rethink TRADE

AMERICAN ECONOMIC LIBERTIES PROJECT

DIGITAL TRADE BRIEFING PAPERS SERIES #1

Big Tech's "Digital Trade" Attack on Working People and Labor Rights

October 2022

RETHINK TRADE

rethinktrade.org

Introduction

The evolution of the internet, the development of artificial intelligence and the growth of the data economy are fundamentally transforming every aspect of our lives. These changes can lead to more efficient exchanges and worldwide diffusion of knowledge. Yet, unchecked and unregulated use of digital technologies has proven to be harmful for workers, as it enables employment discrimination, intrusive worker surveillance and job offshoring. Plus, huge corporations like Google, Facebook and Amazon undermine our privacy, spread misinformation and exploit their monopoly powers to crush business competitors. They use their powerful platforms and billions in lobbying spending to sway governments and influence elections. In the United States and around the world, governments are cracking down on Big Tech's ability to abuse workers, consumers and smaller businesses, while seizing the benefits of the digital revolution.

In response, these huge corporations are relentlessly fighting back. One under-the-radar strategy is trying to lock in binding international rules that handcuff governments and grant digital firms new powers and rights to skirt government regulation and public oversight. Big Tech firms seek to hijack trade negotiations and establish what they call "digital trade" or "ecommerce" agreements that would undermine Congress and U.S. agencies' ability to rein in their abuses. These Trojan Horse "digital trade" deals could derail the legislative and regulatory efforts now underway to finally impose some oversight on Big Tech corporations whose monopolistic power threatens too many aspects of our lives, including our employment opportunities, job security and the health of democracy itself.

Labor Law Violations and Employment Discrimination Enabled by Extreme Source Code Secrecy Protections

Artificial intelligence (AI) is everywhere nowadays. AI is the simulation of human intelligence in machines. These machines are programmed to "think" like humans so as to automate tasks, manage complex workflows and recognize patterns in large datasets to make predictions and decisions. Daily decisions around hiring and workplace management, consumer finance and access to public and private services, among many other things, are now made by AI. Computer programs follow a set of rules when certain data is used as an input; these rules that the computer follows, written in a way that humans can understand it, is called "source code."

When it comes to work, the ways in which AI systems operate are not obvious to experts. People often don't even know that decisions over essential aspects of their lives are been made by machines. Yet 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.[1]

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 — 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.[2]

AI programs also undermine workers' rights to organize unions and foster hazardous working conditions, growth in contingent work and loss of autonomy and privacy.[3]

AI-enabled surveillance technologies already have been used by companies like Walmart, Amazon, Google and HelloFresh with the intent of chilling union organizing.[4] 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.

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.[5] 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.[6]

Additionally, algorithmic hiring and recruitment software can replicate and deepen existing inequities. Certain individuals are systematically excluded from employment when source code

---

1 Annette Bernhardt, Lisa 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, 2021), 7. Available at: https://laborcenter.berkeley.edu/data-algorithms-at-work/.

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

3 Bernhardt, Kresge and Suleiman, 16.

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

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

6 National Employment Law Project and The Athena Coalition, Packaging Pain: Workplace Injuries in Amazon's Empire (2019), 3. Available at: https://workercenterlibrary.org/product/packaging-pain-workplace-injuries-in-amazons-empire/.

reflects the biases of its developers or when the algorithm is trained by inaccurate, biased or unrepresentative data.[7] 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.[8] This is not a negligible issue: Major employers such as Unilever, Hilton and Delta Air Lines use data-driven predictive hiring tools,[9] which inform decisions that could be exacerbating racial, ethnic and gender inequalities.

To sanction and prevent workplace discrimination, 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.[10] For certain AI applications in high-risk sectors, such as energy, healthcare, migration and social security, experts recommend careful review and prior authorization before these technologies are allowed to go to the market.[11]

To ensure the success of these policies, regulators and courts must have the ability to compel companies to disclose information about their AI system, including source code and the data being fed to the machine. However, Big Tech is pushing "digital trade" provisions that forbid governments from enacting laws or regulations that would require access to software source code, save for a few exceptions.[12] Such extreme source code secrecy provisions would gut government efforts to prevent and sanction AI abuses in the workplace and discriminatory employment, housing and banking practices. Such secrecy could also have negative impacts on other AI-facilitated decisions that affect many facets of our lives.

---

7 Jenny Yang, The Future of Work: Protecting Workers' Civil Rights in the Digital Age, Before the Civil Rights and Human Services Subcommittee, 5. Available at: https://edlabor.house.gov/hearings/the-future-of-work-protecting-workers-civil-rights-in-the-digital-age-.

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

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

10 Yang, 13; Bernhardt, Kresge, and Suleiman, 25-26.

11 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? (Amsterdam: University of Amsterdam School of Information Law, 2021), 25. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3786567.

12 Third World Network Briefings, Some preliminary implications of WTO source code proposal, 8. Available at: https://www.twn.my/MC11/briefings/BP4.pdf; 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/IMG/pdf/digital_chapters_and_the_impact_on_labour_en.pdf.

Workers' Privacy and Economic Security Undermined by Guarantees of Unfettered Data Flows Across Borders

The fuel for AI systems, and the digital economy generally, is data. Enormous amounts of personal and non-personal data are collected and built with every keystroke, click and Internet search. Data is also collected when we interact with objects that we use daily, such as home appliances or smart watches that monitor our vital signs. Until recently, the corporations running digital platforms have had free rein to move data across borders without any restrictions, process it wherever they choose and store the data wherever it is cheapest to do so. While the expansion of data flows can contribute to pandemic preparedness and medical research, there are many compelling reasons to regulate how certain kinds of data may be collected, where they can be processed or transmitted and how or where they are stored.

For starters, there is a growing consensus about the need to regulate the use and collection of personal data to protect consumers' privacy and the security of their personal data. The EU General Data Protection Regulation (GDPR) has begun to set a global standard. It requires that companies collecting or processing EU residents' data comply with fairly strict transparency, accountability and data minimization requirements.[13] Under the GDPR, firms must process data for the legitimate purposes for which it is collected, refrain from collecting more data than necessary, keep information accurate and updated and ensure that processing is done in a way that guarantees data security. Additionally, the EU mandates that data can only be transferred to locations where adequate standards of protection are in place.

Technological developments in big data analytics – which means the processing of copious amounts of data to uncover information – communications capture, DNA testing and biometrics have dramatically expanded employers' capability to surveille workers on and off the job. For instance, through productivity apps, employers collect broad swaths of workers' metadata, such as online search queries and social media activity. The output of predictive big data analytics programs, ostensibly promoting "worker wellness programs," allows bosses to amass employees' health information, including the prescription drugs they use or when they stop filing their birth control prescriptions.[14]

Consequently, experts have advocated in favor of a Workers' Bill of Rights for Algorithmic Decisions, modeled after the individual rights-based approach of the EU's General Data Protection Regulation privacy policy.[15] A bill of this nature would ensure that individuals are

13 Yang, 14.

14 Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, Limitless Worker Surveillance. (Berkeley: California Law Review, 2017), 129. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211.

15 Yang, 14.

notified when their employers collect and process their data through AI systems. Workers would have the right to consent to such collection, dispute the accuracy of the information and correct mistakes in the data collected. Workers could also have a say on whether they agree to be subject to decisions based solely on AI tools.

Given the potential abuses caused by digital surveillance, some have even called for policies that outright limit employers from collecting data based on excessive surveillance — such as workers' personal health data and off-the-job online activities.[16] Enforcing such obligations would undoubtedly require some limitations on data outflows for employers.

However, such pro-worker regulatory efforts could be undermined by the "digital trade" agenda. Corporate interests have pushed for the negotiation of international rules that guarantee "free flow" of data without constraint and forbid limitations on the location of computing facilities. Both of these "digital trade" rules would prevent governments from developing policies to protect consumers and workers with respect to where — and how — data is processed, stored or transmitted. Big Tech interests managed to get these rules inserted in the 2019 United States-Mexico-Canada Agreement (USMCA). Even today, U.S. trade officials in Geneva continue to insist on these terms, with support from other countries that are already bound to such rules in the Digital Economic Partnership Agreement (DEPA) and the Trans-Pacific Partnership (TPP), such as Australia, Singapore and Chile. These existing agreements must be changed to protect workers and consumers. Certainly, there must be no further guarantees for Big Tech to do whatever they want with our data.

Gig Workers' Labor Rights Threatened by Use of Trade Lingo Like Expansive "Non-Discrimination" Obligations

The "digital trade" framework reinforces the Original Sin of the "digital economy," namely, the notion that leading players in transportation, hospitality, retail, education, healthcare and other industries that provide services online are altogether different than their brick-and-mortar counterparts. And thus, the domestic policies that generally apply to help protect the rights of workers and consumers somehow do not "apply to" the online version of these businesses. This has allowed "digital trade" rules to label as illegal "trade barriers" requirements such as online ride-hailing companies meeting driver hours-of-service-rules and respecting limits on the number of active drivers. One trick is to use trade concepts, such as "non-discrimination." A common provision in existing "digital trade" deals forbids domestic digital policies that

16 E-Commerce Free Trade Agreements, Digital Chapters and the Impact on Labour, 26.

may have a "discriminatory effect."[17] That lingo captures neutral policies that may have a larger impact on firms that dominate a market.

For instance, in 2015, the Philippines became the first country to issue a regulation that mandated certain conditions for online ride-hailing businesses to be able to operate. The policy required companies like Uber to register with the Filipino transportation authorities as Transportation Network Companies (TNCs). TNCs are required to screen, accredit and register their drivers with the transportation authorities. Drivers are then authorized through a provisional authority with a temporary permit, valid for 45 days, or a certificate of public convenience franchise, which is valid for a year.[18] The Philippines later issued additional rules setting a maximum limit on surge pricing, after reports of customers experiencing fares that ranged from $40 to $530 U.S. dollars during the 2016 Christmas holidays.[19]

After repeatedly failing to comply with the driver permit requirement, much to the frustration of transportation authorities, Uber eventually exited the Philippines and sold its operation to local competitor Grab.[20] Despite the largest U.S. online ride-hailing company leaving the Filipino market, the U.S. government has been recruited by Big Tech interests to attack these policies affecting a market in which they no longer have a stake. The U.S. National Trade Estimate (NTE) report is a statutorily-required annual review issued by the Office of the United States Trade Representative (USTR), which has been used by corporations as a hit list of public interest policies they dislike. The report has included criticism of the Filipino drive-hailing regulations as a "barrier to digital trade." The 2021 NTE report, claims that the Philippines' "restrictive regulatory framework for transportation network vehicle services (...) reduce[s] the value that these services are able to provide to consumers and undermine the competitiveness of these services vis-à-vis local alternatives."[21]

Expanding the intrusive set of "digital trade" rules already included in certain agreements would only provide more footing for these kind of attacks.

17 See Article 19.4 of the United States-Mexico-Canada Agreement: "Non-Discriminatory Treatment of Digital Products: No Party shall accord less favorable treatment to a digital product created, produced, published, contracted for, commissioned, or first made available on commercial terms in the territory of another Party, or to a digital product of which the author, performer, producer, developer, or owner is a person of another Party, than it accords to other like digital products."

18 Katerina Francisco, "What's the fuss about Grab, Uber regulation issue?" Rappler, July 2017. Available at: https://www.rappler.com/newsbreak/iq/176933-you-need-to-know-fuss-grab-uber-ltfrb-regulation-explainer/.

19 Charles D.A. Icasiano and Araz Taeihagh, "Governance of the Risks of Ridesharing in Southeast Asia: An In-Depth Analysis", Sustainability 13, no. 11: 6474 (2021), 6. Available at: https://www.mdpi.com/2071-1050/13/11/6474/htm.

20 Ibid.

21 Office of the United States Trade Representative, National Trade Estimate Report on Foreign Trade Barriers (Washington D.C., 2021), 424.

Service Sector Job Offshoring Can Accelerate if "Digital Trade" Rules Don't Strongly Enforce Broad Labor Standards and Privacy Rules

In the past, the United States has negotiated self-standing "digital trade" agreements with other countries, such as Japan. With this practice — or any approach that does not link the negotiation of rules over the digital economy with strong and enforceable labor standards — "digital trade" deals could accelerate job offshoring and production outsourcing in the service sector, undermining worker and consumer interests.

Over the past few decades, major telecommunications companies, including T-Mobile, Verizon and AT&T, have closed call centers from Oregon to Florida to Maine to Texas. Many of these facilities had union contracts that ensured good wages and benefits. Major financial services firms — banks, insurance firms and others — have done the same, as well as several other service sector firms. By shipping call center jobs overseas in a race-to-the-bottom in wages and working conditions — often to countries where workers now face systematic attacks against unions, like the Phillipines — these companies have hurt the people and communities that depended on these jobs here in the United States, while maximizing profits in locations where basic rights to workers are denied.

The Communications Workers of America (CWA) union has denounced the abuses committed by the Filipino government against labor organizers in the call center industry[22] and, more generally, in the "business process outsourcing (BPO)" sector.[23] Filipino workers and union organizers are subject to physical threats, severe intimidation, arbitrary arrests, red-tagging and even extrajudicial killings just for attempting to form unions in call centers. More than 50 unionists have been killed under the regime of Philippines President Rodrigo Duterte. Large U.S. companies have actively ignored the Duterte government's labor rights violations.[24]

The U.S. Department of Labor's Trade Adjustment Assistance program, which lists a subset of offshored jobs, certified at least 13,491 workers just in major telecommunication firms as having lost jobs in trade-related outsourcing.[25] Other call center jobs, including those of major financial firms, have also been subject to this race-to-the-bottom offshoring.

---

22 "CWAers Build Global Solidarity to Lift Working Conditions for Everyone," Communication Workers of America, September 5, 2019. Available at: https://cwa-union.org/news/cwaers-build-global-solidarity-lift-working-conditions-for-everyone.

23 "CWA Strongly Opposes "Red-Tagging" of Labor Activists in the Philippines," Communication Workers of America, April 9, 2021. Available at: https://cwa-union.org/news/releases/cwa-strongly-opposes-red-tagging-of-labor-activists-in-philippines.

24 "Stand for Filipino Workers' Rights on December 10," Communication Workers of America, December 9, 2021. Available at: https://cwa-union.org/news/stand-for-filipino-workers-rights-on-december-10#:~:text=The%20international%20trade%20union%20movement,of%20Philippines%20President%20Rodrigo%20Duterte.

25 "Trade Adjustment Assistance Database," Public Citizen, extracted on Apr. 13, 2022. Available at: https://www.citizen.org/article/trade-adjustment-assistance-database/.

Much of the financial services job offshoring, as well as in accounting and medical diagnostic work, is profitable – and indeed possible – only because of the gaps in regulation regarding basic privacy protections and professional qualifications. Work related to privacy-protected information cannot be outsourced from European countries except to other locations with equally stringent privacy protections. A 2004 Public Citizen report, Addressing the Regulatory Vacuum: Policy Considerations Regarding Public and Private Sector Service Job Offshoring,[26] noted that many of the service sectors in which offshoring is most prevalent are strictly regulated in the United States on the federal or state levels. Currently, however, federal laws that require privacy safeguards for such information domestically do not prohibit such data from being moved offshore — or being protected if and when moved elsewhere. This means that the work associated with medical and financial information, subject to domestic privacy protections, can be offshored.

If "digital trade" agreements keep prohibiting limits on the movement of data, they would restrict efforts by Congress and state legislatures to fix this gap — for instance, by forbidding the transfer of financial, medical and other sensitive personal information, covered by domestic privacy protections, to offshore entities operating in countries that do not provide similar privacy protections like the European Union does. Such "digital trade" rules would also undermine other policies that would protect privacy and limit service sector offshoring. This includes establishing fines for U.S.-based companies if they have violated basic consumer safeguards, including privacy laws, by transferring work to offshore entities.

Bad "digital trade" deals that guarantee unfettered cross-border data flows and algorithmic extreme secrecy, while not including strong and enforceable labor standards, are likely to contribute to the service job offshoring trend.

Conclusion

If countries are to negotiate international rules to regulate the digital economy, these must be based on worker-centered high standards. They must address the true problems related to digitally enabled international trade that affect workers — such as the entry of hundreds of millions of uninspected packages through customs law loopholes. No new extreme source code secrecy protections should be added, and cross-border data guarantees must respect the policy space required to protect privacy and data security, among other societal objectives. Lastly, respect of internationally recognized labor rights must be a requirement to further integration in the digital economy.

26 Lori Wallach, Fiona Wright and Chris Slevin, Addressing the Regulatory Vacuum Policy Considerations Regarding Public and Private Sector Service Off-Shoring (Washington D.C.: Public Citizen, 2004), 1. Available at: https://www.citizen.org/wp-content/uploads/offshoringreport_final_071306_0.pdf.

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