AFL-CIO

**Testimony Before the**
**Subcommittee on Trade**
**U.S. House Committee on Ways & Means**
**118th Congress, Second Session**

**Eric Gottwald**
**Policy Specialist on Trade and Economic Globalization**
**AFL-CIO**

**Hearing on "Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules."**

**September 17, 2024**

Thank you, Chairman Smith and Ranking Member Blumenauer, for the opportunity to testify before your committee on "Protecting American Innovation by Establishing and Enforcing Strong Digital Trade Rules." This testimony is submitted on behalf of the American Federation of Labor and Congress of Industrial Organizations (AFL-CIO) and the 12.5 million workers represented by its 60 affiliated unions.

As the Biden administration continues to remake U.S. trade policy, we firmly believe its "worker-centered" approach must extend to digital trade and the digital economy by placing the needs of workers, consumers, and society ahead of the profits and interests of big technology companies. Accordingly, Ambassador Katherine Tai's decision to re-examine U.S. digital trade policy provides a vital opportunity to strike a better balance between promoting a robust digital economy and other vital public policy objectives.

To date, the digital chapters of recent U.S. trade agreements have prioritized securing increased market access and broad protections against emerging forms of regulation for its big technology firms with broad prohibitions against any government measures that could restrict corporations' ability to move, process, and store data as they see fit. By comparison, they make no reference to workers' rights and do not require governments to take any meaningful action to protect individuals' personal data.

While the digital transformation has driven real gains in communications, transportation, science, and beyond, it has also brought urgent challenges to the world of work and society, which democratic governments are only beginning to address.

Technology companies and other employers are increasingly supervising, surveilling, and even disciplining workers with automated artificial intelligence (AI) and algorithmic management systems that can shortchange workers' earnings, expose workers to unsafe workplace conditions, infringe on the right to form unions, and exacerbate employment discrimination. Platform companies like ride-hail and delivery services have promoted a new, exploitative model of

employment where so-called "gig" workers endure low earnings, uncertain work schedules, and no benefits. The digital transformation has enabled the corporate offshoring of whole new categories of jobs, including workers in call centers, information technology, back-office, and even health care through telemedicine. It also facilitates the privatization of public data and data services, costing jobs and undermining the quality of publicly delivered services. Many of these jobs are being shipped to countries where workers are paid poverty wages and face severe repression for organizing trade unions.

Outside the workplace, digitalization poses other threats to workers, consumers and people. The large technology companies collect, share, commodify, and sell tremendous amounts of personal data with little or no oversight. Digital apps and social media platforms have eroded personal privacy, undermined the mental health of adolescents, and provided a megaphone to anti-democratic and hateful forces that have corroded the social discourse.

As United States Trade Representative Katherine Tai stated in 2021, digital trade must be "grounded in how it affects our people and our workers" and provide space to "prioritize flexible policies that can adapt to changing circumstances" of rapidly evolving forms of digital commerce.[1] Achieving this vision will require a more balanced approach that preserves the right of governments to fully regulate the digital economy, while also driving greater cooperation to address the very real threats to privacy, democracy, and decent work.

## I. Preserving governments' right to regulate the digital economy

The rapid digital transformation of the economy has emerged largely without the knowledge, consent, or input of the people it most affects — the workers and consumers whose lives are increasingly governed, surveilled, and commodified by the technological revolution.

At a time when governments around the world are grappling with how to regulate emerging digital technologies, recent U.S. digital trade agreements have granted broad digital corporate rights while imposing rigid restrictions on the measures governments can adopt to promote legitimate public policy interests like protecting data privacy, ensuring emerging technologies comply with domestic labor laws, promoting competition, and more. These digital provisions mirror and amplify parallel efforts by Big Tech firms to avoid regulatory oversight in the United States and countries around the world.

The current digital trade model grants broad rights to technology and other companies to control, transmit, process, and store data worldwide, while also shielding their digital systems from regulatory scrutiny. For example, the USMCA and U.S.-Japan digital texts prohibit any restriction on cross-border data flows, with no exception for sensitive forms of personal information. Although the texts contain an exception for "measures necessary to achieve a legitimate public policy objective," in practice this language — which is borrowed from existing

[1] Tai, Katherine. Ambassador, Office of the U.S. Trade Representative, "Remarks of Ambassador Katherine Tai on Digital Trade at the Georgetown University Law Center Virtual Conference," November 3, 2021.

WTO agreements — has been narrowly interpreted by dispute panels and has not proven effective at safeguarding governments' right to regulate.

The USMCA also contains an absolute prohibition on "data localization" policies, which an increasing number of governments are adopting to require that some kinds of data be stored on domestic servers to protect digital privacy or ensure appropriate access for regulators and law enforcement. Unlike the prohibition on restrictions to cross-border data flows, it contains no "legitimate public policy" exception.

In addition, the USMCA adopts a broad prohibition on government access to or forced transfer of corporate source codes and algorithms as a condition for allowing the sale and distribution of digital products in a given country. While the text allows for disclosure on a case-by-case basis to a regulatory body or judicial authority, this is limited to a "specific investigation," which could preclude broader, industry-wide investigations necessary to address the harmful impact of algorithms, artificial intelligence, and machine learning on workers and people. The specific investigation clause also leaves it unclear how governments could initiate an investigation into, for example, employment discrimination and AI management software, without first having the broad authority to conduct an initial review of source codes to understand how they function and what their impacts are in the workplace.

The sweeping nature of these commitments is alarming given that most countries, including the United States, lack a comprehensive federal regulatory framework to address the downsides of digitalization on workers and society. The "legitimate public policy objective" exception lifted from the WTO has proven difficult for countries to invoke in practice, even with regard to sectors with long-standing, well-established regulatory regimes. Applying these restrictions to the fast evolving digital economy risks locking in an unregulated status quo that only benefits large technology companies and could undermine efforts to safeguard worker and consumer data privacy.

The rapidly evolving digital economy warrants new approaches to address the negative impacts of digitalization on workers, consumers, and society. The absence of domestic measures governing the digital economy heightens the importance that digital trade agreements must preserve robust public policy space. A worker-centered digital trade agenda must enshrine the right-to-regulate these new technologies to protect workers and consumers by enforcing current law and addressing emerging impacts on the workplace and society.

## II. Advancing a pro-active agenda to safeguard workers' rights, protect data privacy and security, and combat low-road digital offshoring.

In addition to preserving policy space to regulate, a worker-centered digital trade policy should also include positive commitments by governments to address the myriad of challenges connected to the digital transformation. Commitments to promote reliable, secure cross-border data flows must be offset by corresponding obligations to properly regulate the digital economy, including by addressing a range of issues that threaten workers' rights and privacy in and out of the workplace:

- **Ensure that digital trade agreements are subject to strong and enforceable labor standards:** Given the growing importance of the digital economy, it is essential that countries establish strong guardrails to avoid a race to the bottom in regulation and corporate conduct. Digital trade agreements must contain an obligation to respect the internationally recognized workers' rights contained in the 1998 International Labor Organization Declaration on Fundamental Rights and Principles at Work. In addition, they must contain strong monitoring and enforcement mechanisms to ensure government and corporate compliance.

- **Require governments to enact strong policies to safeguard individuals' personal data:** Governments should be able to adopt restrictions on cross-border data flows to protect the privacy and security of individuals' personal data. In our hyper-connected online world, consumers and workers' personal data is increasingly monitored, collected, shared, analyzed, and sold by companies without their knowledge, consent or oversight. The existing digital trade model promotes a voluntary form of corporate self-regulation that has proven inadequate to protect individuals' personal information. Digital trade policy should encourage rather than deter government efforts to safeguard individuals' personal data inside and outside the workplace.

- **Authorize governments to enact data localization policies with regard to certain categories of sensitive data:** While open data flows are essential to the modern global economy, not all data is the same. Governments should have the ability to require that individuals' sensitive personal information (medical, financial, and biometric data collected in the workplace) or data related to certain sectors (critical infrastructure, national security, law enforcement) be kept onshore to ensure it is subject to strong and enforceable privacy standards and effective government oversight.

- **Discourage low-road digital offshoring:** Safeguarding critical, vulnerable, and personal data not only protects the security of people and the economy, but it also helps keep good jobs here in the United States. Big Tech companies and other employers have demanded unfettered cross-border data flows, in part, to facilitate the offshoring of digitally enabled back office, call-center, data processing, telemedicine and other jobs. Many of these jobs are going to countries with weak data protection regimes and widespread labor rights abuses. For example, tens of thousands of Communications Workers of America (CWA) members have lost call center jobs due to digital offshoring to countries like Mexico and the Philippines.[2] Digital trade agreements should actively discourage this type of low-road offshoring that lowers labor standards, while also placing customers' data at greater risk.

- **Facilitate meaningful oversight of source codes and algorithms to ensure compliance with labor and employment laws:** Employers are increasingly using automated, algorithmic systems to hire, manage, control, monitor, discipline, and even fire workers

[2] Sainato, Michael. "'They're liquidating us': AT&T continues layoffs and outsourcing despite profits." The Guardian. August 18, 2018

largely without the knowledge, consent or input of workers or unions. These new employer tools can undermine workers' rights, compromise workplace safety, violate wage and hour laws, and discriminate against protected classes of workers in hiring, promotion, or termination. Women, people of color, and immigrants are particularly at-risk, as they are more likely to be employed in lower-wage workplaces where these technologies are widely deployed.

Millions of workers in the United States already face challenges from algorithmic management. Amazon's algorithmic warehouse productivity software has created inhumane working conditions where workers are punished for taking bathroom breaks and suffer far higher serious injury rates. Some school districts have been using algorithmic tools to evaluate teachers based on how students perform on tests and to discipline and even fire teachers whose students failed to measure up to a computer modeled test score target. Automated monitoring of call center workers can incorrectly punish agents for allegedly straying from their scripts because the speech recognition software can discriminate against workers with accents, dialects, or different speech tones. In the retail and food service sectors, employers are increasingly using algorithmic "just-in-time" scheduling software that has led to erratic working schedules, unpredictable pay, and threatened health care benefits.

A worker-centered digital trade agenda must ensure that companies are held accountable for the risks associated with automated systems that implement critical decision-making protocol. It should be mandatory for companies to disclose to governments the impact assessments of their automated systems to ensure they are compliant with existing labor and employment laws. In addition, it should facilitate intergovernmental cooperation to address the risk that AI management software is undermining worker safety, wage and hour laws, and anti-discrimination laws.

- **Address emerging threats to workers' privacy, including employer use of workplace surveillance software:** Employer use of digital workplace surveillance tools has skyrocketed during the pandemic with the rise of telework. Workers have little protection from digital workplace surveillance including vehicle telemetry, hand-held equipment that evaluates work speed, keystroke and camera monitoring, and even surveillance of workers' social media presence to assess union sympathies. Employer use of these tools can contribute to workplace safety problems, lead to anti-union coercion and retaliation, and erode worker privacy. A worker-centered trade agenda should require governments to adopt measures to address digital workplace surveillance and other emerging threats to workers' privacy. For example, employers should be required to disclose their use of surveillance tools, what kind of data is collected and for what purpose, whether the data is sold to or shared with third parties, and provide a right for the employee to review and correct any inaccuracies.
- **Address abusive employment practices in the technology sector:** Large technology and platform companies like Uber and Facebook have promoted an exploitative employment model based on rampant employment misclassification and the outsourcing

of core job functions. Hidden behind social media platforms and popular digital assistants like Siri or Alexa are an army of outsourced "ghost workers" who code and enter data, transcribe digital assistant audio recordings, and monitor online platforms for violent and offensive content. These workers, many of whom work in developing countries, are essential to training AI algorithms and keeping hateful and offensive content off social media platforms. Platform gig workers and the ghost workers that power AI systems are employed as precarious contractors with no benefits, sick leave, guaranteed minimum wages, or the ability to form unions and bargain collectively. A worker-centered digital trade approach would require big technology companies to eliminate the labor abuses in their own operations and supply chains.

- **Protect and promote the economic security of creative professionals in the U.S.:** A worker-centered approach to digital trade must protect and promote the economic security of the more than 5 million people who work in the motion picture, television, music, and other parts of the creative sector. Many of these workers earn collectively bargained pay and contributions to their health insurance and pension plans from the sales and licensing of the copyrighted works that they help create. Digital trade policy must aggressively address the stolen or unlicensed use of copyrighted content on digital platforms and avoid replicating the outdated, overbroad copyright safe harbor exclusions that exist in some U.S. laws. In addition, it should promote the "no collection without distribution" principle to address the unfair practice by some countries of collecting royalties based on the work of U.S. creative professionals without passing it on to the artists, depriving them of rightful compensation for the use of their work.
- **Stop the misappropriation of voices, images, and likenesses for use in AI-generated digital content:** It is already clear that there are the dangers and downsides to AI, including image-based sexual abuse, misappropriation for commercial gain, and the proliferation of "deepfake" videos where the digital likeness of one person – usually a celebrity – is transposed onto another the body of another individual without their consent. Digital trade policy must ensure that there are safeguards against these abuses, while also holding online platforms accountable for unlawful user content they themselves facilitated or profit from.
- **Address the rise of cybercrime by both state and private actors:** In 2014, the U.S. charged several Chinese military members with hacking multiple U.S.-based companies and the United Steelworkers. In 2019, the International Brotherhood of Teamsters (IBT) experienced a ransomware attack demanding $2.9 million that forced the union to rebuild computer servers. Digital trade policy must strive to improve cyber security and create a common enforcement agenda to hold the criminals and companies that facilitate these crimes accountable.

## III. Conclusion

Too often, the debate over digital trade is unhelpfully framed as a binary choice between authoritarian digital censorship or the unregulated status quo where companies are largely free to collect, analyze, process, and sell workers and consumers' private data as they see fit. The labor movement rejects this false choice and instead calls for a new democratic, stakeholder-driven approach to data governance that addresses the negative impacts of digitalization on workers, consumers, and society.

To date, U.S. "digital trade" agreements have sought to expand market access for large technology companies by granting broad digital data and IP rights while narrowly constraining the ability of governments (both the United States and our trade partners) to adopt measures to address the digital economic transformation. This combination of broad corporate rights and limited domestic governance threatens to lock-in the current unregulated digital environment that poses significant risks to workers and society.

The Biden administration's worker-centered trade policy is a major opportunity to correct for this narrow, corporate approach to allow for broader policy space to protect personal data, strengthen economic security, protect domestic jobs, and tackle the downsides of the digital transition on workers, consumers, and society. As democracies seek to create a digital economy that is fair and inclusive, digital trade policy must also evolve to facilitate new forms of domestic and international regulation and oversight of the digital economy.