rethink TRADE

AMERICAN ECONOMIC LIBERTIES PROJECT

Undermining AI Regulation in the U.S. and Abroad: The "Digital Trade" Secrecy Ploy

July 2023

DIGITAL TRADE BRIEFING PAPERS SERIES #2

RETHINK TRADE

rethinktrade.org

Introduction

The development of artificial intelligence (AI) technologies, the evolution of the internet, and the growth of the data economy are fundamentally transforming every aspect of our lives. AI technologies can lead to more efficient exchanges and decision making. Yet unchecked and unregulated use of AI has proven to be harmful: It enables biased policing and prosecution, employment discrimination, intrusive worker surveillance, and unfair lending practices. Huge corporations, like Google and Amazon, also use problematic algorithms to self-preference their products and services and crush business competitors, increasing their monopoly power. In the United States and around the world, governments seek to seize the benefits of the digital revolution while also countering tech firms' ability to abuse workers, consumers, and smaller businesses.

In response, these powerful corporations are fighting back relentlessly. One under-the-radar strategy involves trying to lock in binding international rules that limit, if not altogether ban, key aspects of government oversight or regulation of the digital economy. To accomplish this, the tech industry is seeking to commandeer trade negotiations and establish what it calls "digital trade" agreements that would undermine Congress' and U.S. agencies' abilities to rein in their abuses.[1]

A key goal of industry's "digital trade" agenda is imposing rules that thwart governments from being able to proactively monitor, investigate, review, or screen AI and algorithms by forbidding government access to source code and perhaps, even detailed descriptions of algorithms.

Supporters of such source code and algorithm secrecy guarantees argue this is necessary to prevent untrustworthy governments from demanding tech firms hand over their algorithms, perhaps to be passed on to local companies that will knock off their inventions. That governments engaged in such conduct would be disciplined by new rules seems unlikely. Existing World Trade Organization (WTO) obligations and many nations' domestic laws already require governments to provide copyright protections and guarantees against disclosure of companies' confidential business information, including software's source code and other algorithmic data.[2] Businesses often complain that countries such as China do not comply with the existing rules.

Instead, these digital trade secrecy guarantees would bind scores of democratic countries worldwide that are considering new rules to prescreen or otherwise review the algorithms and source code running artificial intelligence applications in sensitive sectors. That industry's real goal is foreclosing AI regulation is underscored by the fact that the countries currently involved in U.S.-led trade negotiations do not have policies in place or under consideration that require government access to or transfer of source code or proprietary algorithms, according to a 2023 U.S. government review.[3]

1 David Dayen, "Big Tech Lobbyists Explain How They Took Over Washington," The American Prospect, 18 Apr. 2023. Available at: https://prospect.org/power/2023-04-18-big-tech-lobbyists-took-over-washington/.

2 Ulla-Maija Mylly, "Preserving the Public Domain: Limits on Overlapping Copyright and Trade Secret Protection of Software,". IIC 52, 1314–1337 (2021). Available at: https://doi.org/10.1007/s40319-021-01120-3.

3 Regarding countries involved in the Indo-Pacific Economic Framework Negotiations, see: Rethink Trade, "What Industry Identified as "Digital Trade Barriers" in the Indo-Pacific Region as Part of the National Trade Estimate Report Process," 17 Apr. 2023. Neither Kenya or Taiwan nor any Latin American or Caribbean country has imposed or is considering imposing this type of requirements according to the 2023 National Trade Estimate report. See: United States Trade Representative, 2023 National Trade Estimate Report on Foreign Trade Barriers. Available at: https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.

The primary effect of limiting governments' ability to demand source code and algorithm disclosure, then, would be to place the tech industry above regulatory oversight.

Casting a secrecy veil over source code and algorithms is especially problematic now that policymakers are responding to a growing movement demanding algorithmic transparency and accountability. The goal is for governments not only to have the tools to be able to sanction AI providers *after* their algorithms have been found to violate the law, but to *prevent* discriminatory or abusive practices. To do so, many AI experts have recommended policies that enable effective third-party audits of AI systems and/or require governmental pre-market screening conditioned upon access to source code and/or other types of algorithmic information particularly for high-risk sectors, like health services, credit, education, or employment.[4]

The European Union's Artificial Intelligence Act would, require firms to conduct conformity assessments prior to introducing high-risk AI applications to the European market to verify that the technology complies with the forthcoming regulation, in addition to prohibiting certain AI systems deemed to pose unacceptable risks to people's basic rights.

Under the EU policy, which is now being discussed by the European institutions, high-risk AI systems include those that can create risks for the health and safety or fundamental rights of natural persons, such as those related to critical infrastructure, education or employment, eligibility for public benefits, and credit scoring. National supervisory agencies in each EU member country

What is AI?

We hear the term "AI" everywhere.

And the use of AI is pervasive. But what is it exactly?

Although often associated with the simulation of human "intelligence," AI is a loosely defined term used to describe a wide spectrum of data-driven technologies that are often used to aid or replace human decision-making or provide recommendations and predictions.

Recently, generative AI, a technology that creates content such as text or video by identifying patterns in large quantities of training data, has received significant public attention.

Yet other AI-powered tools, commonly referred to as automated decision systems (ADS), are much more widely used and until now have a larger impact on everyone's daily lives. Decisions around hiring and workplace management, whether an applicant gets a home loan or insurance coverage, and peoples' access to public and private services, amongst many other areas, increasingly rely on ADS.

Underpinning these AI systems are a few core elements: large amounts of data, algorithms that process such data towards specific objectives, and computational power providing the infrastructure for such processing. The algorithm, expressed in a way that humans can understand it, is an example of "source code."

AI systems in practice have resulted in a range of demonstrated harms including inaccuracies, or biases that disproportionately affect particular demographic groups, such as women, people of color, or people with disabilities. These biases often stem from decisions around the type of data the model has been trained on, or the design of the algorithmic model itself, as embedded in its source code.

4 Timnit Gebru, Emily M. Bender, Angelina McMillan-Major, and Margaret Mitchell, "Statement from the listed authors of Stochastic Parrots on the "AI pause" letter," 31 Mar. 2023. Available at: https://www.dair-institute.org/blog/letter-statement-March2023; Data Ethics Commission, "Opinion of the Data Ethics Commission," 2019. P. 19, 184 Available at: https://www.bmj.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.pdf?__blob=publicationFile&v=2; Emanuel Moss, et al, "Assembling Accountability, Data & Society," Data & Society, 29 Jun. 2021. Available at: https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest/; 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?" (26 Jan. 2021). Available at SSRN: https://ssrn.com/abstract=3786567 or http://dx.doi.org/10.2139/ssrn.3786567.

were to have access to all information necessary to enforce the law, including source code.[5] However, a recent investigation revealed that EU trade authorities demanded that the Commission's proposal be weakened, so as to comply with source code secrecy rules that the EU negotiated with the United Kingdom.[6] The changes restrict the capacity of national supervisory agencies and external auditors to access the source code of high-risk AI applications.

In the United States, the House Committee on Energy and Commerce approved the American Data Privacy and Protection Act (ADPPA) on July 20, 2022, by a large bipartisan majority.[7] ADPPA is expected to be reintroduced in the current Congress. If enacted, this legislation would be the first U.S. national policy protecting personal data. Importantly, the ADPPA also includes a "civil rights and algorithms" title, which requires that certain entities submit impact assessments and algorithm design evaluations to the Federal Trade Commission (FTC).[8]

This bill is part of a broader strategy to ensure tech accountability in the United States. In October 2022, the White House released a document called "The Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People." This document is intended to support the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems. The blueprint calls for pre-deployment testing, risk identification and mitigation, and ongoing monitoring to ensure that AI systems are not unsafe, discriminatory, inaccurate, or ineffective. It calls for this to be confirmed by independent evaluation though algorithmic impact assessments.[9] Some AI experts have lamented the non-binding nature of the Blueprint.[10] However, even the possibility of third-party evaluations triggered the U.S. Chamber of Commerce to send a letter to the White House criticizing the proposal.[11]

To effectively implement the oversight needed to promote AI accountability or algorithmic justice, U.S. regulators and courts must have the ability to gain access to information about companies' AI systems, including source code and the data being fed into the program.

---

5 Mark MacCarthy and Kenneth Propp, "Machines learn that Brussels writes the rules: The EU's new AI regulation." Brookings, 4 May 2021. Available at: https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/; Art. 64.2 of the Artificial Intelligence Act proposal: "Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system." Accessed on 13 Dec. 2022. Available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

6 Mark MacCarthy and Kenneth Propp, "Machines learn that Brussels writes the rules: The EU's new AI regulation." Brookings, 4 May 2021. Available at: https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/; Art. 64.2 of the Artificial Intelligence Act proposal: "Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system." Accessed on 13 Dec. 2022. Available at: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

7 Aysha F. Allos, "American Data Privacy and Protection Act: Are We Finally Getting Federal Data Privacy Protection?" The National Law Review, 21 Sept. 2022. Available at: https://www.natlawreview.com/article/american-data-privacy-and-protection-act-are-we-finally-getting-federal-data-privacy.

8 Section 207(c) of the American Data Privacy and Protection Act (ADPPA). Accessed on 25 Sept. 2022. Available at: https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H6332551148B14109B1F2D9598E099E38.

9 White House, Office of Science and Technology Policy, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. Available at: https://www.whitehouse.gov/ostp/ai-bill-of-rights/.

10 Khari Johnson, "Biden's AI Bill of Rights is Toothless Against Big Tech," Wired, 4 Oct. 2022. Available at: https://www.wired.com/story/bidens-ai-bill-of-rights-is-toothless-against-big-tech/.

11 Derek Robertson, "Some signs that Meta may be playing nice," Politico, 12 Oct. 2022. Available at: https://www.politico.com/newsletters/digital-future-daily/2022/10/12/some-signs-that-meta-may-be-playing-nice-00061504.

Casting a secrecy veil over source code and algorithms is especially problematic now that policymakers are responding to a growing movement demanding algorithmic transparency and accountability.

However, tech interests both are trying to water down regulation at home,[12] while also pushing for "digital trade" provisions that explicitly forbid governments from having access to review software source code or algorithms, save for a few exceptions related to certain agencies and related to specific investigations or known problems.[13] In the most recent U.S. trade deal, the United States-Mexico-Canada Agreement (USMCA), these interests managed to insert prohibition on government access for not only source code, but also algorithms as a whole.[14]

Bournemouth University's legal scholars Maurizio Borghi and Benjamin White have pointed out that, given USMCA's broad definition of 'algorithms,'[15] this disclosure prohibition potentially covers descriptions of algorithms, not only the detailed source code developed by programmers.[16] This problematic, broad obligation and the secrecy protections it would impose could then preclude even the less expansive prescreening requirements proposed to date, like the one included in the ADPPA.[17]

Very few "digital trade" or e-commerce agreements have such extreme provisions. Only 11 of the 181 agreements with digital trade or e-commerce terms include secrecy guarantees for source code according to a trade-pact database that runs through mid-2021.[18] But tech interests hope to use Indo-Pacific Economic Framework (IPEF) negotiations now underway to impose such constraints on the governments that make up more than 40% of the world economy and do the same to the nations involved in the Americas Partnership for Economic Prosperity (APEP) negotiations. By doing so, they hope to "normalize" what are extreme and rare trade-agreement-imposed constraints on AI regulation, and perhaps get such terms inserted into a global agreement some countries are trying to negotiate called the Joint Statement Initiative on E-Commerce.

12 Emily Birnbaum, "The AI 'gold rush' in Washington," Politico, 29 Jun. 2022. Available at: https://www.politico.com/newsletters/digital-future-daily/2022/06/29/small-fry-ai-dc-try-00043278.

13 Third World Network Briefings, op. cit; International Trade Union Confederation, E-Commerce Free Trade Agreements, Digital Chapters and the Impact on Labour. (London, 2019), 4. Available at: https://www.ituc-csi.org/e-commerce-report.

14 USMCA Article 19.16.1 states: "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."

15 USMCA Article 19.1 states: "algorithm means a defined sequence of steps, taken to solve a problem or obtain a result."

16 Maurizio Borghi and Benjamin White, "Data extractivism and public access to algorithms: Mapping the battleground of international digital trade", in Law, Regulation and Governance in the Information Society. London, Routledge, 2022. P. 116.

17 ADPPA Section 207(c)(B) states: "The impact assessment required under subparagraph (A) shall provide the following: (i) A detailed description of the design process and methodologies of the covered algorithm (...)." Accessed on 25 Sept. 2022. Available at: https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H6332551148B14109B1F2D9598E099E38.

18 Calculations made using the TAPED dataset, "The Governance of Big Data in Trade Agreements," Universities of Lucerne and Bern. Accessed on Oct. 3, 2022. Available at: https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-directorinternationalisation/research/taped/.

The chart below shows the horizontal policies (meaning those that apply to multiple sectors and domains), and the area-specific policies that would be undercut by including secrecy guarantees for source code and algorithms in trade deals.

The rest of this Briefing Paper explores in detail some of the policy domains in which source code and algorithm secrecy guarantees could undermine existing government regulatory powers and derail future policies to counter AI-enabled abuses by tech companies.

Algorithmic Transparency and Accountability Policies Undercut by Source Code and Algorithm Secrecy Provisions

Horizontal Policies	White House Blueprint for an AI Bill of Rights American Data Privacy and Protection Act (ADPPA) Rules on Civil Rights and Algorithms Algorithmic Accountability Act of 2019			
	Area-Specific Policies			
	Criminal Justice System and Law Enforcement	**Fair Lending and Housing**	**Labor and Employment Law**	**Anti-Monopoly and Competition Policy**
Federal	Justice in Forensic Algorithms Act of 2021 Facial Recognition and Biometric Technology Moratorium Act of 2023 Facial Recognition Act of 2022	Biden Administration's Rulemaking on Property Appraisal and Valuation Equity Obama Administration's Report on Algorithmic Systems, Opportunity, and Civil Rights	Stop Spying Bosses Act of 2023	Department of Transportation's Algorithmic Disclosure Requirements for Computer Reservation Systems (CRS)**
State	Idaho's Criminal Procedure Rule on Pretrial Risk Assessments*			
	Washington's Guidelines on Government Procurement and Use of Automated Decision Systems			
Local	Washington D.C.'s 2023 Stop Discrimination by Algorithms Act			

* This legislation is already in force in the state of Idaho.

** This regulation expired in 2004.

Source Code Secrecy Protections Can Prevent Efforts to Regulate AI Use and Abuse in the Criminal Justice System

AI is being employed in the criminal justice system, with potentially untold dangerous consequences. From policing to investigation and trials to sentencing, the U.S. criminal justice system is increasingly becoming automated. While inaccurate or biased AI poses threats in many uses, the stakes are particularly high when people's liberty and lives are involved.

Yet law enforcement agencies have unreservedly embraced the use of forensic algorithms when investigating potential crimes and submitting evidence to court. There are three main types of forensic algorithms: facial recognition software, latent prints programs to identify finger and palm prints, and probabilistic genotyping. (Genotyping AI uses DNA samples from a crime scene and through statistical methods and mathematical algorithms compares them to a reference profile from one or more persons of interest.)[19]

AI is presented as infallible to judges and juries. And, when defense counsel seeks to examine forensic algorithm tools and access the source code and underlying data to challenge the evidence being brought against defendants, sometimes developers of these programs have used trade secrets law to block access and scrutiny. In order to contribute to defendants' right to a fair trial, Rep. Mark Takano (D-Calif.) introduced H.R. 2438: the Justice in Forensic Algorithms Act of 2021, which would prohibit the use of trade secrets law to block criminal defense scrutiny of law enforcement technologies, such as forensic algorithms. The legislation would also: (i) require the National Institute of Standards and Technology (NIST) to develop standards for testing computational forensic software; (ii) create a Computational Forensic Algorithm Testing Program at NIST, which would be in charge of testing software; and (iii) require that federal law enforcement agencies could only use forensic software that has been tested and approved by NIST. Finally, the bill requires that defendants are granted access to both the source code for the version of the computational forensic software used in their case and any relevant data used to train the algorithm.[20]

19 'Forensic algorithms: The future of technology in the US legal system,' Brookings Event. 12 May 2022. Video available at: https://www.brookings.edu/events/forensic-algorithms-the-future-of-technology-in-the-us-legal-system/.

20 H.R.2438 - Justice in Forensic Algorithms Act of 2021. Available at: https://www.congress.gov/bill/117th-congress/house-bill/2438/text.

Senators Edward Markey (D-Mass.) and Jeff Merkley (D-Oreg.) and Rep. Pramila Jayapal (D-Wash.) lead a bicameral group of Democrats proposing S. 2052/H.R.3907: the Facial Recognition and Biometric Technology Moratorium Act. This legislation would prevent federal agencies from using facial recognition and other biometric technologies, unless certain conditions are met, including the adoption of auditing requirements to ensure accuracy.[21] Reps. Ted Lieu (D-Calif.), Sheila Jackson Lee (D-Tex.), Yvette Clarke (D-NY), and Jimmy Gomez (D-Calif.) proposed H.R. 9061, the Facial Recognition Act of 2022, which limits use of facial recognition software to cases where law enforcement has obtained a warrant and bans its use to track individuals with live or stored video footage. Importantly, the bill would also require regular auditing of facial recognition systems used by law enforcement agencies and suspensions for agencies that fail audits, plus annual independent testing of any facial recognition software that law enforcement employs.[22]

It is easy to see how the different elements of these proposals are in direct contradiction with tech industry's trade-pact demand for expansive secrecy guarantees for source code. And contrary to claims by tech interests, the exceptions included in the past few pacts that included such secrecy terms do not fix the problem. The exceptions do not cover criminal justice AI uses, but rather focus on critical infrastructure, competition law, and intellectual property, or only cover orders from a regulatory body or court requiring source code disclosure for specific investigations and to a regulatory body, not allowing source code access by courts or a defendant in a criminal case, as proposed by Rep. Takano's bill.[23]

Another problematic use of AI in the criminal system is for risk assessments. Risk assessments are employed in a myriad of ways, from setting a defendants' bail[24] to judging their eligibility for alternative rehabilitative treatment[25] to determining the conditions of their probation,[26] to – in some states – sentencing by mandating the amount of prison time a defendant must serve.[27] However, these forecasting assessment tools rely on algorithms that are potentially fed biased and inaccurate data.

21 Office of Representative Ed Markey, 'Markey, Merkley, Jayapal Lead Colleagues on Legislation to Ban Government Use of Facial Recognition and Other Biometric Technology,' 7 Mar. 2023. Available at: https://www.markey.senate.gov/news/press-releases/markey-merkley-jayapal-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-and-other-biometric-technology.

22 Office of Representative Ted Lieu, 'Reps Ted Lieu, Sheila Jackson Lee, Yvette Clarke, and Jimmy Gomez Introduce Bill to Regulate Law Enforcement Use of Facial Recognition Technology,' 29 Sept. 2022. Available at: https://lieu.house.gov/media-center/press-releases/reps-ted-lieu-sheila-jackson-lee-yvette-clarke-and-jimmy-gomez-introduce.

23 USMCA Article 19.16.2 states: "This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding, subject to safeguards against unauthorized disclosure."

24 Anna Maria Barry-Jester et. al., "The New Science of Sentencing," The Marshall Project, 4 Aug. 2015. Available at: https://www.themarshallproject.org/2015/08/04/the-new-science-of-sentencing.

25 Julia Angwin et al., "Machine Bias," ProPublica, 23 May 2016. Available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. See also Kate Crawford, "Artificial Intelligence's White Guy Problem," New York Times, 26 Jun. 2016. Available at: https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html?mcubz=1.

26 Eileen Sullivan et al., "States predict inmates' future crimes with secretive surveys," Associated Press, 24 Feb. 2015. Available at: https://apnews.com/article/027a00d70782476eb7cd07fbcca40fc2.

27 Alexandra Chouldekova, "Fair Prediction with Disparate Impact: A Study of Bias in Recidivism Prediction Instruments," Updated Feb. 2017, https://arxiv.org/pdf/1703.00056.pdf.

Risk assessment algorithms are informed by questionnaires, which ask about a defendant's education, job status, family, income, parents' involvement with the criminal justice system, and even whether they have a phone. This information constructs a score. The scores are based on previous offenders' behavior who responded similarly to a current defendant. Risk corresponds to the score – if the score is higher, the defendant is deemed higher risk and faces more scrutiny and monitoring.

This model to predict recidivism has been criticized for potentially overpredicting the chance that Black defendants would commit another crime. By relying on data about past offenders to predict what current and future defendants might do after being released from prison, these algorithms reinforce existing racial disparities in the criminal justice system.

A ProPublica study, based on 7,000 risks scores found in Broward County in Florida, concluded that the algorithm was neither reliable nor accurate and exhibited significant racial biases. Only 20% of the people predicted to commit violent crimes by the risk assessment system actually went on to do so. Plus, the algorithm used in that county was likely to flag Black defendants as future defendants at almost twice the rate as white defendants. White defendants were mislabeled as low risk more often than Black defendants.[28]

The parties making the risk assessment software do not publicly disclose the specific process behind how scores are generated. Defendants are unable to challenge these assessments, and they also are not privy to the data calculations. Even judges are unable to understand the logic behind the software. [29]

28 Angwin et al., op. cit.

29 Crawford, et al., op. cit.

According to Professor Christopher Slobogin, director of the criminal justice program at Vanderbilt Law School, "*risk assessments should be impermissible unless both parties get to see all the data that go into them. It should be an open, full-court adversarial proceeding.*"[30] In 2019, Idaho enacted a policy consistent with Professor Slobogin's recommendation. It requires that any pretrial risk assessment must be shown to be non-discriminatory before being used and localities availing themselves of these tools must guarantee that all documents, records, and information used to build or validate the risk assessment are open to public inspection, auditing, and testing.[31] The risk assessment system's source code is part of the information that would be required by a defendant to be able to exercise their right to due process, as well as part of the documentation that Idaho requires to be publicly available. Yet, the source code secrecy terms that tech industry interests seek in "digital trade" agreements would deny access to such information.

AI's role in the criminal system has not been limited to the courtroom. Police departments across the United States are also using data-driven risk-assessment tools in "predictive policing" crime prevention efforts. In many cities, including New York, Los Angeles, San Francisco, Chicago, and St. Louis, software analyses of large sets of historical crime data are used to identify crime "hot spots." The police then aggressively patrol these areas with the objective of deterring crime before it happens.[32]

> The widespread use of 'predictive policing' software, risk assessments systems, forensic algorithms, and the general pervasiveness of AI systems in public administration has fueled claims in many U.S. states for transparency rules at the local government level.

Civil liberties advocates have raised concerns about such software potentially perpetuating a vicious cycle: The police increase their presence in the same places they are already policing, thus ensuring that more arrests come from those areas, which dooms these places as crime "hot spots."[33] Additionally, predictive programs are only as good as the data on which they are trained, and that data has a complex history. A recent study from researchers from the AI Now Institute at New York University shows that the data used by these systems in several jurisdictions were produced during documented periods of flawed, racially biased, and sometimes unlawful policing practices and policies. Basing predictive policing on this "dirty data" risks entrenching the practices that have led to unlawful and biased policing practices.[34]

30 Angwin et al., op. cit.

31 Idaho Legislature. House Bill 118. Jul. 1, 2019. Accessed 8 Dec. 2022. Available at: https://legislature.idaho.gov/sessioninfo/2019/legislation/H0118/.

32 Maurice Chammah, "Policing the Future," The Marshall Project, 3 Feb. 2016. Available at: https://www.themarshallproject.org/2016/02/03/policing-the-future#.9vrCo3ZOH; Andrew Guthrie Ferguson, "Predicting Predictive Policing in NYC," Huffington Post, 8 Jul. 2016. Available at: https://www.huffpost.com/entry/predicting-predictive-pol_b_7757200; Darwin Bond-Graham and Ali Winston, "All Tomorrow's Crimes: The Future of Policing Looks a Lot Like Good Branding," SF Weekly, 30 Oct. 2013. Available at: https://archives.sfweekly.com/sanfrancisco/all-tomorrows-crimes-the-future-of-policing-looks-a-lot-like-good-branding/Content?oid=2827968.

33 Chammah, op. cit.

34 Rashida Richardson, Jason Schultz, and Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," (13 Feb. 2019). 94 N.Y.U. L. REV. ONLINE 192 (2019), Available at SSRN: https://ssrn.com/abstract=3333423.

The widespread use of "predictive policing" software, risk assessments systems, forensic algorithms, and the general pervasiveness of AI systems in public administration has fueled claims in many U.S. states for transparency rules at the local government level. These rules would guarantee public access to software's source code of automated decision systems (ADS) employed by local authorities.

The policies being advanced to address these concerns reflect the audit and review tools included in the Biden administration's Blueprint for an AI Bill of Rights. New York City established an ADS Task Force, consisting of a group of city officials assigned with the responsibility to establish a process for reviewing the city's use of automated decision systems. In 2018, a group of AI experts wrote a report in parallel with the Task Force, recommending that the city release a public list of ADS used by agencies both online and accessible in print at branches of the New York Public Library system. They called for this list to include, among other information, ADS' source code.[35] In Washington, state legislators introduced a bill in 2021 that would require state agencies to ensure that ADS vendors make both the system and data used to develop the algorithm freely available for agency or third-party testing, auditing, and research, while also prohibiting non-disclosure clauses that would preclude access to algorithmic information.[36] The Electronic Privacy Information Center (EPIC) published a report documenting the generalized used of ADS in Washington D.C. that showed at least 20 agencies use 29 systems. EPIC recommended, among other policies, enacting laws requiring comprehensive algorithmic governance, including audits and impact assessments.[37] This recommendation is consistent with the 2023 Stop Discrimination by Algorithms Act proposed by former D.C. Attorney General Karl Racine, a bill requiring companies to audit their algorithms for discriminatory patterns and submit annual reports to the Office of the Attorney General for the District of Columbia with information including the methodologies and optimization criteria of the algorithms.[38]

These policies would likely run afoul of the extreme source code secrecy guarantees that the tech industry seeks in IPEF and other digital trade deals. While most existing digital trade deals have carveouts for government procurement, it is unlikely that the types of policies described above would qualify for this reservation. USMCA, for instance, defines government procurement as *"the process by which a government obtains the use of or acquires goods or services (…) for governmental purposes (…)."* By emphasizing on the procurement "process," the carveout likely only covers the conditions that agencies can adopt when carrying out a public tender or negotiating a government contract. This would leave policies that create general conditions for AI systems that government can use or those that would make public ADS purchased by local governments susceptible to attacks based on source code secrecy guarantees.

35 Rashida Richardson, ed., "Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force," AI Now Institute, 4 Dec. 2019. Available at: https://ainowinstitute.org/publication/confronting-black-boxes-a-shadow-report-of-the-new-york-city-automated.

36 Washington Legislature. SB 5116 - 2021-22: Establishing guidelines for government procurement and use of automated decision systems in order to protect consumers, improve transparency, and create more market predictability. Accessed on 7 Dec. 2022. Available at: https://app.leg.wa.gov/billsummary?billnumber=5116&year=2021&msclkid=7dc3be5fc26c11ecb582ea23e6e5b75d#documentSection.

37 Electronic Privacy Information Center, "Screened & Scored in D.C.," Nov. 2022. Available at: https://epic.org/screened-scored-in-dc/.

38 Office of the Attorney General for the District of Columbia, 'AG Racine Introduces Legislation to Stop Discrimination In Automated Decision-Making Tools That Impact Individuals' Daily Lives,' 9 Dec. 2021. Available at: https://oag.dc.gov/release/ag-racine-introduces-legislation-stop.

Source Code Secrecy Protections Can Obstruct Efforts to Guarantee Fair Lending and Housing

Statistical models and algorithms have been used in consumer finance for decades to provide information for loan officers to consider. However, today's systems are being used in unprecedented ways to decide who will gain access to a home loan or other types of credit and under which terms, with very little human oversight or input.

The extensive use of such AI in consumer finance is controversial, as it is likely to entrench or even worsen the long-standing discrimination that minorities face in credit markets. A 2021 study found that lenders were 40 to 90% more likely to turn down Latino, Asian, Native American, and Black applicants than similar white applicants. Black applicants in higher income brackets with less debt were rejected more often than white applicants in the same income bracket, who had more debt.[39] Another study found that borrowers from minority groups were charged interest rates that were nearly 8% higher than their white counterparts.[40]

When huge datasets are used to analyze creditworthiness, certain variables – such as level of education – could act as proxies for race, ethnicity, or gender, allowing AI systems to systematically determine that, for instance, Black or Latino applicants are less creditworthy than white people.[41] And, if wealth is used as a barrier to entry, white people are automatically favored, given that at present, white families typically hold eight times the wealth of typical Black families.[42] Plus, the type of data collected and/or the exclusion of data is troubling and prevalent. Decades of bias in credit decisions means different amounts of data are available in the credit histories of different categories of people. The absence of data has been shown to result in different mortgage approval rates between minority and majority applicants.[43]

This data is then fed into automated decision systems that employ algorithms that often have disproportionately negative effects on communities of color because they reflect the unequal access to credit that resulted from America's long history of discrimination.

Consider the classic FICO credit model as a way to understand how both data and design problems can result in discriminatory outcomes. This credit scoring algorithm is used by many big lenders, such as the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan

39 Emmanuel Martinez, et al., "The Secret Bias Hidden in Mortgage-Approval Algorithms", The Markup, 25 Aug. 2021. Available at: https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

40 Robert Barlett, Adair Morse, Richard Stanton, and Nancy Wallace, "Consumer-lending discrimination in the FinTech Era," Journal of Financial Economics, Vol. 143, No. 1. Jan. 2022. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0304405X21002403?via%3Dihub.

41 Carol Evans, et al., "Keeping Fintech Fair: Thinking About Fair Lending and UNDAP risks", Computer Compliance Outlook, Second Issue 2017. Available at: https://www.consumercomplianceoutlook.org/2017/second-issue/keeping-fintech-fair-thinking-about-fair-lending-and-udap-risks/.

42 David Brancaccio, "How mortgage algorithms perpetuate racial disparity in home lending", Marketplace, 25 Aug 2021. Available at: https://www.marketplace.org/2021/08/25/housing-mortgage-algorithms-racial-disparities-bias-home-lending/.

43 Will Douglas Heaven, "Bias isn't the only problem with credit scores – and no, AI can't help," MIT Technology Review, 17 Jun. 2021. Available at: https://www.technologyreview.com/2021/06/17/1026519/racial-bias-noisy-data-credit-scores-mortgage-loans-fairness-machine-learning/.

Mortgage Corporation (Freddie Mac), to assess and decide mortgage applications. The Classic FICO algorithm was built using data from the 1990s and is more than fifteen years old. It only considers traditional credit, which is more accessible to white Americans, and does not account for timely rent and telephone bill payments. (It does capture late payments of rent and phone bills as demerits.) FICO will only assign a credit score for people who meet certain minimum scoring criteria, such as having a bank account open for more than six months.

Discriminating on the base of gender, race, or ethnicity is already banned by the Equal Credit Opportunity Act and the Fair Housing Act. However, these statutes are underenforced. Lack of access to the underlying source code is a contributing factor.

To counter such bias, experts have recommended creating fairer credit models or using alternatives. Vantage Score is one example of a credit model competing with FICO. It does not limit the pool of people that can have a credit score via the sort of minimum scoring criteria used in FICO. Vantage reports that it can provide 37 million Americans with credit who currently have no FICO score, a third of whom are Black or Latino.[44] Creating a more inclusive credit rating model would involve the related AI systems omitting data on crime, schools, and income, which in turn would better protect people's ethnicity and race from being disclosed.[45] More accurate metrics to measure risk, such as crediting timely rent and utility payments, would allow mortgage lenders to choose applicants based on their ability to pay back a loan without enforcing historically discriminatory trends.

Discriminating on the base of gender, race, or ethnicity is already banned by the Equal Credit Opportunity Act and the Fair Housing Act. However, these statutes are underenforced.[46] Lack of access to the underlying source code is a contributing factor. Already in 2016, the Obama administration recommended promoting algorithmic auditing and external testing of big data systems to ensure that people are being treated fairly.[47] This recommendation was partially based on already existing concerns about credit eligibility decisions being made by algorithms that have the potential to perpetuate, exacerbate, or mask discrimination. In turn, the Biden administration has committed to include a non-discrimination standard in a forthcoming regulation on automated valuation models used to determine the collateral worth of a mortgage secured by the lender's house.[48] Enforcing the compliance with such a non-discrimination standard would require permitting agencies to have access to these models' source code and underlying data. Yet "digital trade" provisions that ban access to source code and algorithms would be in direct contradictions with these policies.

---

44 Martinez et al., op cit.

45 Tony Cantu, "How one firm is overcoming racial bias in the mortgage industry," Mortgage Professional America Magazine, 10 Dec. 2021. Available at: https://www.mpamag.com/us/news/general/how-one-firm-is-overcoming-racial-bias-in-the-mortgage-industry/319520.

46 Martinez et al., op cit.

47 White House, "Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights," May 2016. P. 23. Available at: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

48 Interagency Task Force on Property Appraisal and Valuation Equity, "Action Plan to Advance Property Appraisal and Valuation Equity: Closing the Racial Wealth Gap by Addressing Mis-valuations for Families and Communities of Color," Mar. 2022. P. 27. Available at: https://pave.hud.gov/sites/pave.hud.gov/files/documents/PAVEActionPlan.pdf.

Source Code Secrecy Can Conceal Labor Law Violations and Employment Discrimination

When it comes to work, AI-enabled digital technologies are being used by employers to recruit, hire, and evaluate the performance of — and exert control over — workers. AI is also being used to partially automate tasks in the name of increasing productivity, by getting more done with fewer people.[49] The use of digital technologies in the workplace doesn't need to hurt workers. However, the unchecked and unregulated usage of AI technologies by employers can easily lead to violations of wage and hour labor laws with work speed-ups and scheduling gimmicks that result in people working when not 'on the clock' and not being paid.

The use of digital technologies in the workplace doesn't need to hurt workers. However, the unchecked and unregulated usage of AI technologies by employers can easily lead to violations of wage and hour labor laws with work speed-ups and scheduling gimmicks that result in people working when not 'on the clock' and not being paid.

For instance, in 2015, workers filed class-action lawsuits against McDonald's stores in California, Michigan, and New York, alleging systematic wage theft associated with workplace management software. The stores involved reportedly used a computer program that calculated labor costs every fifteen minutes as a percentage of revenue. When the labor cost share was above a predetermined target, managers would routinely order employees to clock out and wait in break rooms for minutes or hours without pay. Only when revenue picked up were workers allowed to clock back in. Managers would tell workers to clock out before the end of their shifts but insist that they finish certain tasks before going home.[50]

AI programs also undermine workers' rights to organize unions and foster hazardous working conditions, growth in contingent work, and loss of autonomy and privacy.[51] AI-enabled surveillance technologies already have been used by companies like Walmart, Amazon, Google, and HelloFresh with the intent of chilling union organizing. [52] Among other tactics, these firms have monitored employees' activity, conversations, and social media posts about union activism. Employers have used heat maps, which were based on predictive analytics, to track store locations considered at high risk of union activity. They have also utilized systems to alert managers to any internal meetings scheduled with 100 or more employees.

49 Annette Bernhardt, Annette Kresge, and Reem Suleiman, "Data and Algorithms at Work; The Case for Worker Technology Rights." Berkeley: Center for Labor Research and Education, University of California, Berkeley. 3 Nov. 2021. P. 7. Available at: https://laborcenter.berkeley.edu/data-algorithms-at-work/.

50 Esther Kaplan, "The Spy Who Fired Me," Harper's Magazine, Mar. 2015. Available at: https://harpers.org/archive/2015/03/the-spy-who-fired-me/.

51 Bernhardt, Kresge & Suleiman, op cit. P. 16.

52 Jo Constantz, "'They Were Spying On Us': Amazon, Walmart, Use Surveillance Technology to Bust Unions", Newsweek, Dec. 2021. Available at: https://www.newsweek.com/they-were-spying-us-amazon-walmart-use-surveillance-technology-bust-unions-1658603".

Concerning hazardous working conditions, Amazon tracks and monitors warehouse workers' entire workday. Any "time-off-task," such as unallotted bathroom breaks, can generate algorithm-based warnings or even lead to termination.[53] This kind of workplace surveillance jeopardizes workers' safety. Ratcheting up workloads and work speeds have contributed to Amazon's injury rate, which is three times the national average and, for serious injuries, five times the national average.[54]

Additionally, algorithmic hiring and recruitment software can replicate and deepen existing inequities. Certain individuals are systematically excluded from employment when source code reflects the biases of its developers or when the algorithm is trained by inaccurate, biased, or unrepresentative data.[55] The Equal Employment Opportunity Commission is already investigating at least two cases involving claims that algorithms unlawfully exclude certain groups of workers during the recruitment process.[56] This is not a negligible issue: Major employers such as Unilever, Hilton, and Delta Air Lines use data-driven predictive hiring tools,[57] which inform decisions that could be exacerbating racial, ethnic, and gender inequalities.

To prevent workplace discrimination or sanction it if it occurs, violations of wage and hour laws, and the proliferation of hazardous working conditions, experts recommend adopting policies that require impact assessments or audits for regulatory investigations.[58] Requiring firms to conduct these impact assessments or audits to prevent labor law violations could be a policy to be adopted by the Privacy and Technology Division that S.262: the Stop Spying Bosses Act, a bill recently introduced by Senators Bob Casey (D-Pa.), Cory Booker (D-NJ), and Brian Schatz (D-Hawaii), would create at the Department of Labor to enforce and regulate workplace surveillance.[59] All of these would require access to software's algorithms and potentially source code, which digital firms are trying to preclude through obscure "digital trade" rules.

Guarantees of Source Code Secrecy Can Cloak Anti-Monopoly and Competition Policy Violations

Consumers were promised that the rise of online markets, underpinned by the data economy and powerful algorithms, would encourage competition and efficiency. Yet, behind the façade of virtual

53 Colin Lecher, "How Amazon automatically tracks and fires warehouse workers for 'productivity,'" The Verge, 25 Apr. 2019. Available at: https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.

54 National Employment Law Project and The Athena Coalition, "Packaging Pain: Workplace Injuries in Amazon's Empire," Dec. 2019. P. 3. Available at: https://worker-centerlibrary.org/product/packaging-pain-workplace-injuries-in-amazons-empire/.

55 Jenny Yang, "The Future of Work: Protecting Workers' Civil Rights in the Digital Age, Before the Civil Rights and Human Services Subcommittee," 5 Feb. 2020. P. 5. Available at: https://www.congress.gov/116/meeting/house/110438/witnesses/HHRG-116-ED07-Wstate-YangJDJ-20200205.pdf.

56 Chris Opfer, "AI Hiring Could Mean Robot Discrimination Will Head to Courts," Bloomberg Law, Nov. 2019. Available at: https://news.bloomberglaw.com/daily-labor-report/ai-hiring-could-mean-robot-discrimination-will-head-to-courts.

57 Drew Harwell, "A face-scanning algorithm increasingly decides whether you deserve the job," Washington Post, 6 Nov. 2019. Available at: https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

58 Yang, op cit. P. 13; Bernhardt, Kresge & Suleiman, op cit. P. 25-26.

59 Office of Senator Casey, "Casey, Booker, Schatz Introduce Bill to Protect Workers from Invasive, Exploitative Surveillance Technologies," 2 Feb. 2023. Available at: https://www.casey.senate.gov/news/releases/casey-booker-schatz-introduce-bill-to-protect-workers-from-invasive-exploitative-surveillance-technologies.

competition, algorithms often hide collusive behavior, price discrimination, self-preferencing by the largest platforms, and other forms of monopolistic abuse that thwart the promised benefits and threaten the resilience of the wider economy. The public is seeing the evidence of such misconduct in press reports while policymakers also review scholarly research documenting how dominant platforms use AI to expand their monopoly power.

Yet, behind the façade of virtual competition, algorithms often hide collusive behavior, price discrimination, self-preferencing by the largest platforms, and other forms of monopolistic abuse that thwart the promised benefits and threaten the resilience of the wider economy.

Algorithms can further collusion among competitors either by acting as a "hub" that creates the scenario for competing firms to collude without being even in contact with each other or by providing means to monitor compliance with a human-made or AI-set price-fixing agreements.[60] The French and German governments' competition authorities identified the way in which algorithms can be used by firms to collude and charge higher prices on consumers in a joint report:

"Data collection may also facilitate collusion when these data are used to fix prices through the use of algorithms. Even though market transparency as a facilitating factor for collusion has been debated for several decades now, it gains new relevance due to technical developments such as sophisticated computer algorithms. For example, by processing all available information and thus monitoring and analysing or anticipating their competitors' responses to current and future prices, competitors may easier be able to find a sustainable supra-competitive price equilibrium which they can agree on."[61]

These are not hypothetical concerns. In 2015, the U.S. Department of Justice (DOJ) charged a group of sellers in the Amazon marketplace for fixing the prices of posters sold online between September 2013 and January 2014. According to the DOJ's investigation, the conspirators designed and shared among each other dynamic pricing algorithms that were programmed to coordinate changes to their respective prices.[62] In November 2022, a group of renters filed a lawsuit against RealPage and nine big property managers for allegedly forming a cartel to artificially inflate rents through RealPage's price-setting software for apartments.[63] Two additional lawsuits were filed against RealPage since then, and several lawmakers have called on the FTC and DOJ to investigate RealPage's rent-setting software.[64]

---

60 Competition & Markets Authority, "Pricing algorithms: Economic working paper on the use of algorithms to facilitate collusion and personalised pricing," 8 Oct. 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746353/Algorithms_econ_report.pdf; Ariel Ezrachi, and Maurice Stucke, Virtual Competition: The Promise and Perils of the Algorithmic-Driven Economy. Cambridge, Massachusetts, Harvard University Press, 2016. P. 35 – 37.

61 Autorité de la Concurrence and Bundeskartellamt (2016), Competition Law and Data. Available at: www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publ.

62 Justice News of the US Department of Justice, Office of Public Affairs, "Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution." Available at: www.justice.gov/opa/pr/former-e-commerce-executive-charged-price-fixing-antitrust-divisions-first-online-marketplace.

63 Heather Vogell, "Company That Makes Rent-Setting Software for Apartments Accused of Collusion, Lawsuit Says," ProPublica, 21 Oct. 2022. Available at: https://www.propublica.org/article/realpage-accused-of-collusion-in-new-lawsuit.

64 Heather Vogell, "Pressure Grows on Real Estate Tech Company Accused of Colluding With Landlords to Jack Up Apartment Rents," ProPublica, 14 Nov. 2022. Available at: https://www.propublica.org/article/yieldstar-rent-increase-realpage-lawmakers-collusion.

In these cases, government officials' ability to identify whether an algorithm is designed to facilitate collusion would be key to investigate a pattern when suspicions arise, but absent a review of the underlying code along with datasets and accompanying business documentation, the evidence is not sufficient to prove an anticompetitive conduct.[65]

An often-disregarded goal of the pervasive practice of digital firms' commercial surveillance is engaging in price discrimination, which is the technical term for what Professor Yossi Sheffi of the Massachusetts Institute of Technology (MIT) has called *"the science of squeezing every possible dollar from customers."*[66] Pricing algorithms are a key enabler of this practice. For instance, in 2012, *the Wall Street Journal* reported how Staples' online sales algorithm used customers' location data to charge different prices for the same goods. The algorithm considered the customer's distance from Staples' rivals, such as Office Depot or OfficeMax stores. If rival stores were found within 20 miles, the algorithm automatically offered a discounted price.[67]

Similarly, on-the-job data collection and algorithmic decision-making systems have allowed the use of granular data to produce unpredictable, variable, and personalized hourly pay, a practice dubbed by law professor Veena Dubal as "algorithmic wage discrimination." The clearest example of this practice is currently found in the ridesharing industry, where Dubal found that work allocation systems, dynamic pricing and incentives allow firms like Uber to personalize and differentiate wages for workers in ways unknown to them, paying them as little as the system determines that they may be willing to accept.[68]

AI also enables Big Tech platforms' anti-competitive self-preferencing. In 2017, the European Commission sanctioned Google because its algorithm promoted its own comparison shopper service, called Google Shopping, over competitors, abusing its dominant position in the internet search market. The European authorities found that Google included a number of criteria in its generic search algorithms that resulted in rival comparison shopping services being demoted.[69] The European Commission also preliminarily concluded that Amazon's algorithmic rules and criteria for its Buy Box feature and Prime program unduly favor its own retail business, as well as marketplace sellers that use Amazon's logistics and delivery services.[70]

---

65 Ezrachi & Stucke, op cit. P. 53.

66 James Surowiecki, "In Praise of Efficient Price Gouging," MIT Technology Review, 18 Aug. 2014. Available at: https://www.technologyreview.com/2014/08/19/74207/in-praise-of-efficient-price-gouging/.

67 Jennifer Valentino-DeVries, Jeremy Singer-Vine, and Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information," The Wall Street Journal, 24 Dec. 2012. Available at: https://www.wsj.com/articles/SB10001424127887323777204578189391813881534.

68 Veena Dubal, "On Algorithmic Wage Discrimination," UC San Francisco Research Paper. 19 Jan. 2023. Available at SSRN: https://ssrn.com/abstract=4331080 or http://dx.doi.org/10.2139/ssrn.4331080.

69 European Commission, 'Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service,' 17 June 2017. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1784.

70 European Commission, ;Antitrust: Commission accepts commitments by Amazon barring it from using marketplace seller data, and ensuring equal access to Buy Box and Prime,' 20 Dec. 2022. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7777.

Proof of such conduct often is buried in algorithms' code. Even before the European Commission imposed its 2017 sanctions against Google, legal scholars were positing that "*[a]gencies ought to be able to "look under the hood" of highly advanced technologies like the algorithms at the heart of the Google search engine and the data they process.*"[71]

Additionally, agencies might need to require disclosure of algorithmic information to protect competition in regulated industries. For instance, until 2004, the U.S. Department of Transportation required companies operating computer reservation systems (CRS) for air travel to share the ranking criteria used in sorting algorithms for displayed flights, including "*the specifications used by the system's programmers in constructing the algorithm.*"[72]

The source code and algorithmic secrecy guarantees that tech interests are pushing for to be included in "digital trade" deals are likely to get in the way of agencies or private parties being able to "look under the hood."

The narrow exceptions supported by tech interests could limit antitrust enforcers' ability to effectively fight anticompetitive behavior.

Plus, industry-wide requirements to disclose algorithmic information about ranking criteria and system specifications, such as those applied by the Department of Transportation to CRS until 2004, would certainly not be covered by USMCA's narrow exception.

For instance, the USMCA exception to its source code and algorithm secrecy provision only permits source code disclosure requests or orders by regulatory bodies or judicial authorities and only "*to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding.*" (emphasis added). Namely, the exception only applies after a government agency or private party has sufficient evidence of a violation of a law or right to meet a burden of proof to be able to obtain more information, whether through an agency investigation, court order, or civil suit discovery. (Note that the exception allows disclosure "*to the regulatory body*", meaning that it is unclear whether a private party filing a lawsuit could be allowed to gain access to the required information under this rule.) Yet it may well not be possible to meet that burden of proof without having access to the information about the source code or algorithm, along with the dataset and relevant business documentation, that reveals the antitrust or other violation. And even for agencies whose statutes provide broad investigatory authority, the limitation for "specific" investigation calls into question whether such trade-pact language would encompass a broad investigation into an economic sector or general practices of a firm rather than for a specific suspected violation. Plus, industry-wide requirements to disclose algorithmic information about ranking criteria and system specifications, such as those applied by the Department of Transportation to CRS until 2004, would certainly not be covered by USMCA's narrow exception.

71 Frank Pasquale, The Black Box Society: the secret algorithms that control money and information, Harvard University Press, 2015.

72 14 CFR 255.4 (3); Upturn and Omidyar Network, Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods. Available at: https://omidyar.com/wp-content/uploads/2020/09/Public-Scrutiny-of-Automated-Decisions.pdf.

The EU model for this exception is equally problematic as it covers source code disclosures required to "*remedy a violation of competition law*."[73] This leaves out the disclosures required to unveil or prove that such a violation has indeed occurred.

Conclusion

Corporate interests are advocating for strict limits on government access to source code and even detailed information about algorithms that would effectively establish extreme source code and algorithm secrecy guarantees in U.S. "trade" agreements.[74] Obviously, such terms have nothing to do with trade, but rather represent an effort by special interests to use closed-door international negotiations on future international agreements to lock in powers and rights for themselves that would be difficult to achieve through public debate in more open policymaking venues.

These provisions are premised on the notion that private commercial interests prevail over the public interest. This briefing paper shows how algorithmic transparency and accountability is essential to ensure that AI works in favor of the public and not against it. Yet, if trade deals impose limits on the capacity of governments and courts to mandate disclosure of source code and other algorithm-related information, tech companies could eviscerate prospective regulation and evade government oversight.

It is notable that only 11 of the 181 agreements with ecommerce or digital trade provisions negotiated since 2000 include obligations to limit government access to source code,[75] showing how controversial this particular concept is.

In addition to the fact that "digital trade" source code secrecy provisions are at odds with algorithmic transparency and accountability principles, there is no rationale that justifies granting these special interests extraordinary new privileges and rights. Tech firms that wish to protect their proprietary source code and algorithms can rely on existing intellectual property and trade secrets protections. If a company develops pathbreaking software, it can copyright the code and/or request patent protection to secure the right to commercialize and use the software exclusively, including its source code, with certain exceptions. If the same company does not want to register a copyright or file for a patent, as long as the algorithm complies with the requirements enshrined in existing regulation, it can rely on existing protections to undisclosed information to ensure its code is not improperly accessed or shared.[76]

---

73 See Article 8.73.2(a) of the EU-Japan Economic Partnership Agreement.

74 The U.S. Chamber of Commerce has announced in its "digital trade priorities" that it wants rules that would guarantee that "companies should not be forced to transfer their technology—including source code and proprietary algorithms—to competitors or governments." This is code for the type of source code provisions that would prevent governments from demanding access to source on behalf of the public interest. See U.S. Chamber of Commerce, "The Digital Trade Revolution," P. 19. Available at: https://www.uschamber.com/assets/documents/Final-The-Digital-Trade-Revolution-February-2022_2022-02-09-202447_wovt.pdf.

75 Calculations made using the TAPED dataset under the project 'The Governance of Big Data in Trade Agreements,' Universities of Lucerne and Bern. Accessed on 3 Oct. 2022. Available at: https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/.

76 Ulla-Maija Mylly, "Preserving the Public Domain: Limits on Overlapping Copyright and Trade Secret Protection of Software,". IIC 52, 1314–1337 (2021). Available at: https://doi.org/10.1007/s40319-021-01120-3; International Trade Union Confederation, op cit. P. 4.

These existing protections already are required by the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property, applicable to the entire WTO membership, which encompasses over 95% of the world economy.[77]

Industry's "digital trade" agenda would excavate the policy space out from under Congress and various U.S. agencies before governments can act while also undermining policies already enacted or being developed all over the world. The challenges and opportunities accompanying the growth of the digital economy have generated congressional and agency action aimed at protecting the public from online harms and ensuring that the benefits of the digital economy are widely distributed. The U.S. government is behind other countries in launching such initiatives. Tech interests are trying to derail algorithmic accountability efforts and other elements of the digital governance push. As governments sort out their own policies, it will be helpful to enhance cooperation between countries to deal with the key issues that these technologies pose. One thing that should not be on any agenda, much less slipped into trade agreements under the brand of "digital trade," are handcuffs on legislators, regulators, and courts as they tackle these challenges.

77 "Member states of the WTO: World Trade Organization," WorldData. Accessed 9 May 2022. Available at: https://www.worlddata.info/alliances/wto-world-trade-organization.php

The American Economic Liberties Project is a new, independent organization fighting against concentrated corporate power to realize economic liberty for all, in support of a secure, inclusive democratic society.

Rethink Trade was established to intensify analysis and advocacy regarding the myriad ways that today's trade agreements and policies must be altered to undo decades of corporate capture and to deliver on broad national interests.

economicliberties.us
@econliberties
info@economicliberties.us

rethinktrade.org
@rethinktrade
info@rethinktrade.org