
Level 7, 321 Pitt Street
Sydney NSW 2000
Australia
Ph +61 2 9699 3686
ACN 097 603 131
ABN 83 659 681 462

# Submission to the Joint Standing Committee on Treaties
# Inquiry into the Australia-Singapore Digital Economy Agreement (DEA)

## September 2020

Contact Dr Patricia Ranald
campaign@aftinet.org.au

# Contents

## Summary and Recommendations

The DFAT National Interest Analysis (NIA) argues that the Singapore DEA is a significant agreement that it wants to use as a model for future regulation of the digital economy. If this is the case, the agreement should be subject to the highest levels of public and parliamentary scrutiny and debate. The need for such scrutiny is reinforced by the increased profitability and market concentration of companies operating in the digital domain in the context of the COVID-19 pandemic, and the need for public interest regulation to prevent abuse of market domination and to protect consumers.

In fact, the DEA faces less scrutiny and accountability. The lack of enabling legislation and absence of a parliamentary debate and vote on the DEA means that the process for this agreement is even less transparent and accountable than previous agreements. In this sense it is a Trojan horse which may escape the detailed public and parliamentary scrutiny it deserves.

The DFAT NIA argues that the deregulatory agenda of the DEA goes further than any previous agreement and will be used as a model for the future of the digital economy. The DEA limits regulation of transfer and storage of data across borders and prohibits requirements for local facilities. Combined with provisions in the services chapter of SAFTA, it also prohibits requirements for local presence of digital trade companies doing business in Australia. The DEA also restricts regulation of source code and potentially algorithms. There are exceptions for government data, personal credit data and some health data, but these are limited. This means that companies can conduct digital trade in Australia without any local presence or local facilities and without any scrutiny of source code and algorithms.

DFAT concedes that the DEA "will impose new restrictions on Australia's policy flexibility to impose certain measures to restrict data flows or require data localisation". DFAT claims that adequate public interest regulation will be permitted by exceptions in the agreement.

However this submission presents evidence that, in the context of the rapidly developing digital economy and emerging regulatory challenges identified by the Australian Competition and Consumer Commission and the Human Rights Commission, the exceptions are limited and the DEA restrictions on policy flexibility could restrict governments from regulating in the public interest.

For example, it is not clear whether DEA exceptions would be adequate to address the issues raised by Alinta Energy's recent failure to abide by undertakings to store data in Australia, and its subsequent failure to protect personal data that was stored in Singapore and New Zealand.

The EU's General Data Protection Regulation (GDPR) is an emerging global standard for privacy protection which Australian companies need to do business with Europe. Australia is negotiating a free trade agreement with the EU in which this issue is likely to emerge. Commitments made in the DEA and used as a model for other agreements do not meet EU standards and raise the question of whether it is wise to commit to a lower privacy standard when the EU and many of its trading partners are committing to a higher privacy standard.

When Australia's COVID-19 tracing app was launched in April 2020 amid public controversy about privacy protections, the government hastened to reassure potential users that their privacy would be protected by the data being stored in Australia. It is not clear whether the exceptions in DEA would permit similar requirements to store personal data in Australia in future.

The government agreed to make the source code of the COVID-19 tracing app available for examination by privacy experts and followed their recommendations for changes to protect privacy. The publication of source code and its subsequent modification were made before the DEA text was made public. The Committee should ascertain whether the exceptions in DEA would permit similar

access and modification of source code and algorithms in future.

There is increasing public concern about the mass use of facial recognition technology, reflected in the recommendations of bodies as diverse as the Parliamentary Joint Committee on Intelligence and Security and the Human Rights Commission. Both have recommended suspension of the use of this technology pending the development of robust privacy and human rights protections. The committee should examine whether the DEA gives sufficient regulatory space to enable such regulation.

The recent Victorian report on the on-demand workforce has exposed exploitation of workers through digital platforms and the need for regulatory change to protect workers' rights**.** There is a risk that DEA rules will hinder this process by limiting policy space for regulatory reform and undermining government enforcement mechanisms for digital platforms.

**Recommendations**

1. **The Committee should thoroughly examine the DEA restrictions on regulation of transfer and storage of personal data across borders, on requirements for local facilities, and on regulation of businesses with no local presence, and whether the exemptions are adequate to protect the public interest.**
2. **The Committee should thoroughly examine whether the DEA protects the privacy of data stored overseas to Australian standards, given the DEA lacks agreed and enforceable international standards of privacy protections, .**
3. **The DEA restricts government access to source code with some exceptions. The Committee should examine whether the exceptions are adequate and whether DEA restrictions on access to and regulation of source code would restrict privacy protection in future.**
4. **The DEA also anticipates similar future restrictions on access to regulation of algorithms, despite the ACCC and Human Rights Commission evidence that search engine algorithms are used to reinforce market domination, and that personal data-sorting algorithms can be discriminatory. The Committee should oppose future restrictions on regulation of algorithms.**
5. **The Committee should support the Parliamentary Joint Committee on Intelligence and Security and the Human Rights Commission recommendations to suspend mass use of facial recognition technology pending the development of a robust regulatory framework to safeguard privacy and human rights. The Committee should examine whether the DEA gives sufficient regulatory space to enable such safeguards**.
6. **The SAFTA and the DEA ignore workers' rights, despite the mounting evidence of such rights being undermined by gig economy jobs run through digital platforms, as exposed by the recent Victorian report on the on-demand workforce, and the need for regulatory change to protect workers' rights. The Committee should examine whether the DEA gives sufficient regulatory space to enable such changes to protect workers' rights.**
7. **The Committee should support a review of the DEA three years after implementation to evaluate the impact on public interest regulation of provisions which prohibit limitations on offshore data storage, prohibit requirements to store data onshore or have local facilities or local presence, and limit regulation of source code and algorithms. The reviews should also examine whether ISDS provisions have been used by international companies engaging in digital trade.**

## Introduction

The Australian Fair Trade and Investment Network (AFTINET) is a national network of 60 community organisations and many more individuals supporting fair regulation of trade, consistent with democracy, human rights, labour rights and environmental sustainability.

AFTINET supports the development of fair trading relationships with all countries and recognises the need for regulation of trade through the negotiation of international rules.

AFTINET supports the principle of multilateral trade negotiations, provided these are conducted within a transparent and democratically accountable framework that recognises the special needs of developing countries and is founded upon respect for democracy, human rights, labour rights and environmental protection.

AFTINET advocates that non-discriminatory multilateral rules-based trade negotiations are preferable to preferential bilateral and regional negotiations that discriminate against other trading partners.

AFTINET welcomes the opportunity to make this submission to the JSCOT inquiry into the Australia-Singapore Digital Economy Agreement (DEA).

## The process for negotiation of the DEA has been secretive and the absence of implementing legislation means there will be no open parliamentary debate or vote

Australia's current procedure for negotiating and ratifying trade agreements is secretive. There is limited consultation with civil society stakeholders, and the parliament does not discuss the negotiating mandate.

Negotiating texts are secret and the final texts of the agreements are not made public until after Cabinet has made the decision to sign them. It is only after they have been signed and tabled in Parliament that JSCOT reviews them. There is a current JSCOT inquiry into this process.

The National Interest Analysis (NIA) is not independent but is conducted by the same department that negotiated the agreement. There are no independent human rights or environmental impact assessments. Parliament has no ability to change the agreement and can only vote on the implementing legislation.

The Productivity Commission has made recommendations for the public release of the final text and independent assessments of the costs and benefits of trade agreements before they are authorised for signing by Cabinet (Productivity Commission 2010 and 2019). The EU has developed a more open process, including public release of its negotiating texts during negotiations and release of final texts before they are signed (EU 2019).

AFTINET supports publication of negotiating texts, publication of the final text of agreements and independent evaluation of the economic, health, gender, environmental and regional impacts of agreements before the decision is made to sign them. Parliament should vote on the whole text of an agreement, not just the implementing legislation.

The process for negotiating the DEA has been shorter and more secretive than some other agreements. The absence of enabling legislation means there will be even less parliamentary debate than with other agreements.

AFTINET was informed of the specific DEA negotiations at a general DFAT consultation about all trade agreements in December 2019, by which time the negotiations were nearing completion. AFTINET made a detailed submission in February 2020 about digital trade negotiations which dealt with both the Singapore DEA and the WTO plurilateral negotiations (AFTINET 2020). We had one consultation on March 3, 2020, by telephone about our submission.

The negotiations were announced as completed on March 23, 2020, but the text was not released until after signing on August 10, 2020. The DFAT National Interest Analysis notes that no enabling legislation is required (DFAT 2020a: 30). This means that there is no opportunity for the whole Parliament to debate or scrutinise the agreement.

The secretive process and lack of parliamentary debate matters because the DEA is not just an amendment to one agreement, but is seeking to set an ambitious deregulatory benchmark for other digital trade agreements. In this sense it is a Trojan horse, which it appears may escape detailed scrutiny.

## The need for public interest regulation of the digital domain

Digital trade is a complex area of trade law that is directly tied with provisions relating to financial services and broader trade-in-services as well as the rapid emergence of the digital economy. As the digital economy develops it is bringing both new opportunities and new risks and challenges. It is widely recognised, including by numerous government and expert inquiries in Australia and internationally, that governments must develop new regulatory frameworks and techniques that ensure the digital economy benefits everyone, and that consumer rights and human rights, particularly privacy rights and rights against discrimination, are not undermined.

Recent issues arising from the lack of regulation of digital platforms and the business practices of big technology companies include:

- Facebook and Google's abuse of personal data (Waterson 2018, MacMillan 2018), including an ongoing Australian Information Commission action in the Federal Court (Snape and Bogle 2020);
- Anti-competitive practices by Facebook, Google and Amazon (Ho 2019);
- Uber classifying itself as a technological platform, not an employer, to avoid regulation of working conditions (Bowcott 2017);
- Apple's tax avoidance (Drucker and Bowers 2017).

The 2019 Australian Competition and Consumer Commission (ACCC) Digital Platforms Report recommended more, not less, regulation of digital trading companies to protect consumer privacy and prevent discriminatory use of source code and algorithms and restrictive trade practices. Its recommendations for regulatory change are ongoing (ACCC 2019). There is also an ongoing review of the human rights aspects of digital trade being conducted by the Australian Human Rights Commission (Australian Human Rights Commission 2019).

The COVID-19 pandemic has turbo-charged the digitalisation of many aspects of daily life and has increased the profitability and market concentration of companies operating in the digital domain (Wakabayashi et al 2020).

Threats by Facebook and Google to resist regulation of news media content recommended by the ACCC by withdrawing news media content illustrate their ability to exercise the power associated with such market concentration (Doran and Hayne 2020).

It is clear that the Australian public interest regulatory framework is still developing in this context. Yet the incorporation of digital trade rules in bilateral and regional trade agreements could restrict governments from implementing future public interest regulation. The global digital trade agenda has been heavily influenced by the technology industry lobby, including global companies like Apple, Google, Facebook and Amazon. Digital trade rules seek to codify the technology industry wish list, which is known as the Digital2Dozen principles (Office of the United States Trade Representative 2016). These principles maximise digital trade opportunities for global corporations but can neglect the impacts on consumer rights and human rights.

Key deregulatory principles are the maximisation of cross-border data flows, prohibition of requirements for local data storage and local presence and prohibition of access to source code and algorithms. This framework could restrain governments from regulating the digital domain and the operations of big technology companies.

Australia has been increasingly including more extensive deregulatory provisions on digital trade in recent trade agreements. The Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP) was the most comprehensive prior to the DEA (Kelsey 2017). The Australia-Hong Kong trade agreement was the first to include digital trade rules for financial services (AFTINET 2019). As discussed below, DFAT has confirmed that the DEA places further restrictions on government regulation.

## The DEA restricts regulation of cross-border data flows, data storage and access to source code more than any previous agreement and is being used as a benchmark

The DEA will replace the electronic commerce chapter in the Singapore-Australia Free Trade Agreement (SAFTA), which entered into force on 28 July 2003 and amendments which came into force on 1 December 2017.

The DFAT National Interest Analysis and Regulatory Impact Statement confirm that the DEA has more extensive deregulatory commitments than any previous agreement, and that its objective goes far beyond the amendments to one agreement. The objective is to "secure enhanced benchmark commitments and a platform for further liberalisation in the Indo Pacific and the WTO" (DFAT 2020a Regulation Impact Statement: 4).

Overall, the DEA goes further than any previous agreement in establishing a framework that restricts regulation of cross-border data flows, restricts requirements for local data storage and restricts regulation of source code and algorithms.

The DFAT NIA concedes that the DEA "will impose new restrictions on Australia's policy flexibility to impose certain measures to restrict data flows or require data localisation" but claims that "the restrictions are outweighed by benefits for Australian companies by limiting costly localisation requirements" (DFAT 2020a: 4).

The DFAT NIA claims that public interest regulatory concerns will be addressed by exceptions in the agreement.

Given this context, it is essential that the Committee thoroughly examine the extent of the restrictions on Australia's policy flexibility and whether the exemptions are adequate. It is also essential to consider how the DEA intersects with the overlapping obligations in other chapters of the agreement, especially those in chapter 7 trade-in-services, Chapter 8 investment and chapter 9 financial services.

## Cross-border transfer of information

DEA Article 23.2 states that "neither party shall prohibit or restrict the cross-border transfer of information by electronic means, including personal information, if this activity is for the conduct of business" (DFAT 2020b).

Article 23.3 allows governments to adopt or maintain measures inconsistent with article 23.2 to "achieve a legitimate public policy objective, provided that it is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade and does not impose restrictions on transfers of information greater than are required to achieve the objective".

This wording is common to a number of exceptions in the agreement, and places on governments the burden of proof that the public policy objective is legitimate, and the manner in which the restrictions are applied is not more restrictive than required to meet the objective. The difficulty of meeting these tests have been exposed by WTO case law for its general exceptions, which has identical wording. WTO Member governments have been unsuccessful in 48 out of 50 WTO disputes where they have invoked the WTO General Exception to defend forms of regulation (Public Citizen 2019).

## Location of computing facilities and local presence

Article 24.1 and 24.2 says that governments may have their own regulatory requirements, but cannot require a business to use or locate computing facilities in its territory as a condition of conducting business in the territory.

This should be read in conjunction with SAFTA trade-in-services chapter article 7.6 which says:

> Neither Party shall require a service supplier of the other Party to establish or maintain a representative office or any form of enterprise, or to be resident, in its territory as a condition for the cross-border supply of a service (DFAT 2017).

This could mean that a business conducted online in Australia would not have to have any form of presence or any facilities located in Australia and could store all of its data overseas.

This can present problems for the regulation of such businesses in relation to taxation. For example, in a recent case in France, the Paris Administrative Court of Appeals found that Google Ireland did not have to pay a 1.11bn Euro tax bill because it doesn't have a permanent base in France (Sebag 2019)

The complex impact of digital trade rules on taxation has been analysed in a recent publication by prominent legal academics, *How 'Digital Trade' Rules Would Impede Taxation of the Digitalised Economy in the Global South* (Kelsey et al 2020).

The general exemption for tax measures in SAFTA has not been updated to reflect the complexities of digital trade. The Committee should examine whether the DEA allows enough regulatory space to deal with these issues.

The lack of local presence, and data stored offshore can also have impacts for workers and undermine Australian employment law, which is discussed further below.

### DEA exceptions for cross-border data storage and location of facilities

Exceptions include government procurement, information held or processed on behalf of government, personal credit information (but not other data held by financial institutions), and data related to measures like health listed as reservations in the trade-in-services chapter and the financial services chapter of the SAFTA (Article 2).

Article 25 qualifies the prohibition for financial institutions on locating computing facilities onshore by requiring that the government's financial regulatory authorities shall have access to information processed or stored offshore for some regulatory purposes. The government must provide financial institutions that are locating or processing information offshore with a reasonable opportunity to remediate any lack of access to information before requiring the institution to use or locate facilities within the government's territory.

These exceptions are welcome, but they still leave a wide range of personal information and other that can be stored offshore. Also the Committee should examine whether the exemption for government information clearly applies to government data being managed by privatised entities, or by private companies contracted by government agencies. Note that this was an issue in the Alinta case explained below.

## Personal information protection

Article 17.2 states that each government shall adopt or maintain a legal framework that provides for the protection of personal information. Article 17.5 says that governments shall publish information on how the person can pursue remedies and business can comply with any legal requirements.

However, there is no mandatory standard of protection, as governments are simply asked to "take into account" the principles and guidelines of relevant international bodies (article 17.2), and certain key principles (article 17.3).

Article 17.7 recognises that the parties may take different legal approaches to protecting personal information and says they shall "encourage the development of mechanisms to promote compatibility between different regimes," and "endeavour to exchange information and share experiences".

In summary, each government can develop its own standards, and there are some recommended principles but there is no agreed international mandatory standard.

### Uncertainty about the application of Australia's privacy law to data stored overseas and companies with no local facilities

Australia's privacy law has its own limitations because the Privacy Act does not apply to all entities. For example, it does not apply to small business, employee data and political parties (Office of the Australian Information Commissioner).

The ACCC Digital Platforms Review recommended changes to the Privacy Act including proposed initial reforms for 2020, along with a more expansive review of privacy law to be completed in 2021 (Lincoln *et al* 2020).

The DEA is likely to come into force before this review and could limit its recommendations.

The transfer and storage of information across borders and the prohibition of local facilities and local presence raises the question of whether and how the privacy of Australian consumers will be protected in different jurisdictions, given the lack of agreed and enforceable international standards of privacy protections. Three examples below highlight these issues.

### Alinta Energy company data storage overseas and breaches of personal data privacy standards

Documents leaked to the *Sydney Morning Herald* revealed in March 2020 that Chow Tai Fook Enterprises (CTFE), the Hong Kong company that now owns the privatised Australian Alinta Energy company, was storing sensitive personal data from Australian customers overseas without adequate privacy protections. The data included names, addresses, birth dates, mobile numbers, Medicare and passport numbers, credit card details and in some cases individual health information. This was occurring despite undertakings given to the Australian government at the time of sale in 2017 that data would be stored in Australia and would be protected in accordance with Australian privacy laws (Ferguson and Gillett 2020).

The leaked documents revealed that contrary to these undertakings, one million Australian consumers' data, controlled by a subsidiary company of Alinta Energy, is being stored in Singapore and New Zealand. A June 2019 privacy compliance audit by Alinta's internal auditor EY assigned the company a "red" or "significant" risk rating on key aspects of its privacy compliance. It said Alinta "lacked proper oversight and structure to manage privacy and may not be adequately protecting personal information" and at times "doesn't meet the requirements of privacy laws" (Ferguson and Gillett 2020).

Following publication of the leaked documents, the office of the Australian Information Commissioner launched an inquiry into Alinta Energy's handling of Australians' personal information. That the office only became aware of these issues following the leaking of documents highlights the difficulty of effectively monitoring and regulating data stored overseas, including in Singapore (Office of the Australian Information Commissioner 2020).

In this case, the company appears to have breached undertakings made at the time of sale to store the data in Australia. The DEA commitments against such requirements will make overseas data storage more common. It is not clear how Australia's data privacy standards will be monitored or enforced when data is stored overseas.

### The EU's General Data Protection Regulation (GDPR)

Another example of the difficulty of enforcing privacy standards in other jurisdictions is provided by the EU's General Data protection Regulation (GDPR). This is one of the world's strongest privacy protection frameworks, which requires governments to certify that, if European data is stored in their jurisdiction, they have a comparable level of privacy protection to that provided in the EU. A recent European Court of Justice decision found that US privacy regulation did not meet the EU standards, particularly in relation to government surveillance and access to effective remedies. This ruling means that data about European citizens cannot be exported unless an adequate level of data protection is guaranteed though specific contracts with particular companies (Stolten 2020).

Expert commentators like Monash University Professor Norman Witzleb are now suggesting that EU privacy standards are higher than current Australian standards, and that to comply with the ECJ ruling, international companies need to engage in a more detailed risk analysis than before. In some cases, data may no longer be transferred. He argues that this is likely to contribute to an international trend to house critical data locally (Witzleb 2020).

The EU GDPR is an emerging global privacy standard that Australian entities doing business in the EU are expected to meet. The ECJ ruling means that Australian businesses operating in the EU may have to meet stricter EU privacy standards, which may involve requirements for data storage in the EU. Australia is negotiating a free trade agreement with the EU in which this issue is likely to emerge.

The Committee should ascertain whether the commitments made in the DEA and used as a model for other agreements do not preclude companies being able to meet EU standards and whether it is wise to commit to a lower privacy standard when the EU and many of its trading partners are committing to a higher privacy standard.

### The Australian COVID-19 Tracing App

The trend to store critical data locally emerged when Australia's COVID-19 tracing app was launched in April 2020 amid public controversy about privacy protections. The government hastened to reassure potential users that their privacy would be protected by the data being stored in Australia, even if it was outsourced to a private contractor (Kemp and Greenleaf 2020).

The government claimed that the Biosecurity (Human Biosecurity Emergency) Determination 2020, and the *Privacy Amendment (Public Health Contact Information) Act 2020* prevented data from COVIDSafe being retained outside Australia, and protected against unauthorised disclosure outside Australia (Commonwealth Attorney General's Department 2020).

It appears that in a public debate following the Alinta case, the government itself did not want to rely on the promise that the Australian standard of privacy protection could be extended to data stored overseas, hence it required that data would be stored locally. There was also a public debate about the COVIDSafe source code that is discussed below.

The Committee should ascertain whether the exceptions in the DEA for information held or processed on behalf of government would permit similar requirements to store personal data in Australia, even if the data is being held or processed by a private contractor.

## Limits on access to and regulation of source code

The DEA prohibits governments from requiring the transfer of or access to source code of software as a condition for the import, distribution, sale or use of such software (Article 28.1).

However, governments can require such access to be made available for investigation or enforcement actions by government agencies, or for source code to be modified to comply with laws and regulations (Articles 28.2 and 28.3).

After the public controversy over the privacy regulation of the COVID-19 app discussed above, the government agreed to release the source code for the app, so that it could be examined by IT privacy experts. This was done, feedback was given, and the government made modifications over several months to increase privacy protection (Australian Government Digital Transformation Agency 2020).

The publication of source code and its subsequent modification were made before the DEA text was made public.

The Committee should ascertain whether the exceptions in the DEA would permit similar access and modification of source code in future.

### Limits on access to and regulation of Algorithms

Algorithms are "a set of mathematical instructions or rules that, especially if given to a computer, will help calculate an answer to a problem" (Cambridge Dictionary 2020). They are increasingly used by technology companies to sort data for search engine results, which means that the choice of algorithms increasingly controls access for consumers to information on the internet.

As the use of algorithms is expanding, growing evidence demonstrates that algorithms can be used by companies to reduce competition. For example, in 2017 the European Commission fined Google €2.42 billion for breaching EU antitrust rules after finding that "Google abused its market dominance as a search engine by promoting its own comparison shopping service in its search results, and demoting those of competitors" (European Commission 2017).

The ACCC report raised similar concerns about the opacity of Google and Facebook's key algorithms, arguing that their near monopoly market power and lack of algorithmic transparency increases the potential for anti-competitive behaviour, including self-preferencing to reduce competition (ACCC 2019:12).

In the current negotiation between the ACCC and Facebook about news content, Facebook has refused to enable access to the algorithms used to sort media content (Tonkin 2020).

These examples show algorithms can be abused in situations where impartial selection of data is required to prevent self-referencing.

Evidence of other forms of algorithmic bias is also increasing. Algorithms are used to sort personal data or assess video interviews for purposes like selection for employment interviews, in which value judgements are required to ensure that potential race, gender, class or other biases are identified and minimised.

Algorithms "are inescapably value-laden" and "operational parameters are specified by developers and configured by users with desired outcomes in mind that privilege some values and interests over others" (Mittelstadt *et al* 2016). For example, in 2018 Amazon was forced to abandon a computer program using an algorithm that was designed to review job applications after it found that it discriminated against women (Dastin 2018).

The DEA prohibition on access to source code does not yet apply to algorithms (article 28.4).

However, the same article states that if both governments undertake obligations under future international agreements that prohibit transfer of algorithms, then the prohibition on requirements to transfer would also apply to algorithms.

This could reduce the ability of governments to access and regulate algorithms, at a time when there is increasing evidence that governments need to access and regulate algorithms both to ensure competition in the digital domain and to prevent discrimination.

## Consumer protection, online safety and Artificial Intelligence less legally binding than other parts of the agreement

### Consumer Protection

The DEA requires each party to adopt or maintain consumer protection laws to proscribe misleading and deceptive commercial activities that cause harm or potential harm to consumers (article 15.3).

However, there is no mandatory minimum standard for such laws. Instead, governments will promote cooperation on matters of mutual interest (article 15.5).

### Safe online environment

Clauses on creating an environment where users are protected from harmful content, including terrorist and violent extremist content are also non-binding rather than mandatory.

They recognise that online safety is a significant challenge (article 18.1) and will work together with international fora to create a safe online environment, in accordance with their respective laws and regulations (article 18.4).

Overall the rules that restrict government regulation are stronger, more legally binding and enforceable, while these consumer protections are much weaker and are not legally enforceable.

## Artificial Intelligence and facial recognition technology

The DEA recognises that the use of and adoption of Artificial Intelligence (AI) technology is increasing, emphasises that it offers significant social and economic benefits, and supports co-operation in sharing in the development of AI technology (article 31.1).

There is recognition of the importance of developing ethical governance frameworks for the trusted safe and responsible use of AI technology, taking into account internationally recognised principles or guidelines (articles 31.2 and 31.3). The Memorandum of Understanding (MoU) on AI is separate from the DEA and is not legally binding.

One of the most controversial uses of AI, which is not specifically mentioned in the agreement or the MoU is the mass use of facial recognition technology. AI is used to harvest images of people through social media without their knowledge or consent and can be used to identify them in public places and at mass events.

The AHRC's discussion paper on Human Rights and Technology details the human rights risks associated with mass use of facial recognition technology, which is already being used by government agencies in Australia. A *Sydney Morning Herald* investigation revealed in January 2020 that Australian state police forces are using facial recognition technology and privacy experts warned that this was taking place without public knowledge or any public regulatory framework (Evans and Webb 2020).

The Human Rights Commission highlighted evidence that the use of facial recognition technology by police can increase the risk of profiling, particularly racial profiling. It also pointed to the "emerging evidence that facial recognition technology generally is less accurate when identifying women and people from minority ethnic and racial groups" (Australian Human Rights Commission: 29).

It is clear that the use of this technology is leaping ahead of public awareness and discussion, and government's ability to regulate it to protect individual privacy.

In October 2019 the Commonwealth government's proposed *Identity-matching Services Bill 2019* which would have enabled a national facial biometrics matching scheme was rejected by the bipartisan Parliamentary Joint Committee on Intelligence and Security after a public review received critical submissions. The Committee cited concerns about lack of privacy protections and concluded that the bill should be re-written to incorporate "privacy and transparency and be subject to robust safeguards" (Joint Committee on Intelligence and Security 2019: 5.7).

Following this Parliamentary Report, in December 2019 the Human Rights Commission Report called

for a "moratorium on the potentially harmful use of facial recognition technology in Australia" until there is a legal framework to safeguard human rights (Australian Human Rights Commission 2019).

The Committee should support this recommendation made by both bodies. The committee should examine whether the DEA gives sufficient regulatory space to enable such safeguards.

It is essential that any future international regulation of AI, as foreshadowed in the DEA, should not prevent effective regulation to safeguard individual privacy, prevent discrimination and safeguard against other human rights abuses.

## State-to-State dispute settlement and ISDS apply to the DEA

The DEA, as a chapter of SAFTA, is enforceable through the state-to-state dispute mechanism which applies to all legally binding trade agreements whereby one government can lodge a dispute by alleging a breach of the legally binding terms in the chapter.

Singaporean investors in Australia will also have access to a separate disputes process known as Investor-State Dispute Settlement, if they can argue that a change in Australian law or policy reduces the value of their investment (indirect expropriation) or was introduced without adequate consultation (fair and equitable treatment).

ISDS is controversial and is included in only some trade agreements. ISDS was so controversial that the Howard Coalition government did not agree to include it in the AUSFTA in 2004, and the Productivity Commission recommended against its inclusion in trade agreements (DFAT AUSFTA text 2004, Productivity Commission 2010:274).

ISDS has been rejected by the low-income majority of countries in the 164-member WTO, but has been included in some preferential regional trade agreements like the CPTPP and the SAFTA. But ISDS has been excluded from the current negotiations for the Australia-EU Free Trade Agreement and from negotiations for the 15-member Regional Comprehensive Economic Partnership between Australia, New Zealand, Japan, China, South Korea and the 10 ASEAN countries (DFAT 2019, Ranald 2019b).

ISDS tribunals are staffed by practising advocates, not independent judges, and there are no precedents or appeals, leading to inconsistent decisions (French 2014, Kahale 2014).

There are now over 1,000 ISDS cases, many against low-income countries (UNCTAD 2020a), with costs awarded against governments amounting to hundreds of millions or even billions of dollars (Bonnitcha and Brewin 2019, Tienhaara 2019).

The US Philip Morris tobacco company could not use ISDS in the US -Australia FTA because community opposition had kept it out of that agreement. The company shifted some assets to Hong Kong and used ISDS in a Hong Kong investment agreement to claim billions in compensation from the Australian government for Australia's plain packaging legislation. Defeating this case took a total of seven years, cost the Australian government $12 million in legal costs, and other countries delayed similar regulation pending the result (Ranald 2019a).

There are now ISDS cases against government regulation to reduce carbon emissions and to combat climate change. For example, the US Westmoreland Coal Company is suing Canada over a decision by the Alberta province to phase out all coal powered energy (Tienhaara 2018).

In the context of the COVID-19 pandemic, there are also cases from global companies claiming compensation for government actions during the pandemic that reduced their profits but were essential to save lives.

Peru cancelled road tolls to facilitate internal transport of essential goods during the pandemic and has been threatened with an ISDS case by private road toll operators (Sanderson 2020).

Legal firms specialising in ISDS are already advising corporations on possible cases. An international arbitration law firm has told its clients:

> While the future remains uncertain, the response to the COVID-19 pandemic is likely to violate various protections provided in bilateral investment treaties and may bring rise to claims in the future by foreign investors…While States may invoke *force majeure* and a state of necessity to justify their actions, as observed in previous crises that were economic in nature, these defences may not always succeed (Aceris Law 2020).

Legal scholars critical of ISDS have confirmed that after the pandemic governments could face claims for compensation from global corporations. They have called for all governments to withdraw consent from ISDS rules to avoid an avalanche of cases relating to the pandemic (International Institute for Sustainable Development 2020).

UNCTAD, the UN body which monitors ISDS cases, has also acknowledged this danger (UNCTAD 2020b: 11-12). Prominent global economists and lawyers led by Jeffrey Sachs have called for a moratorium on ISDS claims relating to government actions during the pandemic (Columbia Centre on Sustainable Investment 2020). Six hundred and thirty civil society groups have written to governments about the dangers of such cases, asking them to withdraw from ISDS arrangements (Civil Society Organisations 2020).

It is clear that the regulatory environment for digital trade is still being developed in Australia, and that new regulation will be required in some areas. As discussed above, it is debatable whether the DEA rules and exceptions in areas like cross border data transfer, localisation of computing facilities, local presence, access to source code and algorithms and regulation of privacy and artificial intelligence allow enough regulatory space for such new regulation.

ISDS rules in SAFTA could result in cases from Singapore companies claiming compensation for new Australian regulation in these areas. If the DEA is used as a model in other agreements containing ISDS, there could be cases from companies from countries which are party to those agreements.

## The DEA and workers' rights in the gig economy: retaining regulatory space

The SAFTA has no commitments by governments not to reduce labour rights, nor to implement internationally-agreed labour rights which are defined by the International Labour Organisation (ILO). These rights include freedom of association, right to collective bargaining, no forced labour, no child labour and no discrimination in the workplace, and national minimum standards on wages, hours of work and workplace health and safety (ILO 1998).

Such rights are included in other agreements like the Australia-US FTA, the Korea-Australia FTA and the CPTPP, although they vary in scope and enforceability. AFTINET believes that these rights should be enforced by the government-to-government disputes process of the agreement.

The rise of the digital economy can undermine workers' rights by classifying workers as contractors or individual businesses (Sutherland 2019), thus removing the responsibility for gig-economy giants like Uber or Deliveroo to provide basic employee entitlements (Bowcott 2017, Waters 2017).

By enabling global corporations, including those operating in the gig economy, to access Australian markets without a local presence, digital trade rules could worsen the situation for workers and undermine Australian employment law. The International Trade Union Confederation (ITUC) argues that "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" (ITUC 2019).

The use of digital platforms to organise and compensate irregular work, and the ability of businesses to classify their workers as independent businesses in their own right, raise questions about the effectiveness of existing labour laws and standards, and the need for changes so that minimum standards can apply to all workers.

These issues have been raised by the Report of the Victorian Government's Inquiry into the Victorian On-Demand Workforce. The report has made recommendations for changes in regulation to both the Commonwealth and Victorian governments (Industrial Relations Victoria 2020: 189-206).

Concerns have also been raised about the impact that new technologies like AI can have in recruitment practices and on work conditions. The ITUC points to the risk that "algorithmic bias and data control makes hiring and firing less transparent" (ITUC 2018). Data collection and new technologies can also increase opportunities for workplace surveillance, with workers increasingly monitored and evaluated using AI (Centre for Future Work 2019).

It is essential that the governments retain the flexibility to implement policy reform and innovative regulation to respond to emerging issues in relation to labour rights and conditions. However, there is a risk that digital trade rules will hinder this process by limiting policy space for regulatory reform and undermining government enforcement mechanisms.

# References

Aceris Law (2020) The COVID-19 Pandemic and Investment Arbitration. 26 March, available at https://www.acerislaw.com/the-covid-19-pandemic-and-investment-arbitration/.

Australian Competition and Consumer Commission (2020) Digital Platforms Inquiry Report 26 July, Canberra, available at https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry.

Australian Fair Trade and Investment Network (2020) *Submission to the Department of Foreign Affairs and Trade On the Plurilateral Negotiations on Trade-Related Aspects of Electronic Commerce*, February, available at https://www.dfat.gov.au/sites/default/files/digital-trade-submission-aftinet.pdf.

Australian Government Digital Transformation Agency (2020) "Strengthening privacy protections for COVIDSafe app users", May 26, available at https://www.dta.gov.au/news/strengthening-privacy-protections-covidsafe-app-users.

AFTINET (2019) Submission to the Joint Standing Committee on Treaties Inquiry into the *Free Trade Agreement between Australia and Hong Kong, China And* The *Investment Agreement between the Government of Australia and the Government of the Hong Kong Special Administrative Region of the People's Republic of China,* August 2019, pp 11-13, available at http://aftinet.org.au/cms/sites/default/files/AFTINET%20A-HKFTA%20JSCOT%20submission.pdf#overlay-context=node/1771.

Australian Human Rights Commission (2019) *Human Rights and Technology: Discussion Paper,* December, available at https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights_2019_DiscussionPaper.pdf.

Bonnitcha J., and Brewin S., (2019) Compensation under Investment Treaties, International Institute for Sustainable Development, October, available at https://www.iisd.org/sites/default/files/publications/compensation-treaties-best-practicies-en.pdf

Bowcott, O. (2017) "Uber to face stricter EU regulation after ECJ rules it is transport firm", *The Guardian*, December, available at https://www.theguardian.com/technology/2017/dec/20/uber-european-court-of-justice-ruling-barcelona-taxi-drivers-ecj-eu.

Cambridge Dictionary, (2020) Cambridge, available at https://dictionary.cambridge.org/dictionary/english/algorithm.

Centre for Future Work (2019) "Turning 'Gigs' Into Decent Jobs - Submission to: Inquiry into the Victorian On-Demand Workforce", pp 17-18, available at https://s3.ap-southeast-2.amazonaws.com/hdp.au.prod.app.vic-engage.files/8815/5669/1362/The_Australia_Institute.pdf.

Civil Society Organisations (2020) An open letter to governments on ISDS and COVID-19, June. http://s2bnetwork.org/wp-content/uploads/2020/06/OpenLetterOnISDSAndCOVID_June2020.pdf

Columbia Centre on Sustainable Investment (2020) Call for ISDS Moratorium During COVID-19 Crisis and Response. Columbia Law School, 6 May, http://ccsi.columbia.edu/2020/05/05/isds-moratorium-during-covid-19/.

Commonwealth Attorney General's Department (2020) "COVIDSafe Legislation." May 14, available at https://www.ag.gov.au/rights-and-protections/privacy/covidsafe-legislation.

Dastin, J. (2018) "Amazon scraps secret AI recruiting tool that showed bias against women", October 10, available at https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

Department of Foreign Affairs and Trade (2004) AUSFTA Text available at http://dfat.gov.au/about-us/publications/trade-investment/australia-united-states-free-trade-agreement/Pages/table-of-contents.aspx [accessed February 20, 2015].

Department of Foreign Affairs and Trade (2017) Text of the Singapore-Australia Free Trade agreement available at https://www.dfat.gov.au/trade/agreements/in-force/safta/official-documents/Pages/default

Department of Foreign Affairs and Trade (2019) RCEP outcomes at a glance, November 4, available athttps://www.dfat.gov.au/sites/default/files/rcep-outcomes-at-a-glance.pdf

Department of Foreign Affairs and Trade (2020a) National Interest Analysis Australia-Singapore Digital Economy Agreement, (including Regulatory Impact Statement) August 6, Canberra, available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Treaties/DigitalEconomySingapore/Treaty_being_considered.

Department of Foreign Affairs and Trade (2020b) Text of the Australia-Singapore Digital Economy Agreement, August 6, available at https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement

Doran M., and Hayne J. (2020) "Facebook threatens to ban Australians from sharing news after Google launches attack on Government plans, ABC News, September 1, available at https://www.abc.net.au/news/2020-09-01/facebook-threatens-to-ban-australians-from-sharing-news-content/12616216.

Drucker, J and Bowers, S, (2017) "After a Tax Crackdown, Apple Found a New Shelter for Its Profits", The New York Times, November, available at https://www.nytimes.com/2017/11/06/world/apple-taxes-jersey.html.

European Commission (2017) "Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service", June, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784

European Union (2015) *EU negotiating texts in TTIP*, February, Brussels, available at http://trade.ec.europa.eu/doclib/press/index.cfm?id=1230 [accessed February 12, 2015].

European Union (2020) EU proposal for the EU-Australia FTA Intellectual Property Chapter Article X.45. p.28, available at http://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157190.pdf.

Evans, M and Webb, C, (2020) "Australian police using face recognition software as privacy experts issue warning", January 19, available at https://www.smh.com.au/national/australian-police-using-face-recognition-software-as-privacy-experts-issue-warning-20200119-p53ssj.html.

Ferguson A. and Gillett C. (2020) "Credit cards, addresses and phone numbers vulnerable: More than one million energy customers' privacy at risk", *Sydney Morning Herald*, March1, available at https://www.smh.com.au/business/companies/credit-cards-addresses-and-phone-numbers-vulnerable-more-than-one-million-energy-customers-privacy-at-risk-20200228-p545bw.html.

French, R.F. Chief Justice (2014) "Investor-State Dispute Settlement - a cut above the courts?" Paper delivered at the Supreme and Federal Courts Judges conference, July 9, 2014, Darwin, available at

http://www.hcourt.gov.au/assets/publications/speeches/current-justices/frenchcj/frenchcj09jul14.pdf [accessed August 8, 2014].

Ho, V, (2019) "Tech monopoly? Facebook, Google and Amazon face increased scrutiny", The Guardian, June 4, available at https://www.theguardian.com/technology/2019/jun/03/tech-monopoly-congress-increases-antitrust-scrutiny-on-facebook-google-amazon.

Industrial Relations Victoria (2020) *Report of the Inquiry into the Victorian On-Demand Workforce*, June 12, Victorian Government, Melbourne, available at https://s3.ap-southeast-2.amazonaws.com/hdp.au.prod.app.vic-engage.files/4915/9469/1146/Report_of_the_Inquiry_into_the_Victorian_On-Demand_Workforce-reduced_size.pdf.

International Institute for Sustainable Development (2020) *Protecting Against Investor–State Claims Amidst COVID-19: A call to action for governments.* New York: Columbia University, available at https://www.iisd.org/library/investor-state-claims-amidst-covid-19.

International Labour Organisation (ILO) (1998) *Declaration on fundamental principles and rights at work*, Geneva, available at https://www.ituc-csi.org/IMG/pdf/ituc_globalrightsindex_2020_en.pdf.

ITUC (2018) "A workers' agenda for e-commerce," 2018, available at https://www.ituc-csi.org/WTO-public-forum-2018-workers-agenda-for-e-commerce.

ITUC (2019) "'E-commerce' push at WTO threatens to undermine labour standards", available at https://www.ituc-csi.org/e-commerce-push-at-wto-undermines-workers.

Joint Committee on Intelligence and Security (2019) *Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019* October, Canberra available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Identity-Matching2019/Report.

Kelsey, J. (2017) "The Risks for ASEAN of New Mega-Agreements that Promote the Wrong Model of e-Commerce," October, ERIA Discussion Paper Series. available at: http://www.eria.org/ERIA-DP-2017-10.pdf.

Kelsey J., Bush, J., Montes, M., Ndubai, J. (2020b) *How 'Digital Trade' Rules Would Impede Taxation of the Digitalised Economy in the Global South,* Third World Network, August, Geneva, available at https://www.globaltaxjustice.org/sites/default/files/Digital%20Tax%20-TWN.pdf.

Kahale, G. (2014) Keynote address, Eighth Juris Investment Arbitration Conference, Washington DC, 8 March, available at http://www.curtis.com/siteFiles/Publications/8TH%20Annual%20Juris%20Investment%20Treaty%20Arbitration%20Conf.%20-%20March%2028%202014.pdf.

Kemp, K. and Greenleaf G. (2020) "The COVIDSafe bill doesn't go far enough to protect our privacy. Here's what needs to change," *The Conversation*, May 6**,** available at https://theconversation.com/the-covidsafe-bill-doesnt-go-far-enough-to-protect-our-privacy-heres-what-needs-to-change-137880.

Lincoln J., Tsoi K., and Giral, M. (2020) "Australian Privacy Law Reform And Review Announced", available at https://www.mondaq.com/australia/privacy-protection/892384/australian-privacy-law-reform-and-review-announced.

MacMillan, D and McMillan, R, (2018) "Google Exposed User Data, Feared Repercussions of Disclosing to Public", *The Wall Street Journal*, October, available at https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194.

Mittelstadt, B., Allo, P., Taddeo,M., Wachter, S. and Floridi, L. (2016) "The ethics of algorithms: Mapping the debate", *Big Data & Society,* July–December. pp1-21, available at https://journals.sagepub.com/doi/pdf/10.1177/2053951716679679.

Office of the Australian Information Commissioner, no date "Privacy for Organisations", available at https://www.oaic.gov.au/privacy/privacy-for-organisations/.

Office of the Australian Information Commissioner(2020) "Inquires into Alinta Energy", March 1, available at https://www.oaic.gov.au/updates/news-and-media/inquiries-into-alinta-energy/.

Office of the United States Trade Representative (2016) "The Digital2Dozen principles", available at https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2016/digital-2-dozen.

Productivity Commission (2010) Research Report on Bilateral and Regional Trade Agreements, Melbourne, November, available at https://www.pc.gov.au/inquiries/completed/trade-agreements/report.

Productivity Commission (2020) Submission to the Joint Standing Committee on Treaties inquiry into certain aspects of the treaty making process, July, available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Treaties/Treaty-makingProcess/Submissions.

Public Citizen (2019) 'Fatally flawed WTO Dispute System', November, available at https://www.citizen.org/wp-content/uploads/WTO-Disputes-Summary-November-2019-FINAL.pdf.

Ranald, P. (2019a) When even winning is losing. The surprising cost of defeating Philip Morris over plain packaging. *The Conversation*, 27 March, available at https://theconversation.com/when-even-winning-is-losing-the-surprising-cost-of-defeating-philip-morris-over-plain-packaging-114279.

Ranald, P. (2019b) Suddenly, the World's largest trade agreement won't allow corporations to sue governments, *The Conversation*, September 17, available at https://theconversation.com/suddenly-the-worlds-biggest-trade-agreement-wont-allow-corporations-to-sue-governments-123582.

Sebag, G. (2019) "Google Wins Again in French Court Fight Over $1 Billion Tax Bill", April 26, available at https://www.bloomberg.com/news/articles/2019-04-25/google-wins-again-in-french-court-fight-over-1-billion-tax-bill.

Snape J., and Bogle, A. (2018) "Australian privacy watchdog launches court action against Facebook over Cambridge Analytica access," March 9, available at https://www.abc.net.au/news/2020-03-09/facebook-privacy-oaic-information-commissioner/12039642.

Stolten, S. (2020) "EU-US data transfers at critical risk as ECJ invalidates Privacy Shield," *Euractive*, July 16, available at https://www.euractiv.com/section/digital/news/eu-us-data-transfers-at-critical-risk-as-ecj-invalidates-privacy-shield/.

Sutherland, C. (2019) "It's just a gig: How the gig economy is stealing workers' Rights", May 15, available at https://www2.monash.edu/impact/articles/economy/its-simply-a-gig-how-the-gig-economy-stole-workers-rights/.

Tienhaara, K. (2018) The fossil fuel era is coming to an end but the lawsuits are just beginning. *The*

*Conversation*, 19 December, available at https://theconversation.com/the-fossil-fuel-era-is-coming-to-an-end-but-the-lawsuits-are-just-beginning-107512.

Tienhaara, K. (2019) World Bank ruling against Pakistan shows global economic governance is broken. 23 July, available at https://theconversation.com/world-bank-ruling-against-pakistan-shows-global-economic-governance-is-broken-120414.

Tonkin, C. (2020) "Facebook. Australians from posting news", *Australian Computer Society ICT News*. September 1, available at https://ia.acs.org.au/article/2020/facebook-will-stop-australians-from-posting-news.html.

United Nations Committee on Trade and Development (2020a) Investment Dispute Settlement Navigator. Geneva: UNCTAD, available at http://investmentpolicyhub.unctad.org/ISDS.

United Nations Committee on Trade and Development (2020b) Investment Policy Responses to the COVID-19 Epidemic UNCTAD, *Investment Policy Monitor* Geneva: May 4, available at https://unctad.org/en/PublicationsLibrary/diaepcbinf2020d3_en.pdf.

Wakabayashi, D., Weise, K., Nicas, J., Isaac, M. (2020) "The economy is in record decline, but not for the tech giants", *New York Times*, July 30, available at https://www.nytimes.com/2020/07/30/technology/tech-company-earnings-amazon-apple-facebook-google.html.

Waters, C. (2019) "'Throwing workers a bone': Deliveroo calls for national laws to govern gig economy", February 12, available at https://www.smh.com.au/business/small-business/throwing-workers-a-bone-deliveroo-calls-for-national-laws-to-govern-gig-economy-20190212-p50x72.html.

Waterson, J. (2018.) "UK fines Facebook £500,000 for failing to protect user data", *The Guardian*, October 25, available at https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica.

Witzleb N. (2020) "Data privacy: Stricter European rules will have repercussions in Australia as global divisions grow,' *The Conversation* 31, July, available at https://theconversation.com/data-privacy-stricter-european-rules-will-have-repercussions-in-australia-as-global-divisions-grow-142980.