e-Commerce
Free Trade Agreements, Digital Chapters and the impact on Labour

A comparative analysis of treaty texts and their potential practical implications

ITUC CSI IGB International Trade Union Confederation

Written for the ITUC by: Duncan McCann, Senior Researcher, New Economics Foundation

New Economics Foundation

www.neweconomics.org

info@neweconomics.org

+44 (0)20 7820 6300

@NEF

Registered charity number 1055254

Cover: Adobe Stock

CONTENTS

FOREWORD

E-commerce proposals at the WTO: a recipe for corporate greed

Before the COVID-19 crisis, trust in governments and in democracy itself was collapsing around the world, 60 per cent of the world's workers were in informal jobs with no rights or protections and hundreds of millions of people who in employment were unable to make ends meet. The COVID-19 crisis is having catastrophic effects globally, compounding the existing weaknesses. The push for a WTO "e-commerce" agreement can only further exacerbate inequality and division at a time when the world needs to work as one. It is simply a recipe for yet more corporate greed. Governments are promoting new rules that would further reduce their own authority to regulate in the interests of people, to the extent that they are behaving more as captives of corporations, including giant tech monopolies, than as guardians of the public interest.

Digital technology holds enormous potential for tackling the world's most pressing problems on climate, poverty, inequality, health, education and much more. It has a massive role to play in tackling the spread of the SARS-CoV-2 virus and its consequences. It is now even more important that governments focus their efforts on harnessing technology for the common good, rather than simply being conduits for an agenda that would entrench corporate power and deepen inequality and mistrust.

This report, produced for the ITUC by the New Economics Foundation, reveals several deeply alarming impacts which would arise from an e-commerce agreement, while also exposing elements of some existing trade agreements which are of serious concern.

Control of data is at the heart of the proposals, and through that control of data, the power of digital behemoths such as Amazon would reach new heights. Their power is already far-reaching, due to the failure of governments to apply competition policy to prevent them dominating markets. This market dominance is set to grow even more if governments fail to ensure that the role tech companies play in the COVID-19 crisis in digital tracing and many other areas is done in the public interest with full respect for rights, instead of on the companies' terms.

The report highlights how an agreement on the lines proposed would increase precarious work leading to "Uberisation" of jobs, erode workers' rights, make regulation and enforcement more difficult and increase the power of Big Tech over workers.

With international concern over the implications of artificial intelligence and the deployment of algorithms without accountability, the planned provisions on secrecy of source code would allow corporations to maintain complete opacity and remove means by which victims of corporate malfeasance can achieve remedy for the damage done to them. The use of open source software in public procurement could also be challenged and negated.

It is important to note that the implications of such an e-commerce agreement would extend well beyond the tech sector itself. As data and digitalisation become central to business models in all sectors, rules concerning data affect every part of the economy and every worker, consumer and citizen.

The proposals would hamper, or in some cases eradicate, the potential for small and medium enterprises to grow and thrive, and would even reach into agriculture, where half of the world's workers work. Public services, already underfunded and under assault, would be further eroded by the incursion of digital monopolies into the provision of vital services, while the development of domestic industries, especially in countries which are not yet technologically advanced, would be impeded. Data protection regimes such as the EU's GDPR would also be undermined, and internet neutrality would be at risk.

Big Tech firms are seeking to use a WTO e-commerce agreement to tighten their grip on the global economy and squeeze yet more out of consumers and working people. Much of what they demand is not about trade at all; however, the WTO in its current form is a convenient back door to eliminate labour, privacy, property rights and other standards which are central to democracy.

Indeed, with almost half the world's population still locked out of the internet age, the mission to connect all the world's people must surely take precedence over a drive by some of the world's most powerful and least accountable corporations to extend their power and carve it into stone forever.

The international trade union movement will oppose the development of any agreement, at the WTO or elsewhere, which seeks to so fundamentally undermine the interests of working people and the public at large.

Sharan Burrow, General Secretary
International Trade Union Confederation

INTRODUCTION

When you navigate the internet, send messages or emails, and move around a city using map applications, you create data. These data, when properly analysed, can tell a lot about your behaviour. Big data companies gather your data in return of a "free" service – like an application that helps you measure calories – with your consent granted when you click "I agree" after a lengthy Terms of Use text that you never read.

The value of any one individual's data is pretty low on its own. However, when aggregated in millions of data points, trained algorithms can extract valuable conclusions about consumption, transportation, and work-related and other information. The conclusions are then used in order to target the right consumers at the right time and to pursue workplace rearrangements that would increase productivity.

Big data companies benefit hugely from this large information advantage, and are able to use it to transform the global economy and the world of work to suit their needs. These transformations are now happening outside of worker and democratic control. For instance, wearables, like smart watches, can tell software controllers how we work, and they use the data we produce in order to tighten worker surveillance and control, and potentially in some cases, automate us out of our jobs. Farming applications open up a world of previously unknown information about agricultural tasks, risks, inputs, and future yields that transform the nature of work in these sectors. Big data analytics enables companies to use this knowledge to increase their value-capture in supply chains and take over the value-adding while transforming the sector.

New technologies and the data revolution bear immense opportunities to answer humanity's challenges – global heating, poor quality work, hunger and diseases. However, history shows that not all technological revolutions reach everyone. About 1.2 billion people are still to get to the second industrial revolution when others are launching into the fourth one.

The technological revolution will not benefit us all automatically.

In fact, big companies and their host governments are already working hard to ensure that they maintain control over new technologies and that they set the rules of data governance. For this, they get their governments to agree to specific commitments in trade agreements. The first treaty to contain a whole e-commerce chapter was the 2003 Singapore-Australia free trade agreement (FTA).[1]

The 11th WTO Ministerial Conference may have ended without the adoption of a declaration, but a small number of initiatives were announced. One of them, which announced the intention to start negotiations on e-commerce, came from a group of 70 Members, mostly developed countries. The group was joined by six more countries, and in January 2019 the Members launched plurilateral e-commerce negotiations in the WTO, even though there is no WTO-wide mandate to do so, since a large group of developing countries managed to block the launch of official new negotiations on digital trade. The aim of the plurilateral negotiations is to agree to digital trade provisions that would ensure digital subordinance of small enterprises, a grave shift in the balance of bargaining power between capital and labour, and limited space for developing countries to digitalise with their own strategies.

The e-commerce agreement would create a framework that disciplines our governments' ability to regulate and enforce laws in cyberspace. Uber claims that they are a digital company, not a taxi company, and Fintech claims they provide e-services, not actual loans that should be governed by financial rules. Internet gives them the excuse to evade many aspects of national law and jurisdiction, including taxation. And they want that cemented.

The importance of e-commerce has grown with the development and expansion of the speed and reach of digital networks. In 2019, retail e-commerce sales worldwide amounted to $3.53 trillion and e-retail revenues are projected to grow to $6.54 trillion in 2022.[2] And just as digital is now permeating ever more sectors, the chapters in free trade agreements have also expanded to deal with many issues that are way beyond the original scope of facilitating trade over the internet.

1 Weber, R. (2015, September 10th). *The expansion of e-commerce in Asia-Pacific trade agreements*. Retrieved from https://www.ictsd.org/opinion/the-expansion-of-e-commerce-in-asia-pacific-trade-agreements

2 Statista (2019) *Retail e-commerce sales worldwide from 2014 to 2023*. Retrieved from https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/

For example, one of the most important new areas that is included in trade agreements is the demand for the free flow of data across borders. By including this in trade agreements, the aim is to help ensure that private ownership of data is the default and that transnational corporations should be able to freely move data around the world with minimal or no regulation.

The widening of the scope of the digital chapters along with data's centrality to global trade – it is estimated that in 2020 data flows account for more than 20 per cent of the world's GDP – has led to the WTO negotiations on "e-commerce", which is a deliberate misnomer for "data governance".

A common perception is that the EU and US are diametrically opposed on how their respective digital economies should function. But in fact the proposals from the two economic blocks are remarkably similar. There is one major and important exception, which is with regard to personal data privacy where the EU, through its implementation of the General Data Protection Regulation, has become the global proponent of privacy legislation.

A key element of the strategy has been to package together certain issues on which negotiators believe it will be possible to get agreement more easily, such as spam, authentication or recognising e-contracts, to act as a sort of Trojan horse in order to deliver the real intention of the chapters, which is to ensure the free flow of data across borders and eliminate data localisation requirements along with severely prohibiting source code disclosure

Although the digital revolution has been significant, it is important to remember that it is still a very recent innovation, with the internet recently celebrating its 30th birthday. This means that our institutions and policy framework are still adapting to the changes that the digital economy is driving in the way that we live, work and play.

This is even starker in developing countries, where four billion people do not have access to the internet. Developing countries are now putting in place the first efforts to develop a digital industrialisation agenda aiming at creating local economic activity. Many such countries are still in early stages for creating a legal framework for the protection of personal data and ensuring that digital innovation benefits working people.

Locking in global rules at such an early stage of the development of the internet and digital trade would lock in a status quo which sees ownership and control of data tightly concentrated in the hands of a few corporations while leaving states unable to maximise the public good that comes from digital innovation.

A COMPARATIVE ANALYSIS OF FREE TRADE AGREEMENT PROVISION

In this section we will explore four key texts – the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), the US Mexico Canada Agreement (USMCA), the EU-Japan Economic Partnership Agreement, and the EU submission to the WTO (May 2019) – in order to complete a comparative legal analysis of the texts. The section will cover six different provisions in the digital trade chapter:

1. means of authentication and signatures and electronic contracts;
2. source code;
3. data flows;
4. data localisation;
5. data protection; and
6. open internet access.

In this section we make a number of overarching arguments with respect to the potential issues and impacts that arise from an analysis of the different provisions on digital trade. These are as follows:

- In general, the topics covered in the provisions are not specifically trade issues and therefore are inappropriate for inclusion in free trade agreements. The default position for policy on these topics, therefore, should be to regulate through domestic legislation wherever possible, especially where model legislation exists.
- Indeed, the inclusion of specific digital chapters in international trade agreements is designed to limit the ability of domestic governments to regulate in key emerging areas of the digital economy.
- Digital technologies are already impacting and disrupting our economy irrespective of how and whether they are included in international trade agreements. Nonetheless, these digital chapters will in many instances exacerbate the existing risks of adverse social and economic effects arising from digital disruption by locking in a liberal, under-regulated environment.
- As data and algorithms become ever more central components of our social and economic lives, the importance of digital trade provisions in international trade agreements will also grow.

MEANS OF AUTHENTICATION AND E-SIGNATURES AND ELECTRONIC CONTRACTS

CPTTP	EU-Jap	USMCA	EU Submission to WTO
Article 14.6: Electronic Authentication and Electronic Signatures	Article 8.77 Electronic authentication and electronic signature	Article 19.6: Electronic Authentication and Electronic Signatures	2.2 ELECTRONIC AUTHENTICATION AND ELECTRONIC SIGNATURES
1. Except in circumstances otherwise provided for under its law, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.	Unless otherwise provided for in its laws and regulations, a Party shall not deny the legal validity of a signature solely on the grounds that the signature is in electronic form.	1. Except in circumstances provided for under its law, a Party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form.	1. Members shall not deny legal effect and admissibility as evidence in legal proceedings of electronic signature solely on the basis that it is in electronic form.
2. No Party shall adopt or maintain measures for electronic authentication that would: (a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction; or (b) prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their transaction complies with any legal requirements with respect to authentication.	2. A Party shall not adopt or maintain measures regulating electronic authentication and electronic signature that would: (a) prohibit parties to an electronic transaction from mutually determining the appropriate electronic authentication methods for their transaction; or (b) prevent parties to electronic transactions from having the opportunity to establish before judicial or administrative authorities that their electronic transactions comply with any legal requirements with respect to electronic authentication and electronic signature.	2. No Party shall adopt or maintain measures for electronic authentication and electronic signatures that would: (a) prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods or electronic signatures for that transaction; or (b) prevent parties to an electronic transaction from having the opportunity to establish before judicial or administrative authorities that their transaction complies with any legal requirements with respect to authentication or electronic signatures.	2. Members shall ensure that parties to an electronic transaction are not prevented from: (a) mutually determining the appropriate electronic authentication methods for their transaction; (b) being able to prove to judicial and administrative authorities that the use of electronic authentication or an electronic signature in that transaction complies with the applicable legal requirements.
3. Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its law.	3. Notwithstanding paragraph 2, each Party may require that, for a particular category of transactions, the method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its laws and regulations.	3. Notwithstanding paragraph 2, a Party may require that, for a particular category of transactions, the electronic signature or method of authentication meets certain performance standards or is certified by an authority accredited in accordance with its law.	3. Notwithstanding paragraph 2, certification requirements by an authority accredited in accordance with domestic law or certain performance standards may apply for a particular category of transactions, the method of authentication or electronic signature. Such requirements and standards shall be objective, transparent and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned.
4. The Parties shall encourage the use of interoperable electronic authentication.		4. Each Party shall encourage the use of interoperable electronic authentication.	4. To the extent provided for under domestic law, Members shall apply paragraphs 1 to 3 to other electronic processes or means of facilitating or enabling electronic transactions, such as electronic time stamps, electronic registered delivery services or website authentication.

When people and companies trade, there need to be ways to validate both the details of the transaction and that the people and companies engaging in the transaction are who they claim to be. Technology that enables electronic authentication and e-signature are vital to this process. The battle in this area is between businesses that want the minimum number of laws and regulations specifying, limiting or restricting the use of electronic authentication, versus the public interest, i.e., ensuring that the domestic digital trade environment is safe and secure.

This provision is specifically being pushed by the EU, which has had an e-signature directive since 1999, recently updated by the Electronic Identification and Trust Services for Electronic Transactions Regulation (better known as the eIDAS Regulation) which came into force in July 2016. Due to these earlier regulations and the efforts of EU businesses to comply, this is an area where the EU has a leadership position from a technology perspective, and so there is a direct opportunity to drive business by putting these requirements in treaties.

Although overall provisions on electronic authentication and e-signature appear in only half of trade agreements[3], they appear in detailed form in all four of the documents that we looked at in detail.

This is a section where the marked similarity in the texts is what stands out. The key point that they all reinforce is that "A party shall not deny the legal validity of a signature solely on the basis that the signature is in electronic form." This should be read together with the text that prohibits governments from adopting or maintaining any requirements which would "prohibit parties to an electronic transaction from mutually determining the appropriate authentication methods for that transaction" and, if challenged, that those parties should be able to argue in court as to the validity of the signature. The key point that they want to reinforce is that it should not be up to the government to tell two (or more) parties that are engaged in a transaction what technology, system or implementation model they should use. Instead, the free trade agreements stipulate that it should be up to the parties to the transaction itself to determine what the best authentication technology to use is.

The CPTPP and USMCA and the EU-Japan text all start with the same exemption that the provisions apply "Except in circumstances otherwise provided for under its law." It is interesting that the EU submission to the WTO does not contain the same phrase, since it would seem to be an important derogation that clearly has wide support among other countries, including the EU itself, since it forms part of the EU-Japan text. Finally, they all allow governments to establish performance standards "for a particular category of transactions", without in any way defining what those categories could be. The phrasing of these powers together with the fact that they do not have to secure a legitimate public policy objective could mean that these will provide governments enough room to ensure that transactions that require high levels of security, such as finance or identity, could be legislated for. Again, the CPTPP and USMCA and the EU-Japan text specifically allow for the ability of governments to require that authentication protocols are "certified by an authority accredited in accordance with its law". The EU submission on the other hand provides considerable detail on the limits of the actions of government in this regard. It seeks to require that all requirements are "objective, transparent and non-discriminatory and shall only relate to the specific characteristics of the category of transactions concerned."

Part of the challenge of deciphering the actual impacts of these various provisions is that two key terms remain undefined, namely "parties" and "electronic transaction". So although the parties to the agreements may know how they apply, it is very hard for those without the definitions to come to firm judgements.

What we can do is highlight some potential problems with allowing parties to decide between themselves which authentication technology to use.

- Firstly, there is an efficiency agreement which holds that in a world of multiple private authentication standards, there is additional cost due to lack of interoperability and the need to manage multiple systems.
- Secondly, dominant companies could set standards, which often are expensive to comply with, and then penalise those who do not comply. A recent example involved Visa and Mastercard and their implementation of anti-fraud software in their merchant network with the stated purpose of ensuring that the payment system was secure. However, the scheme has been called a "near scam" by the National Retail Federation in the US, and in a legal challenge it was asserted that "the system is less a system for securing customer card data than a system for raking in profits for the card companies via fines and penalties."[4]
- Thirdly, there is also the serious risk that the standard being pushed by companies is not secure enough. As Richard Hill notes, governments often have to intervene due

3 Wu, M. (2017). *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for Multilateral Trade System.* RTA Exchange. Retrieved from http://e15initiative.org/wp-content/uploads/2015/09/RTA-Exchange-Digital-Trade-Mark-Wu-Final-2.pdf

4 Zetter, K. (2012, November 1). *Rare legal fight takes on credit card company security standard and fines.* Retrieved from https://www.wired.com/2012/01/pci-lawsuit/

to market failure because "externalities associated with insufficient security: the costs of a security breach are borne largely by entities other than the company that suffered the breach because of inadequate security."[5]

- Finally, there are also good consumer protection grounds for government setting standards, since otherwise consumers may struggle to understand whether the myriad of authentication technologies are really secure.

Ultimately, this topic is not well suited to being set down in free trade agreements. The model law[6] proposed by UNCITRAL is a much better way to incorporate these requirements into national law frameworks because it allows countries the opportunity to adapt the legislation to local needs and requirements.

5 Hill, R. (2017). *Notes on & E-signatures and Trade*. Our World is Not for Sale. Retrieved from https://ourworldisnotforsale.net/2017/Hill_E-signatures.pdf
6 UNCITRAL (2001) *Model law on electronic signatures with guide to enactment*. Retrieved from https://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf

SOURCE CODE

CPTTP	EU-Japan	USMCA	EU Submission to WTO
Article 14.17: Source Code 1. No Party shall require the transfer of, or access to, source code of software owned by a person of another Party, as a condition for the import, distribution, sale or use of such software, or of products containing such software, in its territory. 2. For the purposes of this Article, software subject to paragraph 1 is limited to mass-market software or products containing such software and does not include software used for critical infrastructure. 3. Nothing in this Article shall preclude: (a) the inclusion or implementation of terms and conditions related to the provision of source code in commercially negotiated contracts; or (b) a Party from requiring the modification of source code of software necessary for that software to comply with laws or regulations which are not inconsistent with this Agreement. 4. This Article shall not be construed to affect requirements that relate to patent applications or granted patents, including any orders made by a judicial authority in relation to patent disputes, subject to safeguards against unauthorised disclosure under the law or practice of a Party.	Article 8.73: Source Code 1. A Party may not require the transfer of, or access to, source code of software owned by a person of the other Party. Nothing in this paragraph shall prevent the inclusion or implementation of terms and conditions related to the transfer of or granting of access to source code in commercially negotiated contracts, or the voluntary transfer of or granting of access to source code, for instance in the context of government procurement. 2. Nothing in this Article shall affect: (a) requirements by a court, administrative tribunal or competition authority to remedy a violation of competition law; (b) requirements by a court, administrative tribunal or administrative authority with respect to the protection and enforcement of intellectual property rights to the extent that source codes are protected by those rights; and (c) the right of a Party to take measures in accordance with Article III of the GPA. 3. For greater certainty, nothing in this Article shall prevent a Party from adopting or maintaining measures which are inconsistent with paragraph 1, in accordance with Articles 1.5, 8.3 and 8.65.	Article 19.16: Source Code 1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory. 2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure	2.6 Transfer or access to source code 1. Members shall not require the transfer of, or access to, the source code of software owned by a natural or juridical person of other Members. 2. For greater certainty: (a) the general exception, the security exception as well as the exceptions in the paragraph 2 of the GATS Annex on Financial Services apply to measures adopted or maintained in the context of a certification procedure; (b) paragraph 1 does not apply to the voluntary transfer of or granting of access to source code on a commercial basis by a natural or juridical person, for instance in the context of a public procurement transaction or a freely negotiated contract. 3. Paragraph 1 is without prejudice to: (a) requirements by a court, administrative tribunal, or by a competition authority to remedy a violation of competition law; (b) the protection and enforcement of intellectual property rights; and (c) the right to take any action or not disclose any information that is considered necessary for the protection of essential security interests relating to the procurement of arms, ammunition or war materials, or to procurement indispensable for national security or for national defence purposes.

Source code is the set of instructions or rules that a computer programme follows, and is written in a way that humans can understand. It is used for everything from software in our phones, smart appliances and cars, to the algorithms used to sort information for us on the internet, such as Google's search engines or Facebook's newsfeed, to the protocols that manage our traffic lights and national energy infrastructure.

Source code is already included in intellectual property and trade secrets protections across the globe. Where subject to patent protection, it is already an offence for a person, company or government to access, share or copy source code, without legal justification. Patent protection often requires the party seeking protection to divulge the code to the patent office. For those not wishing to do that, they could still use trade secrets protection to ensure their code is not improperly accessed or shared. Trade secrets are protected by Article 39 of the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). This provision in the digital

trade chapter is therefore concerned solely with the power of governments and their agents, like courts and regulators, to take actions that would require the transfer of or access to source code as a condition of being allowed to operate in a particular country.

It is important to stress that there are many legitimate reasons why a government may require a company to share their source code. Contemporary examples of governments range from requiring it for specific legal cases, such as intellectual property disputes, to more general reasons, like ensuring economic stability or investigating potential biases. Here are some examples of governments legally requesting source code that may not be permitted under currently agreed and proposed free trade agreements:[7]

- Some financial regulators, such as the US, require firms operating High Frequency Trading algorithms to disclose their source code so that the regulators can "review code, training data and proprietary formulas" to understand what had caused previous flash crashes[8] in the stock market and to prevent them happening in the future.[9]
- A significant proportion of gambling is now done through electronic machines, apps and websites where the odds of winning is determined by software. The gambling regulators therefore check the source code running electronic gambling machines to ensure that the chance of winning is fairly programmed.[10]
- Toyota cars were involved in a number of suspicious accidents resulting in death. They were required to hand over their source code to regulators who engaged NASA to analyse the data. Although they were not able to find a smoking gun, they found enough to force the company to hand it over to the victim's IT consultants, who found the root of the problem.[11]

Helping to bridge the digital divide through technology transfer has been a legitimate expectation in some sectors for some countries,[12] although seen as a trade barrier in the US.[13] As more and more products and services are run by source code, the prohibition on the requirement to share it as a condition of market access would make technology transfer involving source code illegal under the trade agreement.

Although there is considerable divergence between the four treaty texts analysed, there is overwhelming agreement on the core of what the section should cover, namely that "No Party shall require the transfer of, or access to, source code of software owned by a person of another Party." Only the USMCA adds to this by extending what is covered to include "an algorithm expressed in that source code". The CPTPP and USMCA also stipulate explicitly what the other texts appear to assume, namely that the source code cannot be required to be shared or accessed "as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory".

The extension of the exclusion to algorithms in the USMCA poses a new and more serious challenge even when compared with the already problematic source code provisions. An algorithm is different from the source code itself in so far as it describes the basic logic that a computer program should follow. An algorithm can be understood as a recipe that involves a series of sequential steps with options and decision points, whereas source code is the language and form by which these instructions are written by people to be interpreted by computers. But at the core of an algorithm is ultimately an idea, and as such not currently specifically protected under existing intellectual property regimes. TRIPS has already allowed companies to start to use trade secrets protection for their algorithms. The US proposal goes far beyond this and extends the already problematic protections for source code to the algorithms themselves.

The bulk of the sections on source code are concerned with the instances when the agreed prohibition on sharing source code can be overridden. The evolution of the exceptions is a perfect example of the challenges of agreeing text on matters which continue to evolve rapidly and where some may fail to foresee the full implications of what they are signing up to. The Japan-Mongolia agreement, the first to contain such a provision, only had an exception for critical infrastructure. In the CPTPP the parties realised that carving such a narrow exception list

7 Smith, SR. (2017, December 10) *Some preliminary implications of WTO source code proposal.* Third World Network Briefings. Retrieved from https://www.twn.my/MC11/briefings/BP4.pdf

8 A flash crash is an event in electronic securities markets wherein the withdrawal of stock orders rapidly amplifies price declines. The result appears to be a rapid sell-off of securities that can happen over a few minutes, resulting in dramatic declines.

9 Rieke, A. Bogen, M. & Robinson, D. (2018) *Public Scrutiny of Automated Decisions: Early lesson and Emerging Methods.* Upturn and Omidyar Network. Retrieved from https://www.omidyar.com/sites/default/files/file_archive/Public%20Scrutiny%20of%20Automated%20Decisions.pdf

10 Gambling Commission (2018). *Testing strategy for compliance with remote gambling and software technical standards.* Retrieved from http://www.gamblingcommission.gov.uk/pdf/Testing-strategy-for-compliance-with-remote-gambling-and-software-technical-standards.pdf

11 Safety Research & Strategies Inc. (2013, November 7) *Toyota Unintended Acceleration and the big bowl of Spaghetti code.* Retrieved from http://www.safetyresearch.net/blog/articles/toyota-unintended-acceleration-and-big-bowl-%E2%80%9Cspaghetti%E2%80%9D-code

12 Smith, SR. (2017, December 10) *Some preliminary implications of WTO source code proposal.* Third World Network Briefings. Retrieved from https://www.twn.my/MC11/briefings/BP4.pdf p.4

13 Fefer, R. (2019 March 29) *Digital Trade.* Congressional Research Service. Retrieved from https://fas.org/sgp/crs/misc/IF10770.pdf

would undermine the way that patent law generally works, which requires the handing over of the code in order to get the protected monopoly status.

They therefore expanded the exceptions to include patent law. TiSA extended the exception to legitimate public policy objective (including competition law), albeit knowing that Parties have historically found it very difficult to satisfy the exemption, due to the narrow way in which the legitimate public policy test has been interpreted in the case law.[14] In the EU's submission to the WTO they have listed the exemptions more specifically to include competition law, intellectual property and national security considerations. Finally, the USMCA decided to try another route altogether by no longer trying to create an exhaustive list of fields in which access to source code could be required but instead chose to focus on setting out who could legitimately request the data under which circumstances. In the formulation of the USMCA, as long as the requirement to share source code comes from a "regulatory body or judicial authority" for the purpose of an "investigation, inspection, examination, enforcement action, or judicial proceedings", then it should be permitted. The addition of the word "specific" can be seen as protection against blanket requirements by parties, meaning the source code could only be accessed in specific cases once some form of official proceedings had been instigated by the state.

Another serious issue identified in the EU–Japan FTA and the EU submission to the WTO is that although it allows governments to require disclosure of source codes to remedy a violation of competition laws, it is debatable whether the language would cover the disclosure of the code in order to prove whether a violation had taken place. Yet this is an almost essential prerequisite to the need for a remedy itself. A recent example can be seen from the automotive industry, where Volkswagen's fraudulent software for monitoring emissions was only confirmed when non-state researchers were able to analyse the source code – something that may not be possible in the future.

The evolution of exemptions within the agreements is normal and demonstrates the problem with locking in specific detailed rules before we really understand what is required and the full range of exemptions needed. Although it is clear that in the more recently ratified agreements and proposals, such as the USMCA or the EU submission to the WTO, the exemptions are better drafted, they still leave important cases where source code should be shared unexpressed. As the examples cited earlier show, the non-disclosure of source code poses problems beyond the narrow realms of competition, intellectual property and national security. The USMCA acknowledges this, but its focus on disclosure "to the regulatory body" means that in important cases it may not be possible to share the source code with specialist lawyers or technology experts who are often key to establishing whether there is a case to answer and any remedy may be required. Allowing non-disclosure to these kinds of actors to become the norm will make it much harder to monitor the performance and ensure the compliance of corporate source code. Even getting the text perfect still poses problems for agreements that have already been signed, since the texts do not update automatically as problems are identified and drafting improved.

The proposal around source code supports the corporate strategy that businesses should endeavour to keep their code secret in order to maximise their profit. However, this may not be the best way to keep us all secure. The US Department of Defense prefers to work with open source software because "making source code available to the public significantly aid[s] defenders ... and improves reliability and security." This reasoning shows why we should be very cautious about accepting the notion that source code, and the algorithms that they run, are best kept secret – especially as the areas that will be governed by such code are ever expanding through digitisation and automation. Ultimately, as the Open Rights Group have noted, "these clauses could be used to challenge any public procurement perceived to give preference to open source."[15]

The extension of the prohibition to request source code beyond that already enshrined in patent and trade secret protection represents a brazen attack on the ability of government to ensure that software, in its myriad of applications, is keeping us and our data safe, secure and private.[16] And it is also a short-sighted attack, in terms of the longer-term interests of Western geo-political interests. This is because just as the provision prevents a country demanding to see proprietary code from one of the US tech giants, as was the drafters' principal intention, it will also prevent US and EU governments from looking into Chinese or Russian code as well.

14 World Trade Organisation. *Technical Information on Technical Barriers to Trade.* Retrieved from https://www.wto.org/english/tratop_e/tbt_e/tbt_info_e.htm
15 Ruiz, J. (2019, March 14) *US red lines for digital trade with the UK cause alarm.* Retrieved from https://www.openrightsgroup.org/blog/2019/us-red-lines-for-digital-trade-with-the-uk-cause-alarm
16 Knowledge Ecology International. (2015, December 29) *KEI statement on TPP for the January 12, 2016 hearing of the United States International Trade Commission.* Retrieved from https://www.keionline.org/wp-content/uploads/KEI-USITC-TPP-29Dec2015.pdf

CROSS-BORDER DATA FLOWS

CPTTP	EU-Jap	USMCA	EU Submission to WTO
Article 14.13: Location of Computing Facilities 1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.	Article 8.81 Free Fow of Data The Parties shall reassess 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.	Article 19.12: Location of Computing Facilities No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.	2.7 CROSS-BORDER DATA FLOWS 1. Members 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 by: (a) requiring the use of computing facilities or network elements in the Member's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Member; (b) requiring the localization of data in the Member's territory for storage or processing; (c) prohibiting storage or processing in the territory of other Members; (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Member's territory or upon localization requirements in the Member's territory.

As the digital economy grows and sectors increasingly rely on data as a key input to almost any business they need, especially for large multinational businesses, to move data easily across national borders is becoming a key demand of industry.[17] The aggregation of massive datasets from multiple countries holds out the possibility of helping address some of our global challenges as well as boost global trade and improve our health. A senior employee at the OECD underlined the importance of cross-border data flows for the wider trade negotiations when he stated that "data flows are important, you just won't believe how mind-bogglingly important they are for trade today."[18] While this can be the case, and where possible, data flows should be enabled, this is not the same as demanding that all forms of data, especially that which is personal and sensitive, should be able to cross the border freely without any restriction, control or oversight.

A very interesting aspect to the provisions around cross-border data flows is that there are no common clauses that are shared across all the four key texts that are under analysis reflecting the fact that there is considerable disagreement between key parties. There is commonality in the case of the two US-related texts and again in the case of the two EU-related texts. This reflects the different way that the US and the EU view the cross-border data flows.

In the EU-Japan agreement, there is no provision around free flow of data – only a commitment to look at the issue again in three years time.

Both the CPTPP and USMCA seek to make the free flow of data the default position with both of them requiring parties to "allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." One interesting point is that the CPTPP frames the obligation in the positive

17 The Software Alliance (2017) *Cross-Border Data Flows*. Retrieved from https://www.bsa.org/files/policy-filings/BSA_2017CrossBorderDataFlows.pdf
18 Gonzalez, JL. (2019, June 3) Don't panic! The hitcheker's guide to cross-border data flows. OECD. Retrieved from https://www.oecd.org/trade/hitchhikers-guide-cross-border-data-flows/

that "each party shall allow" whereas the USMCA states that "no party shall prohibit". Although both the CPTPP and the USMCA allow parties to adopt measures to constrain the free flow of data when this "achieves a legitimate public policy objective", this has rarely enabled countries the policy freedom that a layman's reading of the words suggests. This is because "legitimate" has been interpreted in a WTO dispute to mean widely recognised policy solution,[19] while only considering protecting health, environment and privacy as acceptable. This means that novel approaches in sectors, especially ones undergoing digital transformation, could be ruled illegitimate, even when concerned with health, environment or privacy, despite being a valid policy objective. This is especially true when combined with the necessity test that a policy does not "impose restrictions on transfers of information greater than are required to achieve the objective." This has meant that in 44 attempts to use this method to derogate from a particular provision, only one has been successful.

Probably most interestingly, the EU submission to the WTO has a much weaker commitment to cross-border flows when it states that "Members are committed to ensuring cross-border data flows to facilitate trade in the digital economy." The requirement to "commit to ensure" cross-border flows offers parties much greater freedom to restrict cross-border flows than the USMCA's text, which states: "No Party shall prohibit or restrict the cross-border transfer." Because the EU wording offers greater flexibility to the parties, there is no need to balance a strong prohibition with a series of complex derogations.

What is interesting is that the EU clearly considers this compatible with the General Data Protection Regulation (GDPR), which is the most stringent data protection regime in the world, even when far from perfect. Indeed, Wilbur Ross, US Commerce Secretary, has openly called GDPR an unnecessary barrier to trade.[20]

Under GDPR, companies and the public sector operating in the EU, as well as those handling the data of EU citizens outside the EU, must take measures to protect personal data, something that would almost certainly contravene the provisions in the CPTPP and USMCA, since it would represent a restriction, at the very least, on the cross-border transfer of information, even if that information were personal and too sensitive. This means that the EU will never be able to sign up to such a provision as worded in the USMCA or CPTPP.

It will be interesting to see how the UK proceeds in negotiating its new trade deals given the pressure it will be under to accept US terms to ensure a quick trade deal can be signed while at the same time still having the EU's GDPR on the statute books.

19 World Trade Organisation. *Canada – Patent Protection of Pharmaceutical Products.* Retrieved from http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds114_e.html
20 Ross, W. (2018 May 18) *EU data privacy laws are likely to create barriers to trade.* Retrieved from https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c

DATA LOCALISATION

CPTTP	EU-Japan	USMCA	EU Submission to WTO
Article 14.13: Location of Computing Facilities 1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.		Article 19.12: Location of Computing Facilities No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.	2.7 Cross-Border Data Flows 1. Members 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 by: (a) requiring the use of computing facilities or network elements in the Member's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Member; (b) requiring the localization of data in the Member's territory for storage or processing; (c) prohibiting storage or processing in the territory of other Members; (d) making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Member's territory or upon localization requirements in the Member's territory.

Data localisation requirements – where companies are obligated to locate some or all of their equipment that collects, analyses and transfers data internationally within a particular country – have become the topic of important geopolitical debate. At one extreme of the debate, there is Russia, where all personal data collected from all Russians must be stored and processed domestically.[21] Other countries take a more targeted approach focusing only on certain strategically important or particularly sensitive categories of data, such as Nigeria, which requires government data to be stored within the country, and Australia, which only allows health data out of the country (effectively mandating local storage) in a very narrow set of circumstances. At the other extreme, global tech companies want to see a ban on localisation requirements, viewing them as an impediment that will "limit access to global services" because of the additional cost it imposes on the companies and is seen by the global free trade community as "the principal instrument for protectionism in the information age".[22]

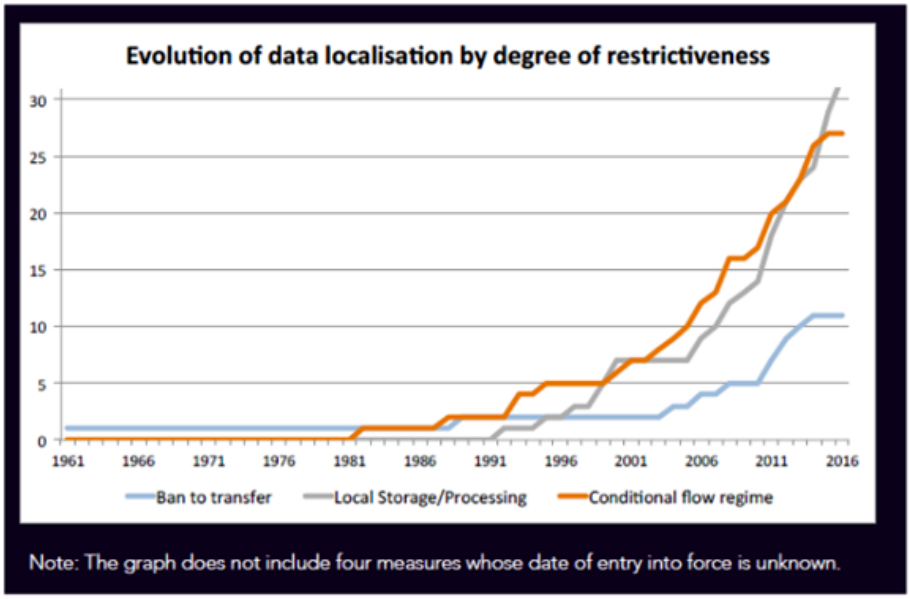
Although localisation requirements have been increasing since the 1990s, as the graph below shows, the TPP, predecessor of the CPTPP, was the first trade agreement to contain such a specific provision severely limiting the contexts in which any form of data localisation is permitted.

There are no common provisions across the four treaties due to the EU-Japan deal failing to include a specific clause on the subject. However, the CPTPP, USMCA and EU submission to the WTO all agree it should never be permissible for countries to require data localisation as a prerequisite for gaining market access to that country. They make this very clear when they state that "no Party shall require a

21 Bowman, C (2017, January 6) *Data Localization Laws: an emerging global trend.* Retrieved from http://jurist.org/hotline/2017/01/data-localization-laws-an-emerging-global-trend.php

22 Chander, A. (2018, October 9) *The coming north American digital trade zone.* Council on Foreign Relations. Retrieved from https://www.cfr.org/blog/coming-north-american-digital-trade-zone

covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory."



Source: ECIPE, Digital Trade Estimates Database

However, the three texts differ greatly when it comes to articulating the circumstances under which parties may apply data localisation requirements, technically known as derogations. The USMCA in effect bars all data localisation requirements in all cases – even for financial (it does so under a different set of rules set forth in the financial services chapter) or health data, two cases where there is a strong justification for requiring it to be stored locally.

The CPTPP does contain a derogation that at first reading seems to allow parties quite a wide margin to operate in. The text states this in relation to data localisation requirements that pursue a "legitimate public policy objective", which includes health, the environment and privacy. However, this wide ranging set of objectives is qualified and constrained by the requirement that it is no greater than the required. This has generally been interpreted quite narrowly within the case law, and the practical experience of attempting to use the derogation tells us that it does not provide the policy space the some countries want in this important area.

There are good arguments both for and against imposing data localisation requirements. As well as the arguments put forward by Big Tech, some digital rights groups also work to limit data localisation requirements. Digital rights groups fear that localisation requirements can be used to "facilitate restrictions on freedom of expression by national governments"[23] as they force tech companies to store data locally which they can then access easily, unlike data stored in a third country. In addition, businesses based in some countries are against data localisation because the local digital infrastructure is of poor quality. [24]

However, arguments for data localisation are also strong. Many are concerned by the amount of data held about us by the tech giants and that localisation could help the development of a more decentralised data infrastructure. This becomes especially important in the context of a growing appetite of countries to develop their own national AI capabilities, since data is the key resource for increasing the capabilities of AI-related technology. There are also a myriad of public policy objectives which could legitimately require data localisation such as a regulatory oversight of the financial system, or other sectors, and national security objectives.

We do not seek to come to a final decision on whether data localisation is good or bad but instead highlight the complexity of the ongoing debate in the subject. One aspect that is very hard to reconcile concerns factors like localisation (which may cause global tech companies to withdraw from the country, leading to impacts for local people and businesses who are not able to use their services) balanced against the fact that the absence of the tech giants may be the only way to ensure that domestic alternatives emerge, since they can be almost impossible to develop in an open and free market. Indeed, our main conclusion in this section is that this area is not suitable to be part of trade negotiations. India is playing a high profile role in this regard and wishing to retain the right to implement data localisation requirements was one of the reasons for its recent rejection of the e-commerce chapter of the Regional Comprehensive Economic Partnership (RCEP) agreement.[25]

23 Ruiz, J. (2018, November 23) *Open Rights Group submission to UK consultation on a new free trade agreement with the United States of America.* Retrieved from https://www.openrightsgroup.org/assets/files/pdfs/submissions/org_fta_consultation_usa.pdf
24 Chander, A. & Uyen, P. (2015 March 13). *Data Nationalism.* Emory Law Journal, Vol. 64, No. 3, 2015. Available at SSRN: https://ssrn.com/abstract=2577947
25 Raghavan, TCA. (2019, October 11) *India rejects RCEP e-commerce chapter.* The Hindu. Retrieved from https://www.thehindu.com/business/india-rejects-rcep-e-commerce-chapter/article29659912.ece

DATA PROTECTION

CPTTP	EU-Japan	USMCA	EU Submission to WTO
Article 14.8: Personal Information Protection5 1. The Parties recognise the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce. 2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies. 3. Each Party shall endeavour to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction. 4. Each Party should publish information on the personal information protections it provides to users of electronic commerce, including how: (a) individuals can pursue remedies; and (b) business can comply with any legal requirements. 5. Recognising that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them.	Article 8.78 Consumer protection 3. The Parties recognise the importance of adopting or maintaining measures, in accordance with their respective laws and regulations, to protect the personal data of electronic commerce users.	Article 19.8: Personal Information Protection 1. The Parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade. 2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade. In the development of this legal framework, each Party should take into account principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013). 3. The Parties recognize that pursuant to paragraph 2, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. The Parties also recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented. 4. Each Party shall endeavor to adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction. 5. Each Party shall publish information on the personal information protections it provides to users of digital trade, including how: (a) a natural person can pursue a remedy; and (b) an enterprise can comply with legal requirements. 6. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. The Parties shall endeavor to exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them. The Parties recognize that the APEC Cross-Border Privacy Rules system is a valid mechanism to facilitate cross-border information transfers while protecting personal information.	2.8 Protection of Personal Data and Privacy 1. Members recognize 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. 2. Members may adopt and maintain the safeguards they deem 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 the agreed disciplines and commitments shall affect the protection of personal data and privacy afforded by the Members' respective safeguards. 3. Personal data means any information relating to an identified or identifiable natural person.

The amount of data we create and share as part of our normal daily lives is increasing exponentially. Ninety per cent of the world's data was created in the last two years, and over 2.5 billion gigabytes of data are produced every day, equivalent to filling over 19.5 million new iPads.[26] Whole companies are built around the principle of relentlessly collecting as much data about internet users as possible, in order to monetise it. The EU has taken the lead in implementing legislation, the General Data Protection Regulation, which requires companies to seek consent when collecting data and governs how they can use and share or sell this data to third parties. This is at odds with most of the rest of the world, exemplified by the US, which has only the most minimal protections for data in place.

This means that the provisions on data protection are without doubt some of the most controversial and difficult, since the fundamental positions of the main

26 Assuming maximum standard iPad storage of 128GB (https://www.apple.com/uk/ipad-10.2/)

negotiating parties (US and EU[27]) are so diametrically opposed.

The texts pertaining to data protections across the four treaties start in reasonably similar fashion – although the small differences actually tell us a lot of the positions of the negotiating parties. In the CPTPP, EU-Japan agreement and USMCA, they all commit to "recognize the economic and social benefits of protecting the personal information." The EU submission to the WTO, however, takes this further by recognising that "the protection of personal data and privacy is a fundamental right." This difference in language between the two is significant, since one merely recognises that there could be a social and economic benefit from implementing data protection policies and leaves countries able to implement legislation, whereas the EU submission phrases "data protection" and "fundamental right" in such a way that arguably requires states to act. This exposes the fundamentally different way that the EU and US view the protection of people's data. The language in the EU-Japan agreement is a mix between the US lead texts of USMCA and CPTPP and the EU submission to WTO by framing data protection legislation as valid and acknowledging existing laws without going as far as calling it a "fundamental right".

The CPTPP and USMCA both seem to require the state to take some positive action to "adopt or maintain a legal framework that provides for the protection of the personal information." However, the clause has an important footnote which provides that "a Party may comply with the obligation in this paragraph by … laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy." This would allow a party to comply merely by placing some oversight on existing voluntary data protection regimes. Voluntary corporate compliance regimes have failed to achieve the aims for which they were implemented[28],[29] and given some of the challenges in enforcing the GDPR in the EU, we should question whether voluntary regimes are appropriate in this area. Whereas the EU-Japan deal is silent on the action that should be taken, the EU submission to the WTO provides clear cover for a party to implement stringent data protection legislation. It provides that countries "may adopt and maintain the safeguards" including "the adoption and application of rules for the cross-border transfer of personal data". The USMCA specifically warns against applying any restrictions on cross-border flows of data unless they are "are necessary and proportionate to the risks presented."

One positive aspect to highlight is the inclusion of data protection as a specific provision, especially since it recognises the role that data protection regimes can play in increasing trust in digital trade. And although it is unlikely that this is how the US will use the provision, it does leave open, even under the USMCA and CPTPP text, for a state to adopt EU-style privacy and data protection rules.

The EU will not sacrifice its position on data protection, since this is part of the region's strategy to differentiate itself from the liberal free market approach of the US and the state capitalism of China. In order for the EU to be able to transfer personal data, its trade partner would need to pass an "adequacy test"[30] to ensure that the data would be protected. There is an interesting argument emerging that should the EU allow the US to insert the footnote mentioned above, which allows voluntary regimes to be sufficient to comply with the provision of the free trade agreement, then this could allow the US to argue that since they comply with their treaty obligations, their protections must be adequate and sufficient. This would represent a massive strategic victory for the US and fundamentally undermine the EU's data protection regime.

The other US strategy to ensure that minimal data protection rules can cooperate with jurisdictions with a high level of protection is contained within paragraph 5 of the provision. The section basically encourages states to mutually recognise each other's privacy and data protection rules, potentially even when they are in no way analogous in terms of impact on data protection. As the Electronic Freedom Foundation notes, what this means in reality is that places like the EU with higher personal data protection laws are strongly encouraged to treat data protections regimes like the US with its weak voluntary arrangements as equivalent enough to ensure that data can be collected, processed and transferred across borders.[31]

27 Arguably also China but none of the agreements analyses for this document involve China.
28 Laufer, W.S. (2013) *Social Accountability and Corporate Greenwashing.* Journal of Business Ethics 43, 253–261 (2003) doi:10.1023/A:1022962719299
29 Koehler, D. (2007) *The Effectiveness of Voluntary Environmental Programs—A Policy at a Crossroads?* Policy Studies Journal Vol 35, Issue 4
30 European Commission. *Adequacy Decisions.* Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
31 Malcom, J. & Maira, S. (2015, November 5) Release of the full TPP text after five years of secrecy confirms threats to users' rights. Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2015/11/release-full-tpp-text-after-five-years-secrecy-confirms-threats-users-rights

OPEN INTERNET ACCESS

CPTPP	EU-Japan	USMCA	EU Submission to WTO
Article 14.10: Principles on Access to and Use of the Internet for Electronic Commerce		Article 19.10: Principles on Access to and Use of the Internet for Digital Trade	2.9 Open Internet Access
Subject to applicable policies, laws and regulations, the Parties recognise the benefits of consumers in their territories having the ability to:		The Parties recognize that it is beneficial for consumers in their territories to be able to:	Subject to applicable policies, laws and regulations, Members should maintain or adopt appropriate measures to ensure that end-users in their territory are able to:
(a) access and use services and applications of a consumer's choice available on the Internet, subject to reasonable network management;		(a) access and use services and applications of a consumer's choice available on the Internet, subject to reasonable network management;	(a) access, distribute and use services and applications of their choice available on the Internet, subject to reasonable and non-discriminatory network management;
(b) connect the end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network; and		(b) connect the end-user devices of a consumer's choice to the Internet, provided that such devices do not harm the network; and	(b) connect devices of their choice to the Internet, provided that such devices do not harm the network; and
(c) access information on the network management practices of a consumer's Internet access service supplier.		(c) access information on the network management practices of a consumer's Internet access service supplier.	(c) have access to information on the network management practices of their Internet access service supplier.

The principle that the internet should be open access and non-discriminatory has been important to the development of the internet and the wider digital economy. The concept of "net neutrality", holds that "internet service providers (ISPs) must treat all internet communications equally, and not discriminate or charge differently based on user, content, website, platform, application, type of equipment, source address, destination address, or method of communication."[32] This principle has real impacts – in fact it is highly debatable whether services like Skype or Netflix would have been able to thrive and grow without being protected from having their traffic discriminated against without basic net neutrality principles.

Without net neutrality, ISPs could limit what you can and can't see. This is already the situation in many authoritarian regimes around the world where they attempt to actively control and manage what information is visible to their citizens and what services they can use. The fear is that were net neutrality to go, then certain content and services may be completely blocked by some ISPs, while they could also force websites to pay or suffer slow data transfer speeds, which might drive many smaller online services out of business.

The text in the trade agreements does not enshrine the principle of net neutrality but instead frames it as "principles on Access to and Use of the Internet for Electronic Commerce", in CPTPP and USMCA, with the EU simply referring to "open internet access". This importantly frames the provision as one that seeks to keep the internet as open as necessary rather that enshrining net neutrality as a concept.

There is no mention of open internet access in the EU-Japan deal. We should probably not read too much into this other than the fact that the issue was not important enough for either side to require its inclusion in the deal, nor were they able to easily agree on suitable wording that reflected their position accurately – since the EU already has both its own text and has signed free trade agreements containing such provisions.

The other three free trade agreements all share the same language with the only difference being that the CPTPP and EU submission to the WTO preface that the requirements are "subject to applicable policies, laws and regulations". The common text does not establish any enforceable obligation on states but instead focuses on ensuring that parties "recognise the benefits" of people and businesses having the ability to "access and use services and applications of a consumer's choice" and are able to "connect devices of their choice to the Internet" and "access

32 Wikipedia - https://en.wikipedia.org/wiki/Net_neutrality

information on the network management practices" of ISPs. There are small qualifications to these, such as only being able to connect a device if it does not harm the network.

There is an interesting subtle but important difference between the CPTPP and USMCA when compared with the EU submission to WTO. All texts state that "access and use services and applications of a consumer's choice" can be subject to "reasonable network management", which is a very broad term and leaves open the potential for ISP to implement traffic management policies. This text clearly opens the door for ISPs to start actively managing the traffic over their network in clear contravention of the principles of net neutrality. The EU adds a vitally important word to the provision, "non-discriminatory". This is omitted from the other treaties and provides a vital safeguard against discriminatory traffic management by ISPs – and therefore preserves some semblance of net neutrality. Overall, the provision on net neutrality provides no protection because it is so weak, especially in the US-led treaties. And even more damningly "it may actually impede the development of stronger, more meaningful global standards."[33]

Even though many already consider net neutrality to be dead in the US following the FCCs Restoring Internet Freedom Order made in 2017 and implemented in 2018 which gave ISPs a free hand "to do practically whatever they like",[34] in Europe, and much of the rest of the world, the fight is still ongoing – and it is a fight that really matters.

33 Malcom, J. & Maira, S. (2015, November 5) *Release of the full TPP text after five years of secrecy confirms threats to user's rights.* Electronic Frontier Foundation. Retrieved from https://www.eff.org/deeplinks/2015/11/release-full-tpp-text-after-five-years-secrecy-confirms-threats-users-rights
34 Kelly, M. (2018, June 11) *Net Neutrality is dead – what now? Retrieved from* https://www.theverge.com/2018/6/11/17439456/net-neutrality-dead-ajit-pai-fcc-internet

PRACTICAL IMPLICATIONS FOR LABOUR AND LABOUR MARKETS

The analysis contained in the previous section clearly shows that there are major concerns about critical areas of the digital economy having their rules set globally in the interests of developed countries and specifically the tech giants that operate in those countries. We have highlighted some of those issues within each provision. In this section, however, we want to look at how the entire digital trade chapter, within the context of the wider free trade agreement that it sits within, could impact on the world of labour and labour markets.

It is important to note that the practical implications that we go through are possibilities based on assumptions. We make these assumptions clear in each example where they are applied. Because the digital economy is still developing and because many countries are yet to sign up to digital trade agreements, there are many impacts that we are yet to see. Equally, it can also be the case that assumptions made about new areas of legal text can miss key practical implications that only come to light when tested by actual implementation and enforcement.

What is clear is that the tech giants are already having a material impact on the world of work – much of it very disruptive and directly affecting the lives of workers, particularly in less secure, less well-paid sectors of the labour market.

In many cases, as the analysis below suggests, what digital trade agreements are often doing is not creating additional problems, although that is sometimes the case. One example is the increased restrictions on source code sharing. Instead, they mostly contain provisions that benefit the tech giants most, like free cross-border flows of data or banning localisation requirements, enabling them to continue to benefit disproportionately from the digital economy. As Deborah James, director of Our World is Not for Sale, puts it, corporations "have long used trade agreements to lock in rules favoring their 'rights' to make profits, while limiting governments' ability to regulate them in the public interest, often in ways that could not advance through normal democratic channels."[35]

IMPLICATION 1 – INCREASE PRECARIOUS WORK

Technology is already disrupting labour markets everywhere, with future automation and the Fourth Industrial Revolution set to make the coming decades' disruption even more severe.[36] Although the tech giants have created some highly skilled jobs such as engineers, coders and product designers, the majority of new jobs created or multiplied by tech are precarious and low skilled. Examples of these types of work include delivery drivers at Hermes, cleaners on TaskRabbit or data entry at Amazon Mechanical Turk. These occupations generally see workers being defined as "self-employed" or "agency", denying them many employment rights.[37] The work often lacks fixed or predictable hours, which is the attraction to some, but makes it very hard to raise a family or get a mortgage. Ratings systems, overbearing surveillance and formal job targets disempower workers at the expense of employers and buyers. This is because low ratings or missed targets, even when unmerited or unattainable, can have serious consequences, including sanctions and loss of employment.

Key to the success of all these platforms is the huge amount of data that they collect and process together with their ambition to disrupt and dominate existing markets, often with little regard for existing regulation or the wider social impacts. Although the tech giants did not invent bogus self-employment or precarious work, they have extended its reach and in certain instances they have changed its nature in important ways. In Spain a recent report found that 17 per cent of people engaged in platform work.[38] As platform work proliferates, collective bargaining has been especially curtailed, since this is much harder for the self-employed. Meanwhile, both the breadth

35 James, D (2017 November 22) *Twelve reasons to oppose rules on digital commerce in the WTO.* Retrieved from https://www.huffpost.com/entry/twelve-reasons-to-oppose-rules-on-digital-commerce

36 Manyika, J et al (2017) *Jobs Lost, jobs gained: Workforce transitions in times of automation.* Mckinsey Global Institute. Retrieved from https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages

37 Eurofound (2018) *Platform work: Employment status, employment rights and social protection.* Retrieved from https://www.eurofound.europa.eu/data/platform-economy/dossiers/employment-status

38 Canigueral, A. (2019, June 30) *How can tech meet the needs of platform workers?* Retrieved from https://www.thersa.org/discover/publications-and-articles/rsa-blogs/2019/06/tech-platform-workers

and depth of worker surveillance has been extended significantly, with examples including logging employee keystrokes on their keyboards, currently done by 45 per cent of American companies,[39] to requiring employees to wear tracking devices, 202 million of which were handed out in 2016,[40] to using specialist software to monitor staff social media and private messaging apps.[41]

Many tech giants, such as Uber[42] or Foxconn[43], have an explicit goal to automate as much of their labour as possible, investing billions to make it happen. Key to making it happen are the workers who provide the data required to build the algorithms to replace them. The nature of these data-driven digital markets is that the company with the largest data trove and the ability to process it into actionable intelligence has a real competitive advantage.[44]

Many of the e-commerce provisions analysed in this report, including the prohibition on data localisation, source code secrecy, free cross-border data flows and the abolition of net neutrality, all favour the largest transnational tech companies because they exploit opportunities of scale, benefit most by keeping source code secret, are best able to exploit global data flows and meet the costs of a non-neutral internet. These data flows, as well as the code and insights built from the data, will become ever more important in the future as we see more and more jobs automated and platformatised. This will make it much harder for local and non-digital alternatives to survive or emerge, especially ones with different social or environmental considerations. In the absence of a change in employment model among tech giants, this is likely to lead to an increase in the number of people who are forced to work under the conditions associated with platformatised work.

IMPLICATION 2 – MAKING ENFORCEMENT OF LOCAL LABOUR LAWS MORE DIFFICULT

When a law is broken, an entity must be brought to court to answer the charge. A company having a locally registered entity makes this process easy because they can be legally compelled to engage with the domestic legal process and comply with its judgements. On the other hand, as the ITUC has previously commented: "without a local presence of companies, there is no entity to sue and the ability of domestic courts to enforce labour standards, as well as other rights, is fundamentally challenged."

The latest EU Submission to the WTO for telecom services is already proposing that providers of services should not be required to establish a local legal entity. The influential Cato Institute say their ideal UK/US trade agreement would "forbid any 'local presence' requirements, conditions that require service suppliers of another party to have an office or store or any form of presence."[45] As more and more services become mediated through platforms, and the internet enables us to exchange goods, services and information with anyone, we need to ensure that we maintain our ability to enforce domestic laws as appropriate, including labour laws.

The erosion of our ability to enforce domestic legislation is not a theoretical possibility but one which is already happening, facilitated by the internet and digital technology and global trade. There are already examples of this happening on a small scale with certain services, like online tutoring. In this sector, it is quite easy to contract a person resident in your country but working for a platform, or an agency based in another country, to tutor you. In some instances the company that you contract the work through will have no legal entity established in your country. This means that it will be hard for those purchasing the service to hold the company to account for failing to properly deliver the service or other issue requiring a legal remedy.

If this were extended to major gig-economy companies such as Uber and they were not required to have a local legal entity, it would become very difficult to enforce domestic labour laws and workers' rights, as is currently the experience of many countries trying to enforce labour laws against platforms with a local presence. If enforcement were compromised in this way, the authority's only option would be to enforce against the drivers themselves, since they are a legal entity located in the country. However, the authorities would find it almost impossible to enforce anything because most employment rights, from minimum wage to sick pay, do not apply to self-employed contractors. It is therefore vital that, in order to ensure that labour law can be enforced locally, any company

39 McCann, D. & Warin, R. (2018) Who Watches the Worker? New Economics Foundation. Retrieved from https://neweconomics.org/2018/06/who-watches-the-workers
40 Wild, J. (2017, February 28) *Wearables in the workplace and the dangers of staff surveillance.* The Financial Times. Retrieved from https://www.ft.com/content/089c0d00-d739-11e6-944b-e7eb37a6aa8e
41 Solon, O. (2017, November 6) *Big Brother isn't just watching: workplace surveillance can track your every move.* The Guardian. Retrieved from https://www.theguardian.com/world/2017/nov/06/workplace-surveillance-big-brother-technology
42 Newton, C. (2014, May 28) *Uber will eventually replace all its drivers with self-driving cars.* The Verge. Retrieved from https://www.theverge.com/2014/5/28/5758734/uber-will-eventually-replace-all-its-drivers-with-self-driving-cars
43 Javelosa, J. (2017, Jan 3) *Apple manufacturer Foxconn to fully replace humans with robots.* Retrieved from https://futurism.com/apple-manufacturer-foxconn-to-fully-replace-humans-with-robots
44 Mayer-Schonberger, V. & Ramge, T. (2018) Reinventing Capitalism. John Murray
45 Ikenson, D., Lester, S. & Hannan, D. (2019) The ideal US-UK Free Trade Agreement. Cato Institute. Retrieved from www.ifreetrade.org/pdfs/US-UK-FTA.pdf

that employs people in a country must have a legal entity in that country. This will ensure that labour laws are there to protect everyone and that companies are held to account for their behaviour towards their workers.

IMPLICATION 3 – ERODING WORKERS' RIGHTS BY NECESSITY

The labour market consists of a balance between different forces, and workers usually need to fight hard for their rights (relative to companies and owners of companies) to be enshrined in law. Ending child labour or creating the five-day week did not happen thanks to the generosity of business, but rather the concerted effort of workers, unions and civil society – and usually against the odds – ultimately implemented by democratically accountable governments. The digital transformation that society is undergoing is testing some of those hard-won rights about what constitutes a worker and what rights and protections they deserve.

Most provisions in trade agreements contain exemptions that allow governments to regulate in an area that would otherwise be prohibited by the free trade agreement. These derogations are often further qualified by the fact that they should meet a "legitimate public policy objective" and that it is "no more restrictive than necessary", known as the necessity test.

It is important to acknowledge that the test has evolved incrementally over time as the WTO Appellate Body has ruled on cases. An early example involved the banning in California of a petrol additive that was polluting water supplies. However, a Canadian supplier of the additive claimed this failed the necessity test because in theory California could have solved the problem by requiring all storage tanks to be dug up and resealed properly. The WTO held in favour of the Canadian company because they had indeed proposed something that was less restrictive on global trade. This early jurisprudence was criticised for being too biased towards trade.[46] Although the jurisprudence has moved a little, it remains very hard for parties to meet the legitimate necessity tests for certain derogations.

When considered in the abstract, the necessity test can seem to be quite reasonable. But as the excellent example laid out by Laura Bannister, senior adviser at the Trade Justice Movement, at the recent WTO Public Forum about worker surveillance shows, this could become problematic.[47] Many gig economy workers are already under heavy surveillance at work, and this is currently expanding to cover non-working hours as well.[48] Already, workers and trade unions are demanding new digital rights for workers and an end to excessive digital surveillance. Should they be successful in their demands and the government enact policy that banned or severely curtailed the ability of companies to collect data based on excessive surveillance, it could be considered "more restrictive than necessary" by a trade court. This is because the tech company would be able to show an impact on its ability to trade, but the unions and workers may struggle to prove scientifically or beyond doubt that the surveillance and data gathering was damaging to workers' well-being or their privacy. Other areas that are critical to workers and unions could also have problems when set against the necessity test such as workers' privacy, data security or common data ownership.

IMPLICATION 4 – CHALLENGES TO ALGORITHMIC TRANSPARENCY

Algorithms are not new, but thanks to the digital revolution, they are becoming a part of an ever-increasing portion of our lives. They are indispensable in the online world due to the need to sort huge volumes of information in order to make the internet the valuable service it is today. As the digital economy has grown, the reach of algorithms has extended. Today they are responsible for almost 40 per cent of stock trades in the UK. They fly planes for over 95 per cent of the time the planes are in the air. And they may soon be driving our cars. Algorithms are also expanding into new areas to help people make decisions about whether to offer an applicant a job interview, whether offenders will reoffend, and what social care provision a service user needs. Despite presenting a technological veneer of objectivity around their decisions, algorithms, and the data collection that powers them, are designed by people, and their parameters and foundational assumptions are shaped by ultimately subjective human decisions.

As algorithms enter increasingly sensitive areas of our lives, we need to have meaningful accountability for those who create and deploy algorithmic decision systems, especially in areas where decisions have a significant impact on individuals.

The source code provisions in emerging e-commerce deals would make it very difficult for governments to require access to source code as a condition of market

46 Howse, R. (2002) *Human Rights in the WTO: Whose Rights? What Humanity? Comments on Petersmann.* 13 EJIL 651, p. 657.
47 Audio recording of WTO Public Forum Session 129. Retrieved from https://www.wto.org/audio/pf19session129.mp3
48 McCann, D. & Warin, R. (2018) *Who Watches the Worker?* New Economics Foundation. Retrieved from https://neweconomics.org/2018/06/who-watches-the-workers

access. The limitation to defined legal areas such as intellectual property or competition could make it very hard to require access in order to meet transparency, accountability and auditing requirements of future algorithmic accountability systems.

The source code provisions would make it hard for workers to examine the internal workings of the algorithms that will become central to the world of work. Algorithms are already being used in a wide range of areas within work, with one of the highest profiles being around hiring algorithms. Algorithmic systems review CVs and online applications to select the most suitable candidates in order to automate some, or all, of the recruitment process. In 2018 Amazon decided to abandon its own hiring algorithm that it had been developing for four years because it "realized its new system was not rating in a gender-neutral way."[49] If Amazon with its deep pockets and strong AI developer base could not rectify for the biases of the algorithm, one has to question whether the many commercial sellers of such software have been able to do so.

In order to be able to have more transparency and understanding of the actual performance of these critical source codes, AI ethics advocates want algorithms to be made visible enough to inspect and understand them, particularly when they lead to decisions that have questionable or negative consequences, such as a job application denial or a driverless vehicle accident. This could be made very hard, or impossible, with the current prohibitions on source code disclosure requirements in FTAs. Indeed, as award-winning journalist Kate Kaye puts it, "The push to restrict access to algorithms doesn't work for people, it doesn't work for users, it doesn't work for consumers."[50]

IMPLICATION 5 – EXPANDING MARKET ACCESS RIGHT FOR DIGITAL FIRMS

There is a quiet revolution going on within government, known as Gov Tech, that could transform the nature of public services and who delivers them, because automated decision systems are being increasingly used to decide who should receive them as well as systems to target "most efficiently" the scarce resources. Mimicking other tech-based disruptions like fintech[51] or proptech[52], a recent PriceWaterhouseCooper report argued that "Gov Tech has the power to transform the delivery of public services, achieve better for less and improve the user experience."[53]

We are already seeing technology companies getting into the heart of key decisions that we normally associate with the state. Examples include predictive algorithms, which give police suggestions for which areas to focus their increasingly limited resources on,[54] and software attempting to predict whether a newborn child will be subject to abuse in the future.[55]

As public service delivery increasingly relies on digital algorithms and data, this could also mean an increased role for the private sector in core areas of public services. The additional challenge that the e-commerce rules may introduce is the limitation of government control and regulation over companies that will be delivering key public services. E-commerce rules could mean that governments will not be able to demand the source code by default, nor limit the flow of data, nor require any of the data collection and analysis to be conducted locally. Demanding the source code is vital in order to ensure that the systems function as per the specifications and design of the system as well as to ensure that it is not biased against certain sections of the population. Equally, limiting the flow of data is vital, since some of the data will be highly sensitive, such as health or police data, and it will therefore not be appropriate for the data to be transferred internationally by default, thereby losing jurisdictional control and access to it.

An additional challenge is that the digitalisation of public services is also being used as a tool to increase and lock in the range or public services that could be delivered by the private sector to areas such as health care, education, local government, electricity and water distribution, by tech firms trying to expand their "market access" rights. For example, Uber, which ultimately wants to operate a single mobility platform with as much automation as possible, has acknowledged its intention to table proposals that would expand the "market access" rights for digital firms in sectors under WTO rules. Uber also wants to expand the scope and coverage of those sectors,

49 Dastin, J. (2018, October 10) *Amazon scraps secret Ai recruiting tool that showed bias against women.* Retrieved from https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-id

50 Kaye, K. (2018, November 8) *How the tech industry coordinated to squelch algorithm transparency in the new NAFTA deal.* Retrieved from https://redtailmedia.org/2018/11/08/how-the-tech-industry-prevented-algorithm-transparency-in-nafta-2-0/

51 Term for a business that is applying technology in order to deliver financial services industry

52 Term for a business that is applying technology in order to deliver property services, especially rentals

53 PriceWaterhouseCooper. *Gov.Tech: the power to transform public services in the UK.* Retrieved from https://www.pwc.co.uk/industries/government-public-sector/gov-tech.html

54 Couchman, H. (2019) *Policing by Machine.* Retrieved from https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf

55 Pegg, D. & McIntyre, N. (2018 September 16) *Child abuse algorithms: from science fiction to cost-cutting.* Retrieved from https://www.theguardian.com/society/2018/sep/16/child-abuse-algorithms-from-science-fiction-to-cost-cutting-reality

which could open up many more public services to the threat of privatisation, even potentially against the express will of the people and government.

Increased privatisation by tech firms could leave important public services in the hands of digital corporations with weak accountability and obligations to local communities for ensuring quality and accessibility of service.

IMPLICATION 6 - INCREASE POWER OF BIG TECH OVER WORKERS

The introduction of data-gathering technology, its analysis and use has disrupted the delicate balance between worker and employer, and has shifted power firmly back to employers. This is especially true within the new labour platforms like Deliveroo or Amazon Mechanical Turk but is now filtering into all areas of work. A recent report by the New Economics Foundation found that companies were increasing their power over employees in a number of ways.[56] Firstly, by extending their surveillance of them temporally, beyond the core hours of work, and spatially, to include surveillance of the body itself. Incredibly, 45 per cent of US companies currently log key strokes of their workers.[57] Secondly, because the company owns the data that is produced, it is overwhelmingly used for the benefit of management, leading to an increased workload for each worker and, when there is no opportunity to use the increase in work to produce more, a reduction of employees. The poster child for work intensification is Amazon, which through compulsive monitoring and stringent targets, ensures that all its workers' activities are tracked, recorded, and assessed to ensure they meet exacting targets at all times. Thirdly, employers are hiding behind algorithmic decision systems that affect workers, materially leading to loss of accountability and the potential to entrench biases.

These developments are already seeing the power of workers reduced in favour of employers. Digital trade agreements did not create these issues but they do limit the policy space of countries so that it can be hard to mitigate for these negative outcomes. There are three provisions within the digital chapters of trade agreements that enable Big Tech to increase and cement their position of power over workers. Firstly, the unregulated cross-border transfer of data will ensure that Big Tech is able to acquire all of the data that it needs to surveil its workforce while careful analysis of the data helps the companies get the most out of their workers. Secondly, the provision to ensure that source code cannot easily be accessed, especially for issues of bias or discrimination, will allow companies to continue to hide behind the "black box" algorithms that they deploy. Finally, the application of the necessity test may act to limit the potential for workers to fight back against intrusive data gathering practices by a company.

As we noted in the example devoted to the necessity test, this could limit the ability of workers and their unions to resist intrusive surveillance and monitoring. This is especially worrying given that we are now seeing cases of people dismissed for behaviour outside the workplace and outside of work hours. It is projected that by 2021 over 500 million employees will be monitored through wearable technology. Companies are using data to develop the digital intelligence to control and manage the remaining workforce even more closely, leading to an ever-increasing cycle of intrusion and surveillance.

The provisions around source code threaten to allow employers to hide behind automated decision-making systems, thereby reducing their accountability. Key decisions about whether to hire someone and who to fire are now frequently made by algorithms. Without getting access to the source code, it may be very hard to ascertain whether the system is functioning correctly or whether the system is discriminatory against certain sections of the population.

IMPLICATION 7 - THREATEN COUNTRIES' DOMESTIC INDUSTRIES' FUTURE BY REQUIRING THE FREE TRANSFER OF THE DATA

From some perspectives it is incredible that the modern tech companies are some of the most valuable companies in the world, especially given the fact that many of them, like Google or Facebook, offer a product that is free to use, while others, like Uber or Spotify, still fail to make a profit. What lies behind the valuations are the incredibly large data troves that they have gathered during the course of their operations and that are central to their success and dominance. All tech companies rely on and benefit from the ability to gather large amounts of data from users and workers within their ecosystem, often supplemented by data sets purchased from third parties. Their engineers build sophisticated algorithms to analyse the data and turn it into actionable intelligence, which they can in turn monetise to generate revenues and profits. Probably one of the best examples to illustrate the point is Uber. Uber is a transportation company that is currently valued at about $50bn yet owns no cars and employs no drivers and continues to makes

56 McCann, D. & Warin, R. (2018) *Who Watches the Worker?* New Economics Foundation. Retrieved from https://neweconomics.org/2018/06/who-watches-the-workers
57 Johnson, C. (2017) *Meeting the Ethical Challenges of Leadership: Casting Light or Shadow.* SAGE Publications Inc.

huge losses.[58] Uber lost a staggering $5.24 billion in the second quarter of 2019.[59] What Uber lacks in terms of capital and infrastructure it makes up for by gathering and analysing an immense volume of data on people, drivers and their cars and how they move around the city and interact with each other. This data not only allows it to refine and improve the service that it offers customers today, in the future it will allow Uber to achieve its ultimate aim of being a transportation company without drivers at all, since the data is being used to build self-driving cars which will ultimately replace its entire fleet. Although not specifically linked to the digital chapter provisions of trade deals, Uber has recently signalled its intention to sue Colombia for banning it from the local market – something which may only become more common when digital chapters are more widely included in trade deals.[60]

It hard to see why, given the circumstances outlined above, countries should be precluded from implementing policies and laws that would enable them to develop their own domestic tech industry by placing limits on the flow of data out of the country or requiring the localisation of servers and people. Just as Norway did with oil extraction technology[61] or South Korea did with consumer technology[62], it is vital that countries have the tools to impose conditions on companies operating domestically that will foster a new generation of businesses along with new jobs.

This is especially the case because in the future the success of businesses in many sectors will be rooted in their ability to collect and analyse data. If a large part of the data is being gathered by transnational platforms who are able to aggregate global data streams, thanks to the liberal and free cross-border flow of data, then it will be much harder for domestic competitors to emerge, since, even if they have the capital to employ the people and data analytics systems, they will never be able to match the quantity of data.

IMPLICATION 8 - PREFERENCING TRANSNATIONAL COMPANIES OVER MICRO, SMALL AND MEDIUM ENTERPRISES (MSME)

One of the main publicly stated rationales for pursuing e-commerce and now digital trade provisions in free trade agreements is to enable and empower MSMEs to be able to trade digitally and therefore open up markets that would previously only been available to large multinationals. Completely reformulated rules, written by and for MSMEs, could deliver on this noble sentiment and provide real opportunities for them to grow and reach wider markets. However, in reality, the proposals and signed agreements will do little or nothing to help MSMEs, and in fact they are very much aligned with the needs of Big Tech companies, who would undoubtedly benefit the most. In addition, the way that the digital economy operates more generally also favours the tech giants over MSMEs.

MSMEs are the real engine of the economy, not just in developing countries but in developed ones too. They generally account for the majority of employment, accounting for as much as 45 per cent of jobs, as well as economic activity, an average of 33 per cent of national income.[63] However the demands of Big Tech, which are promoted by a growing army of lobbyists, are often at odds with the needs of MSMEs. A pertinent example is with regard to tax payments. Tech giants exploit their global presence to ensure that they minimise their tax liability which leads to situations in which Apple's Irish subsidiary pays just 0.0005 per cent tax in 2014.[64] Equally, Uber in the UK routes all its customer payments through Luxembourg, therefore avoiding VAT in the UK, although this is being taken through the courts.[65] This makes it very hard for any MSME to compete, since they are unable to avail themselves of complex legal structures and therefore find themselves at a 20 per cent cost disadvantage.

The combination of several of the provisions could be additional barriers preventing MSME emerging and competing against the established tech giants while at the same time specifically being advantageous to the tech giants. For instance, MSMEs would benefit much less than Big Tech from the cross-border free

58 Palmer, A. (2019, October 1) *Uber and Lyft close to record lows as investor skepticism grows around recent IPO.* Retrieved from https://www.cnbc.com/2019/10/01/uber-closes-at-record-low-worth-less-than-50-billion.html
59 Clark, K. (2019, August 8) *Uber lost more than $5B last quarter.* Retrieved from https://techcrunch.com/2019/08/08/uber-stock-plummets-following-second-quarter-earnings-report/
60 Griffin, O. (2020, January 10) *Uber to take exit ramp in Colombia after 'arbitrary' court ruling.* Retrieved from https://www.reuters.com/article/us-uber-colombia/uber-to-take-exit-ramp-in-colombia-after-arbitrary-court-ruling-idUSKBN1Z921L
61 Heum, P. (2008) *Local Content Development: experience from oil and gas activities in Norway.* Institute for research in economics and business administration. Retrieved from https://openaccess.nhh.no/nhh-xmlui/bitstream/handle/11250/166156/A02_08.pdf?sequence=1
62 Chen, C. & Sewell, G. (1996) *Strategies for technological development in South Korea and Taiwan: the case of semiconductors.* Research Policy Volume 25, Issue 5, Pages 759-783. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/0048733395008616
63 OECD (2017) *Enhancing the Contributions of SMEs in a Global and Digitalised Economy.* Retrieved from https://www.oecd.org/industry/C-MIN-2017-8-EN.pdf
64 Taylor, H. (2016 August 30) *How Apple managed to pay a 0.005 percent tax rate in 2014.* Retrieved from https://www.cnbc.com/2016/08/30/how-apples-irish-subsidiaries-paid-a-0005-percent-tax-rate-in-2014.html
65 Kaminski, I. (2019 October 10) *Uber's VAT liability confirmed.* Retireved from https://ftalphaville.ft.com/2019/10/09/1570629132000/Uber-s-UK-VAT-liability-confirmed/

flow of data because they are much less likely to need the provision to run their operations, since MSMEs are overwhelming based in one country. MSMEs would also be less likely to take advantage of buying large data sets that had been assembled thanks to moving data transnationally. In addition, since digital services can be improved by the analysis of large datasets, the liberal free movement of data across borders will preference Big Tech corporations.

MSMEs have raised very specific concerns about the market concentration of Big Tech players in many sectors that are critical for e-commerce, such as marketplaces, electronic payment solutions and logistics providers. MSMEs also complain that companies operating in these concentrated marketplaces are able to exploit their position to charge excessive fees and membership. These concentrated markets mean that MSMEs, with their limited bargaining power, are at the mercy of these companies, because if they want to participate in the global e-commerce market, they need to use these services, even if the terms feel unfair. The rise of this dynamic has led to a resurgence in interest around the concept of monopsony, the less well-known cousin of monopoly. Whereas "monopoly" is defined as "a market structure characterised by a single seller, selling a unique product in the market", "monopsony" on the other hand describes "a market situation in which there is only one buyer".

As Richard Hill, prominent civil society activist, noted: "While the concept of e-commerce is good for SMEs, the actual e-commerce rules being proposed at the WTO would enable the platforms whose dominance is already a problem for SMEs to further squeeze SMEs to pay them more." As more and more purchases are made online and physical shops close down at ever-increasing rates, this poses a serious challenge to the tax receipts, especially for local government, which is often very reliant on local business property taxes for its revenue.

IMPLICATION 9 – AGRICULTURE AND DIGITAL TRADE

Global agriculture and the wider food system is undergoing a revolution that may well be as dramatic as any previous one. There have been three major revolutions, starting with the original agricultural revolution of the 18/19th century Europe, followed by the green revolution of the 1950s and 60s, and finally the GMO revolution of the 2000s. Today, the prospect of workerless farms staffed by robots is on the horizon, with many working on it[66] while others are already doing it (at huge cost).[67] Mass adoption, however, remains a distant prospect, for now. Instead, what is happening today is a radical restructuring of how, and by whom, our food is produced and distributed. Globally the small-scale food system, where (often family) farmers grow on small plots, often using traditional methods and selling their own produce directly in physical markets or on the streets, still feeds 70 per cent of people around the world.[68] In recent years, just as traditional methods of farming have been challenged, traditional markets have been facing increased competition from online marketplaces. This transition has the potential to inflict hardship on millions as their livelihood becomes a sector driven by big data, technology and global companies.

The advance of Big Tech companies into agriculture and the wider food system presents a number of challenges to those trying to make a living, and feed themselves, from small-scale agriculture. A growing concern is that new digital technologies, which allow genes to be assembled in a lab, allow new forms of bio-piracy that bypass existing regulations to the detriment of local and indigenous communities.[69] This will transfer a valuable asset from the commons, to be used by all farmers, to something owned and controlled by the agritech sector. The behaviour of companies like Monsanto, which came to prominence in the third agricultural revolution, in developing terminator seeds so farmers can't save seeds while taking those who do to court, is stoking this fear. In addition, as the process of growing food becomes ever more reliant on technology, from growing, to harvesting, to distributing, technology companies from outside the agricultural sector, such as Fujitsu and Amazon, are increasingly buying existing companies with the potential to further dominate the agritech sector.[70]And as with all data-driven businesses, the fear is also that over time these large companies will coalesce into an even smaller number of mega companies, as is already the case in many sectors of agriculture today.[71]

More and more food is now being delivered over digital platforms rather than physical markets and shops. The platformisation of the food delivery system is not only calling farmers' livelihoods into question but is also creating a more general problem of regulation and accountability. For instance, Alibaba,

66 Paquette, D. (2019 February 17) *Farmworker vs Robot.* Retrieved from https://www.washingtonpost.com/news/national/wp/2019/02/17/feature/inside-the-race-to-replace-farmworkers-with-robots/
67 Thu, M. & Hong, B. (2016 March 24) *Smart farming a bright future for Vietnam.* Retrieved from https://www.nationthailand.com/business/30282386
68 ETC (2017) *Who will feed us? Industrial food chain vs the peasant food web.* ETC Group. Retrieved from https://www.etcgroup.org/content/who-will-feed-us-industrial-food-chain-vs-peasant-food-web
69 Servick, K. (2016 November 17) *Rise of digital DNA raises biopiracy fears.* Retrieved from https://www.sciencemag.org/news/2016/11/rise-digital-dna-raises-biopiracy-fears
70 Fujitsu website. *IoT in Agriculture.* Retrieved from https://www.fujitsu.com/global/themes/internet-of-things/hyperconnected-business/agriculture/
71 ETC (2018) *Too big to feed: the short report.* ETC Group. Retrieved from https://www.etcgroup.org/content/too-big-feed-short-report

a massive Chinese e-commerce platform, delivers fresh milk via its platform, often imported, directly to consumers in China (and other countries). Given that relatively few countries have existing regulations that adequately deal with the distribution of food online, especially when cross border, including vitally important standards around food safety, the development on international e-commerce channels for fresh food poses serious challenges.[72] For instance, who should be held responsible for issues related to the quality of the milk, how it is produced and ultimately who should be liable for problems that arise? This will be made even more complicated if the proposals in the new wave of trade agreements are implemented which would make it legal for a service supplier like Alibaba, or other e-commerce platform, to operate without a "local presence" in its country or, for example, to avoid a requirement to source food from local producers.[73]

A third challenge to small-scale farming, driven by Big Tech, is the level of vertical and horizontal integration of the agritech sector that we are seeing. An illustrative example is the acquisition by Monsanto of the digital agriculture and insurance company The Climate Corporation for nearly a billion dollars.[74] The huge value to Monsanto in the acquisition was the massive amount of data on farmers, crops and the climate along with the ability to turn the data into actionable intelligence, telling the farmer which seeds to plant, how much nitrogen to use or which pesticide to apply. While for many farmers this is useful information, few of them realise that the data they provide is much more valuable to the tech company, which uses it to target them with marketing and often aiming to eventually automate away their livelihood using the data together with "advancements in computing power, dexterity, motion planning, and computer vision which are enabling a new generation of robot.'[75] The provisions cementing the international free flow of data will make it easier for multinational agritech businesses to harvest and compile data from around the world. This will allow them to generate better products, since they will have more data, than those that could be developed, either locally by farmers using their own data, or even by attempting to aggregate data nationally. In addition, the prohibition on requiring the sharing the source code of the software that will be increasingly essential for farms to use, even under technology transfer programmes, will act to protect the interests of multinational agritech at the expense of empowering local farmers and fostering a domestic industry.

The growth of a new generation of agri-businesses, powered by data and acquisition, seeking to enclose information (rather than land) such as seeds, DNA, or data about land and the efficacy of pesticide use, while marketing ever more sophisticated "precision agriculture",[76] is taking over our food system. This ensures that farmers are increasingly reliant on a few large multinational companies, which, through their use of precision agriculture technology, can minimise the use of inputs, such as water and pesticides, while maximising the outputs. This is compounded by the reliance that many already face on the likes of Monsanto for seeds and fertilizer. This can be seen as providing a solution to climate change for the agricultural sector,[77] but precision agriculture technology is extremely expensive, so only the largest companies can afford it. This change will make the livelihood of small-scale farmers even more precarious as they are unable to obtain the latest precision technology, and unfairly blamed for the climate crisis.

Historically, the agribusiness lobby has been critical of food and agriculture being excluded from bilateral Free Trade Agreements (FTAs).[78] Now not only do many FTAs include the agricultural sector, but FTAs are also often used to try to force open markets or constrain the power of governments to set their own regulatory standards. At the same time, the power of large-scale tech-driven agribusinesses is being advanced through the TRIPS intellectual property provisions through the WTO, which protect specific forms of intellectual property and facilitate mergers.

Even though the digital trade provisions are not creating the underlying issues, the liberal free flow of data linked to the prohibition on requiring source code transfer (as well as issues around local presence) means that large agritech businesses will continue to be benefit most at the expense of small-scale farmer.

72 GRAIN (2018 May 31) *Top e-commerce companies move into retail.* Retrieved from https://www.grain.org/en/article/5957-top-e-commerce-companies-move-into-retail
73 See Implication 2 – Difficulty enforcing local labour law
74 Tsotsis, A. (2013 October 2) *Monsanto buys weather big data company climate corporation for around $1.1B.* Retrieved from https://techcrunch.com/2013/10/02/monsanto-acquires-weather-big-data-company-climate-corporation-for-930m/
75 Alexander, B. (2018 October 3) *If farms are to survive, we need to think about them as tech companies.* Retrieved from https://qz.com/1383635/if-farms-are-to-survive-we-need-to-think-about-them-as-tech-companies/
76 NESTA website. *Precision Agriculture.* Retrieved from https://www.nesta.org.uk/feature/precision-agriculture/
77 Klein, A. (2019 July 26) *How tech is helping the agriculture sector curb carbon emissions.* Retrieved from https://www.weforum.org/agenda/2019/07/agtech-can-climate-proof-the-planets-harvests/
78 Bilaterals webpage. *Agriculture and Food.* Retrieved from https://www.bilaterals.org/?-agriculture-food-