Source Code Disclosure and Free Trade Agreements

DIGITAL TRADE ALLIANCE

Why do we need to verify source code?

Software is an integral part of our lives today with an increasing number of software based products and services intermediating social and economic relations. The growth of the AI ecosystem implies that software (and the algorithms or source code underlying the software)[1] will be used in virtually every area of our lives — from the judiciary and policing to consumer products.

However, software can be programmed to serve illicit purposes or can have unintended consequences. We are, for instance, only beginning to understand the various harms that can occur due to the use of AI tools — which may range from replicating and exacerbating discrimination or biases to expropriating and misusing consumer data.[2]

Critical components of economic and social stability like home loans, job postings, medical treatments, targeted ads, and much, much more are influenced and determined by AI algorithms, enabling modernised redlining. Governments are likewise increasingly turning to these algorithms developed by private corporations for aid with "predictive policing" and other surveillance functions.[3]

Ensuring that a particular software "does what it says" or acts within acceptable legal and ethical bounds is essential to prevent harms ranging from a loss of life and property to illegal surveillance and discrimination.

In response to the potential harms that AI and other software-based systems create, an increasing number of international and domestic regulators have sought measures to enhance the transparency of AI-related products. Indeed, transparency and explainability of AI products is seen as a key regulatory tool to mitigate risks from the use of AI tools.[4] For example, the OECDs AI Principles recognise the need for transparency, explainability, accountability, robustness, security, and safety of AI tools.[5] In the U.S., the Blueprint for an AI Bill of Rights calls for pre-deployment testing, risk identification and mitigation, and ongoing monitoring to ensure that AI systems are not unsafe, discriminatory, or inaccurate, as confirmed by independent evaluation.[6] Similarly, a number of proposed

[1] A simple way of understanding source code is that this is the series of instructions that a computer program uses to perform a particular task. In more complex systems, based on machine learning and other newer forms of computing, the source code may provide guidance on how the program is to go about 'learning'. Algorithms are a set of instructions that are used to perform a specific task. Cosmina Dorobantu, Florian Ostmann and Christina Hitrova, Source Code Disclosure: A Primer for Trade Negotiators, in I Borchert and LA Winters (Eds), Addressing Impediments to Digital Trade, CEPR Press, London, 2021, https://www.turing.ac.uk/sites/default/files/2021-06/dorobantu_ostmann_hitrova_2021_1.pdf

[2] See generally Rick Claypool and Cheyenne Hunt, "Sorry in Advance!", Public Citizen, April 18, 2023 https://www.citizen.org/article/sorry-in-advance-generative-ai-artificial-intellligence-chatgpt-report/

[3] Melinda St Louis, Written Statement before the Subcommittee on International Trade, Customs, Global Competitiveness, US Senate Finance Committee, 117th Congress, December 14, 2022, https://www.citizen.org/wp-content/uploads/Trade-Policy-in-Digital-Economy-Hearing-Public-Citizen-Statement-for-Record-Dec-14-2022.pdf

[4] Explainability (or interrpretability) implies that humans should be able to understand the reasoning and process of arriving at results by an AI based system. Explainability can build trust in the use of AI systems, and enhance the agency of users. It can also reduce risks of harm, including by permitting evaluation of how AI systems are working (reliability and robustness) and course correction. The concept is seen as particularly important where AI systems can directly impact rights of individuals. See P Jonathan Phillips et al., *Four Principles of Explainable AI*, NISTIR 8132, National Institute of Standards and Technology, US Department of Commerce, September 2021, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8312.pdf; Ronan Hamon et al., *Robustness and Explainability of AI*, JRC Technical Report, European Commission, 2020, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC119336/dpad_report.pdf.

[5] OECD, OECD AI Principles Overview, https://oecd.ai/en/ai-principles

[6] The White House, Blueprint for an AI Bill of Rights, https://www.whitehouse.gov/ostp/ai-bill-of-rights/

data protection and other laws seek to ensure that software is safe to use by requiring pre- and post- deployment algorithmic impact assessments and algorithmic audits.[73]

However, these public interest regulations are called into question by provisions in trade agreements that seek to limit the ability of governments, regulators, and independent evaluators to access and verify the source code or algorithms used in various products.

However, these public interest regulations are called into question by provisions in trade agreements that seek to limit the ability of governments, regulators and independent evaluators to access and verify the source code or algorithms used in various products.

What do FTA clauses say about source code disclosure?

A number of recently signed trade agreements, for example the U.S.-Mexico-Canada Free Trade Agreement, the Trans-Pacific Partnership Agreement, the U.S.-Japan Free Trade Agreement, and the EU-UK Free Trade Agreement,[8] seek to limit the ability of parties to require disclosure of or access to the source code of software/algorithms as a condition precedent to the import, sale, use, or distribution of the relevant software or products containing the software. These agreements provide limited exceptions that permit disclosure of source code to a regulatory or judicial body for the purposes of a specific investigation or proceeding, though even in such cases disclosure is subject to unauthorised disclosure.[9]

In essence, these provisions imply that a signatory cannot require disclosure of the source code or algorithms contained in a software product, unless an investigation or inquiry into an identified malpractice or offence involving the relevant software or software product has been initiated. Parties to a free trade agreement (FTA) containing such a provision will therefore not be able to independently verify, ex-ante, whether and how a software product works before permitting its distribution or sale in their territories. Such a prohibition will extend not just to regulatory and public authorities, but will also limit the analysis of source code by independent experts and civil society.

Why do corporations want prohibitions on source code disclosure?

A number of tech companies have sought to protect themselves against source code disclosure requirements by lobbying for prohibitions in FTAs.[10] Corporations fear that disclosure of source code or algorithms could compromise the confidentiality of proprietary information used in their products. They argue that this could make it easier for other countries, and competitors to learn from and 'copy' the source code, thereby compromising strategic interests and affecting the value of their intellectual property.[11]

---

[7] A simple way of understanding source code is that this is the series of instructions that a computer program uses to perform a particular task. In more complex systems, based on machine learning and other newer forms of computing, the source code may provide guidance on how the program is to go about 'learning'. Algorithms are a set of instructions that are used to perform a specific task. Cosmina Dorobantu, Florian Ostmann and Christina Hitrova, Source Code Disclosure: A Primer for Trade Negotiators, in I Borchert and LA Winters (Eds), Addressing Impediments to Digital Trade, CEPR Press, London, 2021, https://www.turing.ac.uk/sites/default/files/2021-06/dorobantu_ostmann_hitrova_2021_1.pdf

[8] Cosmina Dorobantu, Florian Ostmann and Christina Hitrova, Source Code Disclosure: A Primer for Trade Negotiators, in I Borchert and LA Winters (Eds), Addressing Impediments to Digital Trade, CEPR Press, London, 2021, https://www.turing.ac.uk/sites/default/files/2021-06/dorobantu_ostmann_hitrova_2021_1.pdf .

[9] Different FTAs provide different levels of protection to source code and list different exceptions, with some of the common ones including exceptions to cater to government procurement, essential national security interests, to protect public morals, order or safety or protect human, animal or plant life or health. Cosmina Dorobantu, Florian Ostmann and Christina Hitrova, Source Code Disclosure: A Primer for Trade Negotiators, in I Borchert and LA Winters (Eds), Addressing Impediments to Digital Trade, CEPR Press, London, 2021, https://www.turing.ac.uk/sites/default/files/2021-06/dorobantu_ostmann_hitrova_2021_1.pdf

[10] See for instance: BSA Comments on the IPEF, Docket No. ITA-2022-001 (87 FR 13,971), March 30, 2022; Google Comments regarding the IPEF, 87 Fed Reg 13971, Docket No. ITA 2022-001, April 11, 2022.

[1] This fear may be particularly relevant in the case of countries that provide limited or low levels of intellectual property protection for software/algorithms.

Why are such provisions problematic for consumers?

Verification of source code is essential to ensure that software- based products and services function as they are meant to. Verification could also be used to mitigate risks that may arise from the use of the software. In this context, FTA provisions such as those described previously enhance the "black box" nature of AI and software tools. Preventing ex-ante evaluations of source code — whether by regulators or independent entities — limits the regulatory tools available to a State to reduce or mitigate the risks posed by new technologies.

By way of example, let's assume an American company wants to export to Mexico cars containing software that limits emissions. Even if permitted by domestic law, FTA provisions enforcing source code secrecy would prevent Mexican motor or environmental authorities from investigate whether the software component in the car works as declared or intended, before it actually goes on sale. The only instance in which such disclosure could be required, would be if there is a subsequent problem *that is detected* — leading to the opening of a formal investigation or inquiry. Thus, the provision restricts the regulatory powers to ex-post investigation and action, that is, they can only intercede once a problem becomes evident and harm has already been caused.

As software, and in particular AI, is intertwined into more and more sectors of our economies, directly affecting significant rights and interests of individuals and communities, it is vital that society retains the ability to scrutinise these products to ensure that harm can be prevented and not merely remedied. Consumer rights are at risk when FTAs limit the ability of countries, their regulatory and oversight agencies, or appropriate third parties to monitor the software being imported into their territories.

Further reading:

1. Cosmina Dorobantu, Florian Ostmann and Christina Hitrova, Source Code Disclosure: A Primer for Trade Negotiators, in I Borchert and LA Winters (Eds), Addressing Impediments to Digital Trade, CEPR Press, London, 2021, https://www.turing.ac.uk/sites/default/files/2021-06/dorobantu_ostmann_hitrova_2021_1.pdf
2. Daniel Rangel and Lori Wallach, International Pre-Emption by "Trade" Agreement: Big Tech's Ploy to Undermine Privacy, AI Accountability and Anti-Monopoly Policies, Rethink Trade, March 2023, https://rethinktrade.org/wp-content/uploads/2023/03/International-Preemption-by-Trade-Agreement.pdf
3. Kristina Irion, 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?, SSRN, January 27, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3786567