <https://www.cigionline.org/sites/default/files/documents/no.227.pdf> accessed 15 December 2020; Elaine Fahey and Isabella Mancini, "The EU as an Intentional or Accidental Convergence Actor? Learning from the EU-Japan Data Adequacy Negotiations" (2020) 7 International Trade Law and Regulation 99.

[22] Interim Agreement with a view to an Economic Partnership Agreement between the European Community and its Member States, of the one part, and the Central Africa Party, of the other part [2008] OJ L57/2, ch 6, arts 61-65; Economic Partnership Agreement between the CARIFORUM States, of the one part, and the European Community and its Member States, of the other part (n 19), ch 6, arts 197-201.

[23] Instead, data protection either falls under the exceptions (see 28.3(2)(c)(ii) Comprehensive Economic Trade Agreement (CETA) or becomes an object for which the Parties shall "maintain or adopt" (Article 16.4 CETA) or measures or "adequate safeguards" (Article 13.15 CETA) to ensure its protection.

[24] Shintaro Hamanaka, "The future impact of Trans-Pacific Partnership's rule-making achievements: The case study of e-commerce" (2019) 42 World Economy 552, 561.

[25] Hamanaka, "The future impact of Trans-Pacific Partnership's rule-making achievements: The case study of e-commerce", 561.

[26] EU-Japan EPA; Council Decision (EU) 2018/1197 on the Signing, on Behalf of the European Union, and Provisional Application of the Strategic Partnership Agreement between the European Union and its Member States, of the one Part, and

Several agreements explicitly agree to promote the development of electronic commerce only between the parties, or its wider global use or development and the EU-Japan EPA is notable as to the formulation of the latter.[27] The EPA includes specific commitments on domestic regulation, meaning that each party shall ensure that all its measures of general application affecting electronic commerce are administered in a reasonable, objective, and impartial manner. This is accompanied by a best effort commitment not to impose prior authorization or any other requirement having equivalent effect on the provision of services by electronic means.[28] The EPA includes provisions that parties shall not adopt or maintain measures regulating electronic transactions that deny the legal effect, validity or enforceability of a contract, solely on the grounds that it is concluded by electronic means; or otherwise create obstacles to the use of contracts concluded by electronic promotion.[29] While some agreements aim to 'facilitate trade in digital products' or through 'electronic means or technologies', and to improve the effectiveness and efficiency of electronic commerce, or consider e-commerce facilitation as part of general common cooperation activities, other agreements have more concrete obligations- such as the EU-Japan EPA. The EPA has provisions which aim to prevent the denial of the legal validity of a signature solely on the basis that the signature is in electronic form, following the framework of the United Nations Convention on the Use of Electronic Communications in International Contracts.[30]

The EPA has important voluntary cooperation commitments that are understood to be best practice e.g. to "maintain a dialogue" on regulatory issues such as the facilitation of cross-border certification services and which thus seek to institutionalise cooperation as between the parties.[31] The agreement reassesses within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement ('*rendez-vous*').[32] Free flow of data was to be negotiated within three years (Article 8.21), but was agreed earlier than this, as discussed above.

However, some suggest that the textual content of the EPA amounts to a lot less than best practice as to data privacy. For example, Bartl and Irion contended on an earlier draft of the EPA that: that while the Regulatory Cooperation Chapter explicitly states not to interfere with parties' autonomy to regulation in pursuit or furtherance of its public policy objectives, among others, in personal data, this provision does not exclude data flows from the scope of activities, and therefore data privacy issues could be tabled as part of the regulatory cooperation mechanisms.[33] However, it is important to note that the EU-Japan EPA provisions were in a final draft and in existence along with texts on the EU-Mexico modernisation provisions when the EU published its model horizontal texts for the place of trade and privacy in trade agreements.[34] In other words, there are important developments in EU practice taking place at this key point in the development of the GDPR and the EU's practices and perhaps *earlier* critique is overshadowed as a result. It also should arguably be seen in context of the development of convergence of standards substantively in recent caselaw. The EU-Japan EPA will shortly see the EU introduce model articles into the agreement in its *rendez-vous* clauses and subject the agreement to the EU's post-GDPR data protection policies as applied to digital trade. The commitments to multilateralism are also of much significance here in the EPA given the EU's

Japan, of the other Part [2018] OJ L216/1; Strategic Partnership Agreement between the European Union and its Member States, of the one Part, and Japan, of the other Part [2-18] OJ L 216/4.

[27] EU-Japan EPA, art 8.70.

[28] EU-Japan EPA, arts 8.74, 8.75 and 8.76.

[29] EU-Japan EPA, arts 8.74, 8.75 and 8.76

[30] EU-Japan EPA, art 8.77.3.

[31] EU-Japan EPA, art 8.80.2(d).

[32] EU-Japan EPA, art 8.81.

[33] Marija Bartl and Kristina Irion, "The Japan EU Economic Partnership Agreement: Flows of Personal Data to the Land of the Rising Sun" (2017) Amsterdam Centre for Information Law Institute Working Paper <https://www.ivir.nl/publicaties/download/Transfer-of-personal-data-to-the-land-of-the-rising-sun-FINAL.pdf> accessed 15 December 2020.

[34] European Commission, Horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements) (18 May 2018) <https://trade.ec.europa.eu/doclib/docs/2018/may/tradoc_156884.pdf> accessed 15 December 2020.

intentions. The digital trade provisions of the EPA were notably alleged to be significantly capable of being seen as bypassed by the UK-Japan FTA agreed in late 2020, although this appears greatly exaggerated given the relative size of the UK economy to Japan vis a vis the EU. It is also notable that the UK trumpets as innovation the migration of professionals under the agreement which appears ironic given the boost free movement gave the EU economy in the tech sector, providing skills young professionals. Its efforts to portray the agreement as innovative as to AI also are perhaps exaggerated given the place of EU AI regulation on the horizon. The UK-Japan FTA ultimately appears problematic as to data standard protections adopted by the UK if the UK is to join CPTPP and adopt standards at variance with EU standards but these are currently not matters of concern, simply highlighting the regulatory variance challenge of high standards.[35]

3) The EU horizonal strategy on data flows: the bold and the brave?

What has been most significant in theory at least is the very development by the EU of a horizontal strategy on data, governing how the EU integrates cross-border flows of personal data in external trade policy.[36] This strategy developed in the wake of the EU's GDPR and the trade agreements being negotiated in this new era after a number of important policy developments. The far-reaching Commission Communication on Exchanging and Protecting Personal Data in a Globalised world in 2017 set out the mechanisms for international transfers of person data and clarified the criteria to be taken into account in the adequacy mechanism when selecting third countries, in particular in Asia and Latin America.[37] The European Parliament then adopted a targeted resolution "Towards a digital trade strategy" arguing for internal consistency of external trade policy Resolution of 2017.[38] In early 2018, the Commission presented its new position on horizontal provisions on cross-border data flows and personal data protection in EU trade and investment agreements with three major elements with the aim of achieving internal consistency.[39] Article A sets out a declaratory commitment on cross-border data flows and prohibits restrictions in four data and IT localisation requirements. Article B

[35] UK International Trade Department: "Cutting-edge digital & data provisions that go far beyond the EU-Japan deal. These will enable free flow of data whilst maintaining high standards of protection for personal data. We have also committed to uphold the principles of net neutrality, as well as introducing a ban on data localisation, which will prevent British businesses from having the extra cost of setting up servers in Japan", see Department for International Trade, "The UK–Japan Comprehensive Economic Partnership Benefts for the UK" (2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/929065/UK-Japan-Trade-Agreement-sectoral-benefits.pdf> accessed 15 December 2020.

[36] European Commission, Horizontal provisions for cross-border data flows and for personal data protection (n 34).

[37] European Commission, "Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World" (n 6).

[38] European Parliament, Resolution Towards a digital Trade Strategy (2017/2065(INI)), <https://www.europarl.europa.eu/doceo/document/A-8-2017-0384_EN.html> accessed 15 December 2020.

[39] European Commission, Horizontal provisions for cross-border data flows and for personal data protection (n 34):
Article A "Cross-border data flows":
1. The Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy. To that end, cross-border data flows shall not be restricted between the Parties by:
(i) requiring the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of a Party;
(ii) requiring the localisation of data in the Party's territory for storage or processing;
(iii) prohibiting storage or processing in the territory of the other Party;
(iv) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Parties' territory or upon localisation requirements in the Parties' territory.
2. The Parties shall keep the implementation of this provision under review and assess its functioning in 3 years following the entry into force of this Agreement. A Party may at any time propose to the other Party to review the list of restrictions listed in the preceding paragraph. Such request shall be accorded sympathetic consideration.
Article B "Protection of personal data and privacy"
Each Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade.
Each Party may adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data. Nothing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards.
3. For the purposes of this agreement, "personal data" means any information relating to an identified or identifiable natural person.
4. For greater certainty, the Investment Court System does not apply to the provisions in Articles A and B.

sets out unconditional counterbalancing provisions for national measures as to personal data. Article X on regulatory cooperation with respect to digital trade provides a carve out for cross-border data flows and the protection of personal data from the dialogue on regulatory issues. The Commission submitted horizontal provisions on cross-border data flows and personal protection in trade negotiations with Australia, Chile, Indonesia, Mexico, New Zealand and Tunisia and to replace the EU-Japan EPA *rendez vous* clause.[40] It has also reproduced its position in its proposal for the ongoing WTO negotiations on trade related aspects of electronic commerce.[41] The proposals are understood to be positively bold and exceed normative counterbalancing provisions in many trade agreements as to labour standards, environmental protections and sustainable development. The new approach is of unconditionally excepting a party's safeguards to endure the protection of data and privacy needs to be agreed could be understood as a pretext for abuse or unjustifiable data localisation.[42] It can also be understood as upsetting approaches to mutual recognition of data privacy as practised by the EU. On one level, this could stymie the EU's institutionalisation of regulatory cooperation in this field. On the other hand, it suggests consistency on the part of the EU in evolving its standardised approach as an important shift in the EU's protection of data and its consistency with external trade agreements.

It is important to state that the EU's ostensible commitment to data protection and privacy does not only manifest itself in opposition to data flow provisions in trade agreements. In CETA, the EU voiced concerns about the privacy impact of disclosing obligations throughout the agreement. As a result, there are interesting and significant provisions- e.g. Article 10.4.2 (subjecting data sharing regarding temporary entry of business persons to each party's privacy and data protection law); Article 20.5 (affirming that intellectual property related disclose of information was not required except under either party's privacy laws); Article 21.4.e (subjecting provision of proposed regulations to applicable privacy law); Article 32.1 of the Protocol on rules of origin and origin procedures (affirming furnishing or access to information was not required if contrary to either party's personal data protection and privacy law). CETA notably, however, does not include a general free data flow provision.

The CJEU ultimately struck down the Privacy Shield in July 2020 on the basis of US surveillance laws therein and the inadequacy of the Ombudsman as an institutional figure in *Schrems* II.[43] Landmark decisions of the CJEU in *Schrems II* are said to mark key shifts towards data localisation in Europe and less openness, evinced through technology surveillance.[44] The logic of data localisation has evolved through to tech sovereignty.[45] As the EU appears likely to be nudged in the direction of data localisation after its *Schrems II* decision, the '*identity*' of data will matter all the more. Currently, global businesses are grappling with its implementation to enable data flows. *Schrems II a*rguably marks the high-water-mark of EU interventionism in global standard-setting for privacy.

[40] Yakovleva and Irion, "Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade" (n 15).
[41] Communication from the European Union, Joint Statement on Electronic Commerce, "EU Proposal For WTO Disciplines and Commitments Relating to Electronic Commerce" INF/ECOM/22 (2019) <https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf> accessed 15 December 2020.
[42] Yakovleva and Irion, "Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade" (n 15) 219-220.
[43] *Schrems II* (n 7).
[44] Ibid.
[45] European Council, "Special meeting of the European Council (1 and 2 October 2020) – Conclusions" EUCO 13/20 (2020): "…to be digitally sovereign, the EU must build a truly digital single market. Define its own rules, to make autonomous technological choices. At international level, the EU will leverage its tools and regulatory powers to help shape global rules and standards….".

The final section moves *beyond* the contents of trade agreements and considers the place of a Digital Services Tax (DST).

4) Digital Services Tax- the EU's role

A global digital services tax has a complex place to play in contemporary digital trade chapters in trade negotiations. It is in short legally irrelevant from a trade-logic point of view yet highly contextually salient. A new multilateral OECD proposal in 2019 brings together common elements of three competing proposals from member countries, and is based on the work of the OECD/G20 Inclusive Framework on BEPS, which groups 134 countries and jurisdictions on an equal footing, for negotiation of international tax rules, making them fit for purpose for the global economy of the 21st Century.[46] Multilateral negotiations have been progressing poorly, particularly after US Trump administration withdrawal therefrom in 2020.

On 21 March 2018 the EU introduced a digital taxation package, seeking to "establish a modern, fair and efficient taxation standard for the digital economy", critiquing outdated corporate tax rules, and the need for an international solution.[47] A French Digital Services Tax (DST) was adopted by the French parliament in 2019 to apply retroactively from 1 January 2019 creating the GAFA tax on digital services, inspired by the EU Directive for which no consensus was found. France has agreed to delay collecting a new tax on multinational technology firms until the end of 2020 pending developments at the OECD.[48] Many other EU Member States have followed suit e.g. Czech Republic, Austria, Spain and Italy. The United States Trade Representative (USTR) had threatened to impose swingeing retaliatory tariffs on $2.4bn (£1.8bn) of French goods, including champagne and cheese, after the tax was passed in July 2019 and launched an investigation, with the tariffs pending the OECD developments. In February 2020, the USTR Initiated Section 301 Investigations of Digital Services Taxes under the US 1974 Trade Act which are currently are ongoing as to a 'broad church' of countries: Austria, Brazil, the Czech Republic, India, Indonesia, Italy, Spain, Turkey, and the United Kingdom, and the EU. The USTR stated that the US President was concerned that many of the trading partners of the US are adopting tax schemes designed to unfairly target US companies, "with the US being prepared to take all appropriate action to defend our businesses and workers against any such discrimination."[49] The aggressive pursuit of allies by the US Trump administration as to the impact of DSTs remains to be seen where US companies are the target of such taxes but also paradoxically are being compelled to return supply chains to the US or to be subjected to significant taxation issues domestically, as in the case of Facebook.[50]

---

[46] OECD, "Public Consultation Document Secretariat Proposal for a 'Unified Approach' under Pillar One 9 October 2019 – 12 November 2019" <https://www.oecd.org/tax/beps/public-consultation-document-secretariat-proposal-unified-approach-pillar-one.pdf> accessed 15 December 2020.

[47] European Commission, Proposal for a Council Directive on the common system of a digital services tax on revenues resulting from the provision of certain digital services COM(2018) 148 final; A European Parliament resolution of 16 December 2015 called for legislative proposals adjusting the definition of "permanent establishment" to grasp the digital presence and introducing a definition of "minimum economic substance"; Cf. Maria Kendrick, "The Future of EU Differentiated Integration: The Tax Microcosm" (2020) 7(S2) Journal of International and Comparative Law, forthcoming; See Franco-German Joint Declaration on the taxation of digital companies and minimum taxation <https://www.consilium.europa.eu/media/37276/fr-de-joint-declaration-on-the-taxation-of-digital-companies-final.pdf> accessed 15 December 2020; Johannes Backer and Joachim Englisch, "EU Digital services Tax: A Populist and Flawed Proposal" (*Kluwer International Tax Blog*, 16 March 2018) <http://kluwertaxblog.com/2018/03/16/eu-digital-services-tax-populist-flawed-proposal/?doing_wp_cron=1594366177.2683420181274414062500> accessed 15 December 2020.

[48] "France signals breakthrough in US digital tax talks" *Financial Times* (20 January 2020) <https://www.ft.com/content/345a5850-3ba1-11ea-b232-000f4477fbca> accessed 15 December 2020.

[49] United States Trade Representative, "USTR Initiates Section 301 Investigations of Digital Services Taxes" (*USTR*, 6 February 2020) <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2020/june/ustr-initiates-section-301-investigations-digital-services-taxes> accessed 15 December 2020 2020; Office of The United States Trade Representative, "Initiation of Section 301 Investigations of Digital Services Taxes" (Docket No USTR-2020-0022, 2020) <https://ustr.gov/sites/default/files/assets/frn/FRN.pdf> accessed 15 December 2020.

[50] Josh White, "The IRS takes Facebook to court over its Irish tax structure" (*International Tax Review*, 19 February 20020) <https://www.internationaltaxreview.com/article/b1kdw0nx8h3jz1/the-irs-takes-facebook-to-court-over-its-irish-tax-structure> accessed 15 December 2020.

Until now, digital services taxes had no specific relationship to trade agreements. However, they increasingly appear awkward and complex hindrances where other forms of duties are the subject of trade agreements. Ultimately, the "awkward space" between DSTs and trade agreements entails that all law-makers globally can confidently pass DSTs for now. It seems likely that in the absence of mutual consensus within the EU 27 on the DST that an enhanced cooperation mechanism legal basis may be pursued. Revenue generation has become a significant issue in the COVID-19 era of EU law post-Brexit, with bigger financial gaps to be breached. The national EU MS DSTs were to be temporary, while waiting for a longer-term and coordinated solution by OECD members. However, the significance of the requirement of revenue in the midst of COVID-19 for the EU will render its adoption in some form, possibly by enhanced cooperation, all the more likely.[51] The European Commission is now considering a DST as part of the financing package for its proposed COVID-19 recovery plan, as well as a digital levy and a financial transaction tax.[52] One of the first approaches by a European government to the US Biden administration elect was to negotiate on the future of a DST. It is thus a context of much significance. Ultimately, however, the EU desire to regulate and govern Big Tech will entail that the EU's position thereon has global effects.

Conclusions

The global legal order appears increasingly fragmented as between multiple regimes in digital trade. The EU is an innovator in high standards of data flows and has caused a paradigm shift in discussions of privacy and protection that many others are following now, nationally and regionally. The EU is a longstanding supporter of WTO innovations on ecommerce developments but this forum looks unlikely to deal with high standards of privacy in data flows. The EU has been a leading data actor for some time on account of its first-mover advantage. All of these high standards statuses are increasingly problematic but not necessarily fatal. The EU and its national data protection authorities are currently struggling with the implementation of *Schrems II*. Most of the world appears to be coming closer to the EU's position but still significant gaps remain. Leading liberal positions but maintaining high standards of privacy remains a conundrum for the EU going forward. The EU has largely adopted historically a mixed position, in-between key actors, i.e. US and China, as a 'middle-ground' actor in digital trade conventionally but this middle ground is unlikely to be the best barometer of change going forward. A transatlantic shift on data and digital trade in the next US administration could have dramatic implications for the future thereof. EU treads a difficult tight-rope in the manner in which it is proceeding. A context of a digital services tax, significant regulation and enforcement of tech companies and lies ahead. However, its impact upon digital trade remains complex and a global standard remains highly unlikely. Ultimately, the EU has started a difficult conversation on privacy and standards but it remains a challenge to see whether its institutionalised vision of data can succeed as much in the next wave of trade, regulation and governance ahead.

[51] European Commission, "An Action Plan for the fair and simple taxation supporting the recovery strategy" COM (2020) 312 final.

[52] European Council Conclusions 17-21 July 2020 Brussels, 21 July 2020 (OR. en) EUCO 10/20.