Algorithms Off-Limits?

If Digital Trade Law Restricts Access to Source Code of Software then Accountability will Suffer

Irion, K.

DOI
10.1145/3531146.3533212

Publication date
2022

Document Version
Final published version

Published in
Proceedings of 2022 5th ACM Conference on Fairness, Accountability, and Transparency (FAccT 2022)

Algorithms Off-limits?

If digital trade law restricts access to source code of software then accountability will suffer

Kristina Irion
Institute for Information Law, University of Amsterdam
k.irion@uva.nl

ABSTRACT

Free trade agreements are increasingly used to construct an additional layer of protection for source code of software. This comes in the shape of a new prohibition for governments to require access to, or transfer of, source code of software, subject to certain exceptions. A clause on software source code is also part and parcel of an ambitious set of new rules on trade-related aspects of electronic commerce currently negotiated by 86 members of the World Trade Organization. Our understanding to date of how such a commitment inside trade law impacts on governments right to regulate digital technologies and the policy space that is allowed under trade law is limited. Access to software source code is for example necessary to meet regulatory and judicial needs in order to ensure that digital technologies are in conformity with individuals' human rights and societal values. This article will unpack and analyze the implications of such a source code clause for current and future digital policies by governments that aim to ensure transparency, fairness and accountability of computer and machine learning algorithms.

CCS CONCEPTS

• **Social and professional topics**; • **Computing / technology policy**; • **Government technology policy**; • **Governmental regulations**;

KEYWORDS

Software, Source code, Computer algorithms, Application Programming Interface, International trade law, Digital policy, Transparency, Fairness, Accountability

ACM Reference Format:
Kristina Irion. 2022. Algorithms Off-limits?: If digital trade law restricts access to source code of software then accountability will suffer. In *2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22), June 21–24, 2022, Seoul, Republic of Korea.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3531146.3533212

1 INTRODUCTION

International trade law is made up of a vast network of bilateral and multilateral agreements that govern trade relationships between contracting states. It forms a subset of international public law that creates binding and enforceable commitments between contracting states. Reflecting the growing significance of crossborder digital trade, a new generation of free trade agreements (FTAs) defines new rules in specific chapters on digital trade (or electronic commerce). The digital trade space has evolved into an important 'laboratory' for developing novel international rules that set the conditions for the crossborder supply of digital services and, more broadly, holds guarantees for the conduct of transnational digital business.

FTAs are increasingly used to construct an additional layer of protection for source code of software. This comes in the shape of a new provision which prohibits governments to require access to, or transfer of, the source code of software owned by a (natural or legal) person of the other party. Such a provision is for instance included in the 2018 Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) [9] which is a mega-regional trade agreement between eleven countries of the pacific rim. It features in the 2018 United States-Mexico-Canada Agreement (USMCA) [39] and the 2019 US-Japan Digital Trade Agreement [2]. Also the European Union (EU) inscribed provisions on software source code in its recent bilateral trade agreements with Japan [14], Mexico [15] and the United Kingdom [37]. In substance, these provisions converge around the principle to protect software source code against government mandated access. Each commitment carves out a distinct policy space for governments of contracting states that conditions domestic regulatory measures that require access to software source code.

Meanwhile, 86 World Trade Organization (WTO) members are negotiating an ambitious set of new rules on trade-related aspects of electronic commerce [44, 45]. These negotiations aim for a plurilateral trade agreement that–once ratified by a majority of WTO member states–would represent most of the world's digital trade. The negotiations which take place behind closed doors have been criticized by civil society for a lack of transparency and democratic deliberation [22, 23]. Some parties to this negotiations keep their proposals classified, however, a first consolidated draft of the agreement was prematurely leaked [46]. Known is that Canada, the EU, Japan, South Korea, Singapore, Ukraine, and the United States (US) back a prohibition on government mandated access to source code of software, China opposes it and also developing countries mount opposition [38]. Uploading the protection of software source code in a plurilateral agreement at the level of the WTO would have repercussions for a range of public interest regulations [21]. Pundits and digital rights advocates are worried that this could hamper efforts to hold developers and providers of transnational algorithmic systems accountable [25, 31].

This article aims to unpack the implications of a software source code clause inside digital trade law for current and future digital policies by governments that aim to ensure transparency, fairness and accountability of computer and machine learning algorithms.

FAccT '22, June 21–24, 2022, Seoul, Republic of Korea

ACM ISBN 978-1-4503-9352-2/22/06.
https://doi.org/10.1145/3531146.3533212

After a primer on the digital trade law clause and how it can condition domestic regulation requiring access to source code, the analysis will develop three critiques: Firstly, the ability to adopt a measure to meet regulatory needs, such as requiring independent audits of algorithmic systems. Secondly, the ability to mandate access to technical interfaces in order to observe the workings of an algorithmic system and to carry out input-outputs-audits. Thirdly, the relationship with existing international regimes on copyright and trade secrets that already protect software will be discussed.

Aside from a handful of studies [18, 21, 22, 25, 31, 38], there is hardly any literature on the interface between trade law protection of software source code and regulatory governance of digital technologies, let alone with a focus on computer and machine learning algorithms. The main thrust of this literature is to convey an overview of public interest regulations that require access to software source code [12, 21, 31] and to provide reasons why algorithmic transparency is important [12, 21, 25]. Analyses informed by international trade law scholarship [12, 21] which is short in supply will be related to multidisciplinary literature on algorithmic transparency [3, 24], ethics of algorithms [4, 26], algorithmic accountability [11, 22] and auditing of algorithms [6, 32, 34].

The methodology used in this article is qualitative research and doctrinal legal research. The article's empirical basis is the body of digital trade law, academic literature, official and stakeholder documents. The article strives to convey legal knowledge in a way that is accessible for a multidisciplinary audience and provides examples where appropriate. The article's findings will be of particular relevance for researchers and practitioners interested in fairness, accountability, and transparency of algorithmic systems and digital trade law.

The article will start with explaining how international trade law is increasingly used to prohibit governments' policies to require access to source code and what exceptions from that rule are recognized. Next, three implications this can have for the transparency, fairness and accountability of algorithmic systems will be analyzed in more detail. The conclusions sum up that protecting software source code through digital trade law is oftentimes at cross with emergent best practices underpinning algorithmic accountability, excessive in light of existing legal regimes that already protect software and highly problematic with a view to constructing just algorithmic societies.

2 THE PROTECTION OF SOFTWARE SOURCE CODE IN DIGITAL TRADE LAW

International trade law has evolved into a potent form of transnational rulemaking. What set out as a vehicle to remove import tariffs and trade restrictions at the border has acquired direct influence on states' domestic regulation. Contemporary FTAs seek deeper integration of domestic regulation across a wide range of public policy issues [33]. Reflecting the rising importance of digital trade, a new generation of bilateral and multilateral FTAs have embarked on facilitating crossborder electronic commerce, or rather digital trade. Currently, about 188 of the 353 FTAs concluded between the years 2000 and 2020 contain provisions relevant to crossborder digital trade [8].

Source code of software has more recently moved into the focus of trade negotiators and its protection was inscribed in a number of important mega-regional and bilateral FTAs. A new commitment is part of the ongoing negotiations for a prospective plurilateral agreement on trade-related aspects of electronic commerce at the level of the WTO [44, 45]. However, protecting source code of software owned by a natural or legal person against government mandated access or transfer implicates, as will be shown, algorithmic governance.

The second section will revisit the rational for introducing a software source code clause, provide examples of its inclusion in specific FTAs, interpret the notion 'software source code' and demonstrate how the layered exceptions play out.

2.1 Rational for new source code protection in FTAs

The stated reason why international trade diplomacy cares about source code of software has to do with a practice known as forced technology transfer. It harks back to disputes between technology exporting countries, e.g. EU member states and the US, among others, and yet other countries, such as China [36], among others, that make market access and foreign direct investment conditional upon disclosing commercially valuable information:

> "Concerns have been raised about the use of registration, certification and approval procedures by government bodies to request, formally or informally, sensitive proprietary information which does not appear to be necessary, or indeed requirements to disclose source code." [5]

Such a measure can in particular interfere with business secrets of the foreign company which are often central to business models in high-technology sectors. In that vein forcing a foreign company to divulge propriety source code of software to a government entity or local business partner is considered extortionate.

That is not to say that all technology transfers are necessarily bad. Especially intellectual property law, e.g. patent and copyright law, seeks to strike a balance between the protection of innovation and its release as a public good after the term of protection has expired. There is another important caveat to be made about technology transfers being used to enable developing countries' economic development and to narrow the digital trade imbalance which is further explored elsewhere [31, 38].

The intuitive link between the risk of forced technology transfer and the inclusion of the source code clause is not always evident. For instance, neither the EU and its member states nor Japan, the UK or the US are implicated to use practices that force technology transfers. Nevertheless, the EU and these states incorporate this particular clause in their bilateral FTAs. To these states and the EU the template on software source code is considered best practice ('gold standard') and its proliferation serves to build clout for future negotiations with yet other trading partners.

International trade law thus comes in as an additional layer of protection for software source code that is commonly justified as countering a country's practices that would amount to forced technology transfer. Yet, inscribing the protection of source code of

software in FTAs can have unintended consequences for perfectly legitimate public interest objectives:

> "On the one hand, it encourages international trade by reassuring foreign software developers that they will not have to disclose the source code underlying their products and services. On the other hand, this general prohibition, even when accompanied by extensive exemptions, places limitations on the powers of governments and their agencies to examine source code." [12]

This can render a FTA's commitment that protects software source code against government access and transfer a double-edged sword that can be used to contest a country's measure in pursuit of algorithmic transparency, fairness and accountability, as will be argued below.

2.2 Digital trade rules on source code of software

New clauses on source code of software have come to proliferate in dedicated digital trade chapters of FTAs, however, not across the board. Several countries, notably the Australia, Canada, the EU, Japan, South Korea and the US, actively pursue the inclusion in their FTAs of a prohibition on government mandated access to source code of software. 2018 marks the inception of FTAs that contain a binding commitment on software source code [9, 14, 15, 39]. The actual text of the source code clauses covered in this section are reproduced in the Appendix.

Mega-regional FTAs are set apart from bilateral FTAs by their regional scope of application covering several signatory states. The 2018 CPTPP [9] is a case in point which is a regional trade agreement between eleven countries of the pacific rim, i.e. Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam. The CPTPP incorporates by reference the original 2016 Trans-Pacific Partnership (TPP) that had been negotiated with the involvement of the US but was later abandoned by the incoming Trump administration. The CPTPP Chapter on Electronic Commerce, prohibits a party to this agreement to require the transfer of, or access to, "source code of mass-market software or products containing such software" as a condition for the import, distribution, sale or use of such software in its territory. Excluded from the scope is "software used for critical infrastructure". The prohibition does not preclude "requiring the modification of source code of software necessary for that software to comply with laws or regulations", however, without requiring access to it [12].

Likewise the USMCA [39] that was concluded in 2018 between the US, Mexico and Canada, features a clause on source code in its Chapter on Digital Trade that is even more ambitious. Hereafter "no Party shall require the transfer of, or access to, a source code of software owned by a person of another Party" to this agreement. In addition, "an algorithm expressed in that source code" is explicitly covered. Algorithm is defined as meaning "a defined sequence of steps, taken to solve a problem or obtain a result." The USMCA clause does "not preclude a regulatory body or judicial authority of a Party from requiring" access to the source code of software, including an algorithm, for a specific regulatory investigation or judicial proceeding, "subject to safeguards against unauthorized disclosure".

The Regional Comprehensive Economic Partnership (RCEP) Agreement [30] concluded among fifteen Asia-Pacific nations in 2020, by contrast, does not contain a source code clause in its Chapter on Electronic Commerce. Neither does the Digital Economy Partnership Agreement (DEPA) signed in 2020 between Singapore, Chile and New Zealand considered to be one of the most innovative multilateral FTAs. The state of play in the ongoing negotiations at the WTO concerning source code is unclear but compared to other aspects where a consolidated draft has been provisionally agreed the issue of source code appears still controversial [45, 46].

From the plethora of bilateral FTAs it will suffice to highlight a few examples. The 2020 Digital Trade Agreement between the US and Japan [2] for instance reproduces by and large the source code clause of the USMCA.

How the EU protects software source code in its bilateral FTAs with Japan, Mexico and the UK is interesting to trace. The EU-Japan Agreement on Economic Partnership [14] and the EU-Mexico Agreement in principle [15] have seen the introduction in EU external trade policy of a novel clause on source code of software. More recently the EU-UK Trade and Cooperation Agreement (EU-UK TCA) [37] inscribes protection of source code of software in its Chapter on Digital Trade. The general prohibition that "a Party may not require the transfer of, or access to, source code of software owned by a person of the other Party" [14, 15, 37] resembles the FTAs mentioned earlier. As compared to the earlier FTAs of the EU with Japan [14] and Mexico [15], the custom-made exceptions in the EU-UK TCA [37] are more layered and also contain new elements. There will be more to say about the evolving language to carve out exceptions to the prohibition at a later stage.

While it is easy to loose orientation in this thicket of FTA provisions it will be important for the remainder of this article to recall that requiring access to source code of software by governments is increasingly governed by FTAs. While the exact language varies between FTAs there is a common core framing a general prohibition, subject to certain custom-made exceptions. The bilateral FTAs with the EU [14, 15, 37] do not mention 'algorithms expressed in source code' anywhere in contrast to US-led FTAs [2, 39]. Whether this is significant as regards the application of the general prohibition on government mandated access to algorithmic code will crucially depend on the interpretation of 'source code of software' which will be discussed next.

2.3 Defining source code of software

For determining the scope and impact of a digital trade law provision on source code of software the exact meaning of 'source code of software' is decisive. This term is not defined in any of the aforementioned FTAs. In this case the rules of treaty interpretation set out in the Vienna Convention [41] would guide the interpretation by the parties to an agreement and ultimately the relevant dispute resolution bodies. It provides that a treaty shall be interpreted "in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose." [41]

In the field of computing 'source code' means "a program in a source language." [28] In order to be executed by a computer the source code has to be converted first into machine-readable object code. Conventional source languages are text-based and human-readable. Source languages are not static but dynamically connected to the state-of-the-art of programming implying that older source languages become less relevant meanwhile newer source languages are adopted [42]. The ordinary meaning of source code is potentially very broad covering inter alia any kind of computer program, software system and even the software architecture of entire online platforms expressed in a source language [21].

Whether the term 'source code of software' can also be interpreted as covering computer and machine learning algorithms will be established next.

> "Coding [. . .] consists of two key translation challenges centered on producing algorithms. The first is translating a task or problem into a structured formula with an appropriate rule set (pseudo-code). The second is translating this pseudo-code into source code that when compiled will perform the task or solve the problem." [24]

The answer is straight forward when it comes to 'hand-coded' computer algorithms where human software engineers program the decision-making rules in a source language. What would not be covered by the term 'source code' is the more conceptual version of the algorithm before it is turned into a source language.

Machine learning algorithms by contrast are increasingly not 'hand-coded' and may no longer use a text-based source language. Predictive models can for example generate source code automatically or they are expressed in graphical languages as opposed to text-based. As [21] stipulates:

> "That does not appear to disqualify visual programming languages and machine-generated code from the ordinary meaning of source code since they are listed as latest developments in programming languages."

It follows that the ordinary meaning of 'source code' does not have a clear demarcation that would categorically exclude computer algorithms expressed in source code, be they hand-coded or automatically generated. That certain FTAs [2, 39] explicitly mention 'algorithms expressed in source code' does help to clarify but may ultimately not be decisive for concluding that computer algorithms expressed in source code are covered anyway. In practice, the 'source code' of computer algorithms is licensed [35], required for reproducibility [20] and also used in official documents on algorithmic governance.

Another, often overlooked aspect of protecting source code inside digital trade law is that Application Programming Interfaces (APIs) are also expressed in source code. APIs provide the gateways through which the algorithm receives its inputs and queries as well as produces some sort of output [34]. This matters because API access may turn out to be crucial to carry out non-invasive introspection that does not require access to an algorithm's source code as such.

2.4 Exceptions permitting access to source code of software

As initially explained each provision prohibiting access to source code of software comes with different exceptions attached. As a first line of defense, the custom-made exceptions that are inscribed in the same clause serve to counterbalance the general prohibition. A second line of defense is the possibility to justify a trade law violation pursuant to the general exceptions for general interest measures and the security exceptions that are standard for FTAs. As a result parties to a FTA are bound by a rule prohibiting government-mandated access to source code of software, unless one of the custom-made exceptions to this rule applies or the violation of the rule can be justified.

A comparison of the custom-made exceptions to the prohibition of government mandated access to source code of software reveals:

> "a shared recognition that source code disclosure may be required to ensure compliance and enforcement of laws, but differences when it comes to the particular legal or public interests explicitly recognised by individual agreements." [12]

A recurring exception has been inscribed for a requirement by a court, administrative tribunal, or a competition authority in order to meet regulatory and judicial needs. The EU-UK TCA specifies that the prohibition does not prevent "a requirement by a court or administrative tribunal, or . . . by a competition authority" [37]. Another inroad inscribed as an exception is "a requirement by a regulatory body pursuant to a Party's laws or regulations related to the protection of public safety with regard to users online" [37]. The US-led FTAs [2, 39] are more stringent in that source code must be required for "a specific investigation, inspection, examination, enforcement action, or judicial proceeding". In spite of the different formulations used this type of custom-made exception is limited to judicial and regulatory powers that are applied on a case-by-case basis in the context of ex post regulatory enforcement or judicial remedies. It implies a recognition of qualified transparency which would authorize regulatory authorities and domestic courts to request access to source code of software for investigations that would selectively override business secrets of developers and providers.

The thrust of this source code clause are general laws that require transfer of, or access to software source code that can't be already excepted under the first line of defense. Legislation that mandates conformity assessments, certification schemes or standardized APIs would be inconsistent with the protection of software source code inside trade law. Besides, the custom-made exceptions exclusively qualify government bodies to make a requirement for software source code, however, subject to requiring safeguards against unauthorized disclosure. In addition to diverting from the important role of independent private expertise for algorithmic accountability, legislation that would enable public scrutiny by academics, media, critical engineers and civil actors would not be recognized under such a trade law clause.

Following the second line of defense, two different exceptions on grounds of security interests and general interests are typically inscribed in FTAs that can be invoked to justify an inconsistent measure. As a rule of thumb, invoking the exceptions on grounds

of a party's security interests is less demanding as compared to the more rigorous legal test required to meet the general exceptions. One can imagine the margin of discretion to adopt measures in pursuit of a general interest objective as the hole in a doughnut that is "left open by a surrounding belt of restrictions" [13]. The burden of proof is placed on the party that seeks to justify an inconsistent measure in pursuit of a general interest objective. The contemporary lack of international standards and consensus on algorithmic governance increases a party's legal risk that an attempt to justify an inconsistent measure on ground of the general exceptions does not succeed.

Whenever this new clause is inscribed in a FTA government-mandated access to source code of software becomes subject matter of international trade law, even if this measure does not afford discriminatory treatment or impedes market access. The margin of discretion a government retains to adopt measures that require access to source code of software is confined to the policy space that is allowed by the FTA. New tensions are bound to arise between domestic regulation and a FTA's source code protection:

> "The source code clause is too broad for domestic digital policies that need to build on interoperability, accountability, and verifiability of digital technologies." [21]

Turning to algorithmic governance, the source code clause stands in the way of a legal requirement that mandates independent audits or access to standardized technical interfaces in the interest of auditability, scientific research and public scrutiny. A FTA's source code clause has thus real implications for the domestic policy space at a moment that concepts of and approaches to algorithmic governance are still evolving.

3 CRITIQUES OF DIGITAL TRADE LAW PROTECTION OF SOURCE CODE

It is the opacity of how a machine learns and makes predictions that has captured our imagination [7]. Frequently, algorithmic systems are referred to as "black boxes" to coin the inscrutability of its decision-making. Yet, an algorithmic system should not be perceived "as a technical, objective, impartial form of knowledge or mode of operation" [24] but as a socio-technical assemblage that combines and enacts human and non-human judgments [3, 4, 24, 26]. The resources, purpose, the choice and quality of training data, expertise and judgement, internal and external constraints have a significant influence on the technology.

> "The non-technical properties of these systems – for example, their purpose and constraining policies – are just as important, and often more important than their technical particulars." [24]

The epistemic and normative issues raised by algorithmic systems are challenging for their transparency, fairness, interpretability and accountability [26]. Algorithmic governance is the umbrella term for different kinds of initiatives that ought to keep the black-box in check. Algorithmic transparency refers to a spectrum of different types, audiences and mechanisms; these in turn reflect the current state of knowledge about transparency motivated policy interventions. It is moreover understood that transparency is not a magic wand that can produce accountability of algorithmic agents and their developers by itself [3, 24]. Focusing transparency exclusively on certain technical components of an AI system, such as the algorithm, is not the same as holding all its technological and social aspects accountable [3].

There is a surge of noteworthy initiatives on responsible, ethical and human-centric algorithms by researchers, civil society, policy makers and developers. International standard-setting is in full swing. The 2019 OECD Recommendation on Artificial Intelligence calls for responsible and trust-worthy artificial intelligence, therein promoting transparency, explainability and accountability of AI systems [27]. The Council of Europe is preparing the first binding convention on artificial intelligence [1]. A legislative proposal for an EU Artificial Intelligence Act is currently underway [16].

The third section will develop three critiques of digital trade law protection of source code of software. First, the ability to scrutinize computer algorithms to meet regulatory needs and to generate external accountability will be questioned. Next, the ability to mandate access to APIs in order to carry out input-outputs-audits is discussed. Finally, the relationship with existing international regimes that protect software and open source licenses will be briefly discussed.

3.1 Requiring access to source code of computer algorithms

Public policy and regulation has an important role to play in providing incentives for rigorous impact assessments and testing before introducing a new algorithmic system that can affect individuals and society. Supervision and enforcement of compliance with domestic regulations and individuals' rights continue to play an important role after an algorithmic system has been deployed. Besides, developers and providers have to resume accountability for the predictive outcomes of algorithmic decision-making systems they implement as well as legal responsibility for its lawful operations. Governance of algorithmic systems requires mechanisms that can hold developers and providers accountable with algorithmic audits being the most aspirational solution [40]. While not all auditing types require access to source code, a government can adopt regulation that mandates code audits, especially in high stakes deployments and in order to mitigate individual or collective harm.

Auditing an algorithmic system that involves an analysis of its source code requires resources, specialized knowledge and access to proprietary information. This method can be fruitful in a highly targeted investigation to identify the source of an existing concrete problem. This type of code review has for example successfully been used by US academics to identify the offending section of code in the US investigation of the Volkswagen Diesel nitrogen oxide emission cheating scandal [19]. The proposal for an EU Artificial Intelligence Act [16] proposes to introduce conformity assessments before 'high risk' artificial intelligence can be placed on the Union market. Under the proposal, designated bodies would be tasked with conformity assessments which will primarily be based on reviewing documentation but can also involve a review of the source code. As a regulatory design the risk based approach to mandating conformity assessments is better attuned to meet the general exceptions in FTAs; however, a broader regulation may not fit the

margin of discretion left to the government. Also other public interest regulations will have to cope with the increasing adoption of algorithmic agents that can require updating regulation to mandate independent audits. This covers the entire spectrum of regulatory regimes ranging from consumer protection law to antidiscrimination law, product liability, unfair commercial practices laws, medical regulations and many more.

3.2 Application programming interfaces as source code

Access to the technical interfaces of the algorithmic system can be a means to carry out non-invasive introspection that does not require access to an algorithm's source code as such. In order to carry out more sophisticated testing experts must gain access to input and output data as well as to the respective technical interfaces. However, in many situations developers and providers treat APIs just as proprietary as the algorithms behind them. Moreover the trade law protection vested on source code of software does shield APIs from government mandated access too.

Proposals on algorithmic accountability underscore the role of APIs for auditing algorithms, setting up accountability APIs or observe the algorithmic system in a sandbox setting [10, 21, 32]. It is not a coincidence that the potential of requiring access to interfaces of algorithmic systems for accountability purposes is discussed across several domains, such as competition law, antidiscrimination law, online platform regulation and broadly algorithmic governance. Public-facing or internal APIs can be of strategic importance for ensuring the accountability and trustworthiness of algorithmic decision-making systems.

> Committing to a trade law clause that would make it harder to engage with AI systems via these interfaces or mandate standardized interfaces in the interest of auditability is counterproductive. [21]

While algorithmic governance would benefit from "regulation towards auditability" [34] digital trade law by contrast curtails regulation requiring non-invasive access to the technical interfaces of algorithmic systems. Consider in this context the EU proposal for a Digital Services Act (DSA) which, if adopted, introduces access to data of very large online platforms for vetted researchers either through online databases or APIs [17]. What could become an important precedent for researchers' access to an API in order to scrutinize an algorithmic recommender system would be deemed inconsistent with the source code clause. Whether the general exceptions for measures on grounds of general interests can be invoked in justification of researchers' access via an API is by no means certain.

3.3 Relationship with intellectual property and trade secret protections

The protection of source code is a strange guest in digital trade chapters of FTAs. After all, source code of software can be copyright protected and may qualify as a trade secret. For reasons of consistency source code protection would be more appropriately dealt with inside the WTO Intellectual Property (TRIPS) Agreement [43]. Following TRIPS Article 10.1, computer programs, whether in source or object code, qualify for copyright protection. Parties to TRIPS had to align their national laws in order to afford copyrights protection of computer programs in their domestic laws and via its dispute resolution procedures the TRIPS is enforceable.

Next to qualifying for copyright protection, source code can also be protected as a trade secret under the TRIPS agreement. An explanatory footnote in the USMCA [39] for that matter clarifies that "software source code's status as a trade secret" shall not be negatively affected "if such status is claimed by the trade secret owner." The explanatory footnote aims to ensure that source code of software continues to be treated as a trade secret in the case of disclosure in the context of a regulatory investigation, enforcement action or judicial proceeding, requiring safeguards against unauthorized disclosure.

Last but not least, digital trade law is not cognizant of open source licenses even though they are widely used in practice to share source code and computer algorithms [29]. The clause on source code of software prohibits government mandated access of source code of software; thereby overriding what has been open source by origin. The upshot is that the source code clause in FTAs creates an additional *sui generis* right that, next to copyright protection and trade secret law governments ought to respect, shields software source code from being interfered with by governments.

4 CONCLUSIONS

This article traces new international rulemaking that inscribes a new layer of protection for source code of software in FTAs. The provision is addressed to governments who commit to refrain from requiring the transfer of, or access to, source code of software owned by a natural or legal person of the other party. The commitment has already entered several important multilateral and bilateral FTAs and is actively supported by, for example, Australia, the EU, Canada, Japan, and the US. The exceptions are highly specific to a particular FTA and range from more open to fairly closed regimes as regards to government mandated access to source code. At WTO level efforts are underway to upload a similar provision into a plurilateral agreement on trade-related aspects of electronic commerce.

This article argues that the clause on software source code is a double-edged sword that can conflict with the regulatory governance of digital technologies and in particular with algorithmic accountability. In spite of exceptions tailored to ensure that certain regulatory and judicial needs can be met, the trade law clause nevertheless curtails a government's margin of discretion to adopt measures in pursuit of general interest objectives. Absent a legal definition of 'source code of software' an interpretation of the ordinary meaning of the term concludes that computer and machine learning algorithms when they are expressed in source code fall inside the scope of such a trade law clause. Moreover, also the technical interfaces through which a computer algorithm receives inputs and produces outputs are expressed in source code and thus covered by the new trade law clause. Contrary to the balance struck by FTAs, mandating access to these APIs holds great potential for the observability of algorithmic decision-making and would thus benefit from "regulation towards auditability" [6, 21, 32, 34].

Considering that digitalization is leading to ever more digital artefacts made of software the endeavors to inject yet another layer

of protection for software into digital trade law is highly problematic. The source code clause may already turn out too restrictive for domestic digital policies that need to build on interoperability, accountability, and verifiability of digital technologies [21]. That a government would violate a trade law commitment when it adopts a law in the interest of the auditability is difficult to reconcile with efforts to institute algorithmic governance. Policy-makers and trade negotiators would be well advised to reduce inconsistencies and overlaps with existing legal protections of software as well as to solicit expertise and engage with best practices of algorithmic auditing and accountability before codifying a new clause to protect source code of software inside trade law.

ACKNOWLEDGMENTS

The article benefited from a subgrant (5.000 USD) from Digital Trade Alliance managed by Public Citizen, Washington (US). This article draws from an independent study [13] that the author carried out on request of the German Federation of Consumer Protection Organizations.

REFERENCES

[1] Ad hoc Committee on Artificial Intelligence (CAHAI). 2022. Possible elements of a legal framework on artificial intelligence, based on the Council of Europe's standards on human rights, democracy and the rule of law. Council of Europe Committee of Ministers. CM(2021)173-add. Retrieved January 19, 2022 https://rm.coe.int/possible-elements-of-a-legal-framework-on-artificial-intelligence/1680a5ae6b

[2] Agreement between the United States of America and Japan concerning Digital Trade, signed October 2019. Retrieved January 19, 2022 from https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf

[3] Mike Ananny and Kate Crawford. 2018. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. New Media & Society. 20(3):973-989. doi:10.1177/1461444816676645

[4] Mike Ananny. 2016. Toward an Ethics of Algorithms: Convening, Observation, Probability, and Timeliness. Science Technology and Human Values. 41(1):93-117. doi:10.1177/0162243915606523

[5] Andrea Andrenelli, Julien Gourdon and Evdokia Moïsé. 2019. International Technology Transfer Policies. 222 OECD Trade Policy Papers 4. Retrieved January 19, 2022 https://www.oecd-ilibrary.org/deliver/7103eabf-en.pdf?itemId=%2Fcontent%2Fpaper%2F7103eabf-en&mimeType=pdf

[6] Balasz Bodo, *et al.* 2017. Tackling the Algorithmic Control Crisis – the Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents, The Yale Journal of Law & Technology, 19(1), pp. 133–180. Retrieved January 19, 2022 http://hdl.handle.net/20.500.13051/7813

[7] Jenna Burrell. 2016. How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms. Big Data and Society. 3(1). (January 2016). https://doi.org/10.1177/2053951715622512

[8] Mira Burri and Rodrigo Polanco. 2020. Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset. Journal of International Economic Law, 23(1). (March 2020). pp. 187–220. https://doi.org/10.1093/jiel/jgz044

[9] Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) between Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam, March 2018. Retrieved January 19, 2022 from http://www.dfat.gov.au/sites/default/files/tpp-11-treaty-text.pdf

[10] Data Ethics Commission. 2019. Opinion of the Data Ethics Commission. Berlin. December 2019. Retrieved January 19, 2022 https://datenethikkommission.de/wp-content/uploads/DEK_Gutachten_engl_bf_200121.pdf

[11] Nicholas Diakopoulos, 2016. Accountability in Algorithmic Decision Making. Communications of the ACM, Vol. 59 No. 2. (February 2016), pp. 56-62. doi: 10.1145/2844110 62

[12] Cosmina Dorobantu, Florian Ostmann and Christina Hitrova1. 2021. Source code disclosure : A primer for trade negotiators, in Borcher, I. and Winters, L. A. (eds) Addressing Impediments to Digital Trade. London: CEPR Press. doi: 978-1-912179-42-8

[13] Ronald Dworkin. 1978. Taking Rights Seriously. Harvard University Press.

[14] EU-Japan Economic Partnership Agreement (EPA), signed July 2018 and into force since February 2019. Retrieved January 19, 2022 from http://trade.ec.europa.eu/doclib/press/index.cfm?id=1684

[15] EU-Mexico Agreement in principle, announced on 21 April 2018 (pending ratification). Retrieved January 19, 2022 from http://trade.ec.europa.eu/doclib/html/156811.htm

[16] European Commission. 2021. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM/2021/206 final. Retrieved January 19, 2022 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[17] European Commission. 2021. Proposal for a Regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. COM(2020) 825. Retrieved January 19, 2022 https://ec.europa.eu/info/sites/default/files/proposal_for_a_regulation_on_a_single_market_for_digital_services.pdf

[18] Michèle Finck. 2020. Legal analysis of international trade law and digital trade (PE 603.517), briefing requested by the INTA Committee. Brussels. Retrieved January 19, 2022 https://op.europa.eu/en/publication-detail/-/publication/18173e33-2954-11eb-9d7e-01aa75ed71a1/language-en/format-PDF/source-172804686

[19] Megan Geuss, 2017. A Year of Digging through Code Yields "Smoking Gun" on VW, Fiat Diesel Cheats. Ars Technica. 28 May 2017. Retrieved January 19, 2022 https://arstechnica.com/cars/2017/05/volkswagen-bosch-fiat-diesel-emissions-cheats-cracked-open-in-new-research/

[20] Benjamin Haibe-Kains, George Alexandru Adam, Ahmed Hosny, *et al.* 2020. Transparency and reproducibility in artificial intelligence. Nature 586, E14–E16. (October 2020). https://doi.org/10.1038/s41586-020-2766-y

[21] Kristina Irion. 2021. AI Regulation in the European Union and Trade Law: How Can Accountability of AI and a High Level of Consumer Protection Prevail over a Trade Discipline on Source Code?, Study commission by the German Federation of Consumer Protection Organizations (vzbv). Amsterdam. Institute for Information Law. doi: 10.2139/ssrn.3786567

[22] Deborah James. 2020. Digital Trade Rules: a Disastrous New Constitution for the Global Economy, by and for Big Tech. Rosa Luxemburg Foundation. Brussels. Retrieved January 19, 2022 https://cepr.net/wp-content/uploads/2020/07/digital-trade-2020-07.pdf

[23] Burcu Kilic and Renata Avila. 2020. Opening Spaces for Digital Rights Activism: Multilateral Trade Negotiations. Philadelphia. Retrieved January 19, 2022 https://www.citizen.org/wp-content/uploads/Trade-Report_IPO-1.pdf

[24] Rob Kitchin. 2017. Thinking critically about and researching algorithms, Information, Communication & Society, 20:1, 14-29. doi: 10.1080/1369118X.2016.1154087

[25] Ansgar Koene. 2018. Some Implications of WTO Ecommerce Proposals Restricting Access to Algorithms on Algorithmic Transparency. Paper Presented at the WTO Public Forum, 2-4 October 2018. Retrieved January 19, 2022 https://ourworldisnotforsale.net/2018/Koene_algorithms.pdf

[26] Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter, and Luciano Floridi. 2016. The Ethics of Algorithms: Mapping the Debate. Big Data & Society, (December 2016). doi: 10.1177/2053951716679679

[27] OECD. 2019. Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). Adopted by the OECD Council on 22 May 2019. Retrieved January 19, 2022 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[28] Oxford English Dictionary. "source code". Retrieved January 19, 2022 https://www.oed.com/view/Entry/185182?redirectedFrom=%22source+code%22#eid21845861

[29] Shin-yi Peng, Ching-Fu Lin, and Thomas Streinz. 2021. Artificial Intelligence and International Economic Law: A Research and Policy Agenda. Chapter. In Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration, edited by Shin-yi Peng, Ching-Fu Lin, and Thomas Streinz, 1–26. Cambridge: Cambridge University Press, 2021. doi:10.1017/9781108954006.002

[30] Regional Comprehensive Economic Partnership (RCEP) Agreement between Australia, Brunei, Cambodia, China, Indonesia, Japan, South Korea, Laos, Malaysia, Myanmar, New Zealand, the Philippines, Singapore, Thailand, and Vietnam, signed in November 2020 and entered into force in January 2022. Retrieved January 19, 2022 https://rcepsec.org/legal-text/

[31] Sanya Reid Smith. 2017. Preliminary analysis of aspects of some WTO ecommerce proposals – MC11 briefing paper. Third World Network, 10 December 2017. Retrieved January 19, 2022 https://ourworldisnotforsale.net/2017/TWN_E-commerce.pdf

[32] Bernhard Rieder and Jeanette Hofmann. 2020. Towards platform observability. Internet Policy Review, 9(4). (December 2020). doi: 10.14763/2020.4.1535

[33] Dennis Rodrik. 2020. What do trade agreements really do?. Journal of Economic Perspectives, 32(2), pp. 73–90. doi: 10.1257/jep.32.2.73

[34] Christian Sandvig *et al.* 2014. Auditing Algorithms, in ICA 2014 Data and Discrimination Preconference. ICA, pp. 1–23. doi: 10.1109/DEXA.2009.55

[35] Kevin Scott. 2020. Microsoft teams up with OpenAI to exclusively license GPT-3 language model. Official Microsoft Blog, September 22, 2020. Retrieved January 19, 2022 https://blogs.microsoft.com/blog/2020/09/22/microsoft-teams-up-with-openai-to-exclusively-license-gpt-3-language-model/

[36] Alan O. Sykes. 2021. The Law and Economics of "Forced" Technology Transfer and Its Implications for Trade and Investment Policy (and the U.S.–China Trade

War). Journal of Legal Analysis. 13(1). (March 2021). pp. 127–171. https://doi.org/10.1093/jla/laaa007

[37] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part (TCA), signed on 30 December 2020, applied provisionally as of 1 January 2021 and entered into force on 1 May 2021. ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj

[38] UNCTAD. 2021. What is at Stake for Developing Countries in Trade Negotiations on E-commerce? The Case of the Joint Statement Initiative. New York. United Nations. doi: 10.18356/9789210056366

[39] United States-Mexico-Canada Agreement (USMCA), November 2018. Retrieved January 19, 2022 from https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

[40] Briana Vecchione, Karen Levy, and Solon Barocas. 2021. Algorithmic Auditing and Social Justice: Lessons from the History of Audit Studies. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3465416.3483294

[41] Vienna Convention on the law of treaties (with annex), concluded on 23 May 1969. Retrieved January 19, 2022 https://treaties.un.org/doc/publication/unts/volume%201155/volume-1155-i-18232-english.pdf

[42] Wikipedia. "history of source code". Retrieved January 19, 2022 https://en.wikipedia.org/wiki/History_of_programming_languages

[43] WTO. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Annex 1C to the Agreement establishing the World Trade Organization, signed in Marrakesh. Morocco on 15 April 1994. Retrieved January 19, 2022 https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm

[44] WTO, Joint Statement on Electronic Commerce (WT/L/1056), Geneva, 25 January 2019. Retrieved January 19, 2022 from https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/251086/q/WT/L/1056.pdf

[45] WTO, Joint Statement Initiative on E-commerce: Statement by Ministers of Australia, Japan and Singapore, Geneva, 1 December 2021. Retrieved January 19, 2022 from https://www.wto.org/english/news_e/news21_e/ji_ecom_minister_statement_e.pdf

[46] WTO plurilateral ecommerce draft consolidated text. Unofficial leaked document. August 2020. Retrieved January 19, 2022 https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text.pdf

APPENDIX

Table 1: Software source code commitments inside FTAs

FTA	Parties	General prohibition	Exceptions
Article 14.17 CPTPP [1]	Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam	**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 19.16 USMCA [2]	US, Mexico, Canada	**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,[a] subject to safeguards against unauthorized disclosure.
Article 17 US-Japan DTA [3]	US, Japan	**1.** Neither Party shall require the transfer of, or access to, source code of software owned by a person of the other Party, or the transfer of, or access 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,[a] subject to safeguards against unauthorized disclosure.
Article 8.73 EU-Japan EPA [4]	EU, Japan	**1.** A Party may not require the transfer of, or access to, source code of software owned by a person of the other Party.[b] 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.** For greater certainty: **a.** the general exceptions, security exceptions and prudential carve-out referred to in Article DIGIT.4 [Exceptions] apply to measures of a Party adopted or maintained in the context of a certification procedure; and **b.** paragraph 1 of this Article does not apply to the voluntary transfer of, or granting of access to, source code on a commercial basis by a natural or legal person of the other Party, such as in the context of a public procurement transaction or a freely negotiated contract. **3**. Nothing in this Article shall affect: **a.** a requirement by a court or administrative tribunal, or a requirement by a competition authority pursuant to a Party's competition law to prevent or remedy a restriction or a distortion of competition; **b.** a requirement by a regulatory body pursuant to a Party's laws or regulations related to the protection of public safety with regard to users online, subject to safeguards against unauthorised disclosure; **c.** the protection and enforcement of intellectual property rights; and d. the right of a Party to take measures in accordance with Article III of the GPA as incorporated by Article PPROC.2 [Incorporation of certain provisions of the GPA and covered procurement] of Title VI [Public procurement] of this Heading.

FTA	Parties	General prohibition	Exceptions
Article 9 EU-Mexico Agreement in principle	EU, Mexico	**1.** No Party may require the transfer of, or access to, source code of software owned by a juridical or natural person of the other Party.	**2.** For greater certainty: **a.** this Article shall not prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective, including to ensure security and safety, for instance in the context of a certification procedure, in accordance with [reference to general exception, security exception and prudential carve-out]. **b.** paragraph 1 does not apply to the voluntary transfer of or granting of access to source code on a commercial basis by a person of the other Party, for instance in the context of a public procurement transaction or a freely negotiated contract. **3.** Nothing in this Article shall affect: **a.** requirements by a court, administrative tribunal or competition authority to remedy a violation of competition laws; **b.** intellectual property rights and their enforcement; and **c.** the right of a Party to take any action or not disclose any information that it considers necessary for the protection of its 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.
Article 207 EU–UK TCA	EU, UK	**1.** No Party may require the transfer of, or access to, source code of software owned by a juridical or natural person of the other Party.	**2.** For greater certainty: **(a)** the general exceptions, security exceptions and prudential carve-out referred to in Article 199 apply to measures of a Party adopted or maintained in the context of a certification procedure; and **(b)** paragraph 1 of this Article does not apply to the voluntary transfer of, or granting of access to, source code on a commercial basis by a natural or legal person of the other Party, such as in the context of a public procurement transaction or a freely negotiated contract. **3.** Nothing in this Article shall affect: **(a)** a requirement by a court or administrative tribunal, or a requirement by a competition authority pursuant to a Party's competition law to prevent or remedy a restriction or a distortion of competition; **(b)** a requirement by a regulatory body pursuant to a Party's laws or regulations related to the protection of public safety with regard to users online, subject to safeguards against unauthorised disclosure; **(c)** the protection and enforcement of intellectual property rights; and **(d)** the right of a Party to take measures in accordance with Article III of the GPA as incorporated by Article 277 of this Agreement.

[a] This disclosure shall not be construed to negatively affect the software source code's status as a trade secret, if such status is claimed by the trade secret owner.

[b] For greater certainty, "source code of software owned by a person of the other Party" includes source code of software contained in a product.