Open Rights Group submission to UK consultation on a new Free Trade Agreement with the United States of America

Javier Ruiz <javier@openrightsgroup.org>

We have general concerns about the process of trade policy, shared with much of civil society. Modern trade agreements regulate more than trade, covering a staggering range of public policy, as evidence in the list of topics presented in these consultations.

As a rights organisation we believe that a focus on trade weakens the wider international framework of rules. Trade treaties are easier to enforce than other types of international treaties and end up taking precedent. The special tribunals staffed by trade experts that can impose tariff sanctions on sectors not related to the original dispute are problematic. For example, the EU has been paying the US for years to avoid importing hormone-treated beef, while the US pays the Caribbean island of Antigua over restrictions on the burgeoning internet gambling industry based on the small nation.

As a digital rights organisation we find particularly worrying that the complex issues we deal with could be literally traded away by negotiators. This is particularly the case given the track record of secrecy surrounding trade deals, which create a democratic deficit, with the executive legislating through diplomacy without proper parliamentary input. This is being criticised in debates over the Trade Bill, with no sign of the government agreeing to give up their powers.

While thanks to grassroots pressure WTO proposals are now public, most Free Trade Agreements are secret and only made public once the consolidated texts have been agreed. At that point it is too late to make any modifications. We expect the UK government will be fully transparent and engage civil society.

In this note we focus on the aspects of digital trade. This is one of the most cutting edge and concerning aspects of future trade negotiations. There is evidence of a concerted global lobby by the “Big Tech” companies of Silicon Valley to rewrite the rules of trade to

consolidate their global position through the"e-commerce" or "digital trade" agenda[i]. In this they are copying the model that Big Pharma used 30 years ago to irreversibly rewrite the rule of intellectual property worldwide. Once that these treaties are fixed there are not sunset clauses, no proper courts to evolve jurisprudence or even strike treaties down.

Therefore we see the current discussion on digital trade deals as an existential threat to digital rights and are unambiguously opposed to its inclusion on any US-UK FTA. Our analysis also shows that, similarly to other areas such as agriculture or foods, many of the proposed items in the US digital trade agenda would create a fundamental regulatory conflict with EU policies and could lead to problems with future data flows with the EU, including jeopardising a UK future adequacy decision under GDPR

The United States has presented an official proposal to open negotiations on digital trade at the World Trade Organisation (WTO)[ii]. The content of the proposal is indicative of the kind of demands that will be placed on the UK during the negotiations for a FTA. While the agenda of the current negotiations is not transparent we know that the UK and the US have "agreed to hold the 3rd U.S.-UK SME Dialogue in the United States before the end of the year, with a focus on digital trade opportunities for SMEs".[iii] The use of SMEs to advance the Digital Trade agenda is widespread but misleading, as the actual beneficiaries of the proposed measures are the US digital giants (Google, Facebook, etc.)

Many of the proposed measures are similar to those found in the CPTPP, where the US lobbied heavily for these, although it is currently not a signatory. The new NAFTA 2.0 treaty also contains various such provisions. Similar proposals have been made at the WTO by Japan as well. Below we discuss some of the main proposals.

FREE FLOWS OF INFORMATION

Cross-Border Transfer of Data:

The US proposes that "Internet users must be able to move data as they see fit". This policy objective is important but has to be balanced with certain restrictions put in place to protect the personal information of these same users. There is a fundamental difference between individual internet users being able to send information and companies sending data to jurisdictions with weak or non existent data protection regimes.

This requirement openly clashes with the EU General Data Protection Regulation (GDPR), which prohibits such transfers. Wilbur Ross, US Commerce Secretary, has openly called GDPR an unnecessary barrier to trade. Agreeing to US demands would put the UK in a double bind that could jeopardise data flows to and from the EU.

Preventing Data Localisation:

This requirement is transparently designed to deal with the fall out of the Snowden revelations, which has led in some cases to countries demanding that data infrastructure is located within their jurisdiction to avoid the reach of US spying agencies. Critics have termed this process the "Balkanisation" of the Internet. Digital rights groups such as ORG

are concerned about such demands to localise data because it can facilitate restrictions on freedom of expression by national governments. At the same time, many of these groups are also concerned about the growing concentration of data in the hands of a few US companies, and believe that some level of localisation might help with the necessary decentralisation of the Internet. This is a very complex fractious debate that should not be reduced to trade negotiations.

These discussions are complicated by the growing interest by many countries to develop a national capabilities in Artificial Intelligence, and the understanding of the importance of data in this process. It is to be foreseen that not only personal information, such as health records, but all sorts of data from industry and agriculture will be perceived as a national asset in a digital arms race, as other countries wake up to the way the USA and China are propping their own national AI industries and capabilities, creating a gulf with the rest of the world. The terms “AI nationalism” and “data colonialism” are already in use by social scientists and commentators. Countries wishing to develop their own AI national champions may attempt to use data localisation as part of their industrial strategy. The main AI company in the UK, DeepMind, is part of the US Google/Alphabet conglomerate.

There are also many public policy objectives that would justify maintaining local data infrastructure, including national security and regulatory oversight of specific sectors. Data localisation clauses found in existing trade agreements, such as TPP, sometimes contain limited exceptions, but we do not believe these would be sufficient to deal with he broader issues.

Prohibiting Web Blocking:

The US proposes to use trade rules to “ensure that governments do not arbitrarily block or filter online content, nor require Internet intermediaries to do so.” Protections against filtering and content restrictions and limits to the liability of intermediaries are critical to the functioning of the Internet. These protections are under severe strain as governments everywhere demand that internet companies monitor and filter their content for a variety of reasons, from “fake news” to terrorism.

ORG broadly supports this objective, and have campaigned extensively in this area, from ISP filters and broad copyright injunctions to the current EU DSM Copyright Directive. The EU E-Commerce Directive provides the current backbone for such regulation in the UK, but this will change after Brexit. We are not sure though that trade deals are the right space to implement such protections related to the free expression of end users of Internet services. Companies can use the arbitration mechanisms provided in trade frameworks to protect their economic interests, but citizens cannot use them to enforce their rights. A rights based system enforced by a proper judicial authority, such as the CJEU, is preferable. The inclusion of such positive measures does not outweigh the negative aspects of the bulk of the digital trade agenda.

PROTECTION OF PROPRIETARY INFORMATION

Protecting Source Code:

The US wants to ban countries from forcing companies to “share their source code, trade secrets, or algorithms as a condition of market access.” This is one of the most concerning aspects of the new digital trade agenda, already found in the CPTPP and draft TISA, and criticised by groups such as Third World Network.[iv]

Source code is the set of instructions, written and readable by people with the necessary training, used to generate a computer program. Source code is generally protected under copyright laws, similarly to literary works. There are many legitimate reasons why a government may require a foreign company to “share” their source code. Regulators may need to examine source code to ensure technical systems are not biased, for example in electronic voting or casino slot machines, or car emissions. Governments may also require that public funding is spent on freely available open source code, forcing companies to share the code created as part fo a public contract. Source code can also be required as part of patent applications or during court proceedings on competition issues, such as the Google v Oracle dispute over the Java programming language. These requirements could be banned if the current proposals are implemented in a US-UK FTA or at the WTO.

Trade secrets are protected by the WTO’s Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Art 39 of TRIPS protects “undisclosed information” to prevent unfair competition. This means for example that an employee of a company should not be able to share secrets of that company with her new employer, although such information might still be obtained through fair commercial practices, which could include reverse engineering. TRIPS envisages that some such information may need to be disclosed to governments, particularly in the context of chemical or pharmaceutical regulatory approval, and sets out that governments must protect that information from unfair commercial use.

TRIPS has already been criticised for giving companies new powers to protect what used to be a simple matter of fair business practice and a matter for courts to decide. These protections stifle innovation and protect incumbent industries. The current proposals go further than TRIPS in potentially preventing legitimate disclosures, such as those discussed above for source code.

Algorithms present a new challenge. An algorithm is the basic logic of a computer program. An algorithm can be represented as a flow chart of steps and options but ultimately it is an idea, and as such not protected by traditional intellectual property rights such as copyright or patents. Since TRIPS many companies will claim trade secret protection for their algorithms, but the US proposes to create protections for algorithms in their own right. This is extremely worrying. Many companies will use similar algorithms but delivered through different source code, and protection on stand alone algorithms would handicap technological developments.

Preventing the disclosure of algorithms would also hamper efforts to prevent unfairness and bias in many technological systems used to make decisions about citizens, from credit to court sentencing. There is a growing body of evidence showing that the increasing use of algorithms to support decisions requires new forms of technological transparency and accountability.

The EU GDPR includes a right for individuals in certain circumstances to be informed of the logic of the systems making decisions that significantly affect them, in a potential conflict with the US digital trade proposals.

Barring Forced Technology Transfer:

In addition to the general prohibition on the disclosure of source code or algorithms, the US is demanding that trade rules specifically ban "requirements to transfer technology, trade secrets, or other proprietary information." Technology transfer is a central aspect of economic development and global socio-economic justice. Third World Network in their briefing show how for example the Norwegian oil industry and the Taiwanese textile sector were built through forced technology transfers. As digital technology is increasingly embedded in every industrial sector the proposals could have far reaching implications.

While this issue may not seem critical within a US-UK FTA, given that both countries enjoy comparable levels of technological development, its inclusion in the deal would facilitate the propagation of this very harmful idea into other FTAs.

Barring Discriminatory Technology Requirements:

The US wants to ban countries from requiring the use of a national technology as a condition of market access, proposing instead market based competition. It is not completely clear what this would mean in the UK-US context, but as we discuss elsewhere in this note the US has been criticising the EU regime of technical standards for some time. The EU standards are not mandatory, but the wider system of market approval in practice makes them compulsory to follow in order to market products in the EU.

DIGITAL SECURITY

Encryption:

The US wants trade rules to "ensure that suppliers are able to use innovative and secure encryption technology, *while providing for government access to data consistent with applicable law.*" We agree that restrictions on encryption are problematic, but are concerned at the inclusion of government access in the core proposal, as it could be read that as a positive measure countries must implement, rather than a qualification. Besides, in some cases government may need to mandate minimum standards and it is unclear how this would fit with the proposals.

Cybersecurity:

The US warns that "overbroad efforts to protect cybersecurity can stifle the digital economy" and wants trade rules to ensure that "responses to cybersecurity incidents follow a risk-based approach." The current EU framework for cybersecurity requires disclosure of incidents in certain protected critical infrastructure sectors - transport, energy, etc. - to be made to relevant authorities, in the UK the National Cyber Security Centre. In addition, GDPR requires data breaches to be reported to the Information

Commissioner within 72 hours, if there is a risk to the rights and freedoms of individuals, and in some very limited cases to the affected individuals themselves.

We believe that these requirements are already fairly lax and "risk based", particularly in the high risk threshold to inform individuals, but many companies still wish to avoid any scrutiny and will lobby heavily against disclosure requirements. If the UK signs up to such principles in a FTA with the US this will provide ammunition to such companies and eventually likely lead to a weakening of the requirements. In turn this could mean problems with EU-UK data flows after Brexit.

FACILITATING INTERNET SERVICES

"Over the top" (OTT) services

OTT communications services are telephony, video or text services that run on the internet, as opposed to the traditional phone and SMS systems. Well known examples include Skype, FaceTime or WhatsApp, but also Gmail. Authorities in the EU and elsewhere are increasingly trying to bring these operators into a more restrictive regulatory framework, as currently there are markedly different expectations for each type of service ranging from universal service obligations to the privacy and confidentiality of communications. The US argues that OTTs are generally cross-border and highly competitive and should not be regulated as traditional telecommunications services. This is an issue that the US also raises in its annual report on EU barriers to trade.

ORG and most digital rights organisations are generally in favour of raising the privacy standards of OTT services, but are wary of bringing full telecommunications regulations to the sector. The regulatory overheads would be excessive for most small internet companies, and many OTT services are provided by non-profits and individuals, in one of the more equalising aspects of the Internet. In addition, during the 20th century national telecoms were developed in close collaboration with intelligence agencies and police, and even after liberalisation and the development of private companies, phone call logs and SMS remain subjected to extensive mass surveillance, particularly in the UK.

The US proposals would directly clash with the new Regulation on Privacy and Electronic Communications (e-privacy) currently being approved in Brussels, which is also mentioned explicitly in the US 2018 National Trade Estimate Report on Foreign Trade Barriers[v]. It is unclear yet to what extent it will apply to the UK, but we can expect that its provisions may form part of any common rulebook for telecoms.

Digitally Relevant Market Access Commitments:

The specific requirements of the US in this area are not clear and we would require that the UK government engages extensively with civil society over this. The General Agreement on Trade in Services (GATS) defines four main modes of supply.[vi]

Mode 1 involves the cross-border trade of any service from one territory to another, and being technology neutral it also includes electronic means. Examples include consultancy, distance training or architectural drawings, and it is easy to see how these can work digitally.

Mode 2 covers consumption abroad, i.e. the provision services directly to consumers across borders. The typical pre-Internet examples are tourism or travelling to receive medical treatment. The US has in the past argued that Internet services should be classed as Mode 2[vii] on the basis that a consumer, for example in Italy, accessing a Netflix server in the US is initiating the transaction and virtually "travelling" to the US for trade purposes.

Mode 3 involves establishing a commercial presence in the country. Most strict Internet services will fall out of this Mode, but at the recent Costeja/Google case on the Right to be Forgotten at the CJEU, the court found that Google was established in Spain, despite protestations. Some EU las will demand establishment in one of the Member States for regulatory purposes, for example in the draft package on European Production Orders.

Mode 4 involves allowing personnel to temporarily move across borders in order to supply a service, and it is not very relevant here, except that it will likely be raised in FTA negotiations with other countries.

In addition, there is a current debate as to a new Mode 5 services. This is defined as services embedded in creating the value added in goods. These include the design of products or broader regulations that increase the quality of goods, but exclude services bundled with goods, such as maintenance and support contracts.[viii]

There is an ongoing debate as to whether Internet services should be classed Mode 1 or 2 with important ramifications. In principle Mode 1 would seem to better protect consumers as the transaction would be deemed to operate under the jurisdiction of their location, while in Mode 2 it would be that of the service supplier, where recourse may be inaccessible.

Once a country agrees to "liberalise" a specific sector, in principle it should also allow digital trade in that sector. The US argues that this is not happening because countries are applying restrictive services classifications, particularly for communications services, and countries should agree that old classifications and commitments can apply to new technologies.

The OECD has recently carried a review of digital services that shows the complexity and challenges involved in deterring the mode classification of digital services, particularly for platforms (STD/CSSP/WPTGS(2017)3). One of the examples they analyse is Uber, which could arguably be classed as either a transport service, requiring Mode 3 presence, or as a Mode 1 business service. The OECD says that it should be classed as Mode 3, but there is no consistency on this across countries.

Open Government Data:

Making public information available in machine-readable, open formats that can be searched, retrieved, used, reused, and redistributed is generally not a controversial issue, and ORG and most digital rights organisations would support this.

In principle current relevant UK regulation - the Public Sector Information (PSI) Directive - is completely aligned with this. The Directive is being reviewed at present, however, with a

controversial proposal to include “public undertakings” in the scope. This would mean that public companies across the EU - transport, energy, telecoms, etc. - would need to make their data available similarly to government departments. This has been rejected by various MEPs who argue that it would create unfair competition and give an advantage to the private sector and specifically big US tech companies.

The idea of opening PSI is based on creating a *level playing field* where the section of a public body that produced data as part of their public task would share it in equal terms with both the section of the public body that created a commercial value added product and private sector competitors.

Extending PSI to data generated by public undertakings is a substantial move. In some countries (Finland, Italy, Greece, France) public undertakings form around 15% of the economy, and for the EU as a whole is 10%. In employment terms it’s even more important: 56% in transport and telecommunications and 55% in the energy sector.[ix]

It is unclear whether the proposal will be accepted, and in that case whether the UK will implement it, but it could have huge implications. In the UK there is a lot of public mistrust of big tech companies such as Google and Facebook, along the lines expressed by MEPs. If these open data controversies get entangled with a US FTA there could be a backlash, so it may be wiser to keep open data out of trade discussions.

Liability for Non-IP Content:

The US wants to use trade rules to enshrine the protection of Internet intermediaries from liability for content created by third parties. As discussed elsewhere, this is one of the basic blocks of the Internet, but we are concerned about using trade deals to introduce such proposals. In addition to the lack of a rights framework and due process for consumers, bundling such positive aspects can act as a sweetener that enables the introduction of measures that groups such as ORG would reject.

i https://www.theguardian.com/commentisfree/2018/may/22/data-big-tech-eu-regulation-gdpr

iihttps://bit.ly/2Pl80xr

iiihttps://ustr.gov/about-us/policy-offices/press-office/press-releases/2018/july/fourth-meeting-us-uk-trade-and

ivhttps://www.twn.my/MC11/briefings/BP4.pdf

vhttps://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf p. 184

vihttps://www.wto.org/english/tratop_e/serv_e/cbt_course_e/c1s3p1_e.htm

viihttps://www.bu.edu/ilj/2015/11/24/mode-1-mode-2-or-mode-10-how-should-internet-services-be-classified-in-the-global-agreement-on-trade-in-service/

viiihttp://blogs.sussex.ac.uk/uktpo/publications/the-engagement-of-uk-regions-in-mode-5-services-exports/

ix(http://www.europarl.europa.eu/workingpapers/econ/w21/sum-1_en.htm)