Testimony Before the
Subcommittee on International Trade, Customs, and Global Competitiveness
U.S. Senate Finance Committee
117th Congress, Second Session

Patrick Woodall
Policy & Research Director
AFL-CIO Technology Institute

Hearing on "Opportunities and Challenges for Trade Policy in the Digital Economy."

November 30, 2022

Thank you, Chairman Carper and Ranking Member Cornyn, for the opportunity to testify before your committee on "Opportunities and Challenges for Trade Policy in the Digital Economy." This testimony is submitted on behalf of the AFL-CIO Technology Institute and the American Federation of Labor and Congress of Industrial Organizations and the 12.5 million workers represented by its 58 affiliated unions.

The digital transformation of the economy has generated real societal gains — with significant scientific, communications, healthcare, commercial, and other advances — but also raised urgent challenges for workers and society. This rapid technological change 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 digital revolution. The U.S. Congress and U.S. regulators as well as governments worldwide are only beginning to confront these challenges.

Digital commerce and cross-border digital trade affects people at work and at home as technologies become built into workplaces and daily life. Digital commerce and digital trade covers any services or products that are delivered over the internet. Much of this is consumer facing content or services like e-books and movies, email services, smartphone apps, and software downloads. But it also concerns the backbone of e-commerce (everything except the delivery of goods purchased online), global cloud computing, and the big data services that undergird an increasing portion of big business operations and impact workers on and off the job.

The forces of global digital commerce are dramatically affecting millions of workers whether they know it or not. These workers include back-office and call-center workers that can lose their jobs from digital offshoring to countries where workers are paid poverty wages and face severe repression for organizing trade unions. They include workers whose jobs are managed or controlled by automated software that hires, rates, fires, schedules, and prods them to work faster to hit

ramped up productivity targets. These technologies can shortchange workers' earnings, expose workers to unsafe workplace conditions, infringe on the right to form unions, and exacerbate employment discrimination. Digital trade includes low-paid workers who toil for platform companies that assign tasks, set pay rates, and impose unaccountable discipline on "gig" workers who endure low earnings, uncertain work schedules, and no benefits. And workers everywhere who are monitored on and off the job by their employers.

Working families face the threats of digitization outside the workplace as well. 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.

The digital trade rules set the parameters of how governments can address these global data flows and cross-border software that affects workers, consumers, and society. The current digital trade rules, included in the U.S.-Mexico-Canada Agreement and the U.S.-Japan digital trade agreement, grant broad powers to the companies that control these technologies and data and set stringent prohibitions against government efforts to curb the demonstrable excesses of the digital economy.

There needs to be a new way forward for digital trade that prioritizes workers and people and not just the technology industry. 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] This requires 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.

A new worker-centered approach to digital trade 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. The absence of domestic measures governing the digital economy heightens the importance that digital trade agreements must preserve robust public policy space.

This testimony describes the significant problems with granting broad powers to cross-border digital trade while narrowly constraining government oversight in the context of trade approaches of other sectors (Section I). It discusses the issues around digital trade provisions on cross-border data flows and data localization (Section II), source codes and algorithms (Section III), and other digital trade issues that impact workers and society (Section III).

.

I. Existing digital trade rigid constraints on domestic governance are inappropriate because digital is different

The past three decades of globalization and international trade have cost millions of American manufacturing and service sector jobs and contributed to the widening economic and racial

[1] Tai, Katherine. (Ambassador Tai). 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.

inequality in the United States. Prior trade agreements focused on the shipments of physical goods and cross-border services but also addressed so-called regulatory non-tariff barriers to trade that affected goods and services. These trade provisions were adopted long after industrialized countries had established regulatory structures designed to protect workers, consumers, the environment, and communities from unsafe workplaces, dangerous products, and pollution.

But the current provisions in digital trade are fundamentally different. First, they grant broader powers to the technology companies and employers that deploy digital technologies and ship data worldwide than have previously been included in trade provisions. Second, the digital trade language sets far narrower constraints on government oversight of these cross-border data and technology transactions and transmissions than in other sectors. The combination of these two elements delivers a far more unbalanced combination of unilateral corporate power for Big Tech with far more rigid constraints on domestic oversight of the ubiquitous technologies and data that govern workers' lives at home and on the job.

Critically, existing U.S. digital trade provisions are delivering these broad cross-border corporate powers unfettered by government regulation when the United States and many trading partners have almost no regulatory structures to address the excesses of the technology industry. The United States has only a patchwork of laws and rules that govern Big Tech business models and expanding the current digital trade model would effectively lock-in an unregulated technology sector with little or no meaningful oversight. The technology companies have pushed for tough digital provisions to "lock-in their political power in international rules that are difficult to change," according to a 2016 London School of Economics paper.[2] Providing meaningful public policy space that is not curtailed by digital trade provisions is especially crucial for the new and novel concerns that are rapidly impacting workers and society.

Trade agreements infringe on domestic governance: Trade agreements were designed to reduce barriers to cross-border shipments of goods, largely import tariffs and quotas but increasingly domestic regulations that are deemed so-called non-tariff barriers. Over the past three decades, tariffs were substantially reduced or eliminated through multilateral or bilateral trade agreements. In the United States, this led to a dramatic surge in imports that cost millions of U.S. manufacturing jobs and created far more vulnerable supply chains.[3] Unlike physical goods, there has been a tariff moratorium on cross-border data flows, electronic transmissions, and e-commerce transactions since 1998.[4]

The trade agreements since the 1990s have also aimed to curb domestic regulations that purportedly act as non-tariff barriers to cross-border trade. The World Trade Organization and other bilateral agreements constrained domestic governance over workplace safety, the environment, food safety, regulatory standards and more. These agreements imposed significant limitations on governments'

---

[2] Azmeh, Shamel and Christopher Foster. London School of Economics. "The TPP and the Digital Trade Agenda: Digital Industrial Policy and Silicon Valley's Influence on New Trade Agreements." Working Paper No. 16-175. January 2016 at 7.

[3] Scott, Robert E. and Zane Mokhiber. Economic Policy Institute. "Growing China Trade Deficit Cost 3.7 million American Jobs between 2001 and 2018." January 30, 2020; Acemoglu, Daron et al. National Bureau of Economic Research. "Import Competition and the Great U.S. Employment Sag of the 2000s." Working Paper No. 20395. August 2014.

[4] Farge, Emma. "WTO provisionally agrees to extend e-commerce tariff moratorium — sources." *Reuters*. June 16, 2022.

ability to implement policies that can affect trade and brought domestic governance under the disciplines of trade dispute settlement.

Trading partners can demand that domestic policies (or measures, in trade language) be assessed to determine whether they pose illegitimate trade barriers. These evaluations are significantly biased against the ability of governments to establish domestic policies to protect workers, consumers, communities, or the environment. Policies are evaluated on a series of trade tests (the legitimacy and necessity of the measure, the trade restrictiveness or whether a less protective measure would facilitate more trade, and whether the measure poses arbitrary or unjustified non-discrimination, including whether it is a disguised trade restriction).

These policy caveats have proven difficult for countries to invoke in practice, even for sectors with long-standing, well-established regulatory regimes. At the World Trade Organization (WTO), fewer than 5 percent of domestic measures that were challenged as illegal trade barriers were upheld in trade disputes as trade-legal under these regulatory exceptions.[5]

The prior trade agreements' approach to domestic regulations over goods and services were built upon an architecture of long-standing domestic regulatory regimes in countries like the United States. Even the severe bias against domestic regulations often contained language that affirmatively granted the right to regulate and established guidelines for evaluating domestic regulations to purportedly ensure they were consistent with the international commitments.[6] These approaches at least recognized that global trade commitments interacted with robust domestic regulatory policies.

Digital trade provisions include tough proscriptions against domestic governance: The existing digital trade provisions grant more powerful constraints on domestic policymaking in an environment where there is little or no regulatory oversight of the technology sector. The technology industry generally views all efforts to regulate digital commerce and trade — including in areas like privacy protection and national security — as illegitimate trade barriers motivated more by parochial protectionism than by legitimate public policy concerns.[7]

Many USMCA and the U.S.-Japan digital provisions include prohibitions against domestic regulations. For example, the agreements dictate that "no party shall prohibit or restrict" cross-border data flows,[8] "no party shall require" local data storage,[9] "no party shall require" access to software source codes,[10] and "no party shall adopt or maintain" policies that hold platforms accountable for the content posted on their networks.[11]

---

[5] Rangel, Daniel. Public Citizen's Global Trade Watch. "WTO General Exceptions: Trade Law's Faulty Ivory Tower." January 2022.

[6] For example, the WTO Sanitary and Phytosanitary Agreement Art. 2.1 gave members "the right to take sanitary and phytosanitary measures necessary for the protection of human, animal or plant life or health, provided that such measures are not inconsistent with the provisions of this Agreement.

[7] Horowitz, Jeff. "U.S. International Trade Commission's Digital Trade Roundtable: Discussion Summary." *Journal of International Commerce and Economics*. October, 2015 at 3.

[8] U.S.-Mexico-Canada Agreement (USMCA) Art. 19.11.1; U.S.-Japan Digital Trade Agreement (U.S.-Japan). Art. 14.11.1

[9] USMCA Art. 19.12; U.S.-Japan Art. 12.

[10] USMCA Art. 19.16.1; U.S.-Japan Art. 17.1.

[11] USMCA Art. 19.17.2; U.S.-Japan Art. 18.2.

This digital language begins with broad prohibitions against domestic governance which sets a presumption that any domestic laws or regulations to safeguard workers or consumers from the excesses of the technology industry could be deemed illegal trade barriers. Some provisions contain the same weak trade policy caveats (legitimate, necessary, minimally trade restrictive, and disguised protectionism) that make it harder to establish domestic policies to protect workers and consumers from the downsides of digitization.[12]

The significant constraints on domestic governance could make it easier for trading partners to challenge any future regulatory efforts to rein in the technology industry and protect workers and consumers. This effectively would lock-in the current absence of regulatory oversight of Big Tech in the United States.[13]

Constraint of governance over unregulated technology: The United States has a patchwork of largely outdated statutes and regulations that fail to protect people and workers from the potential abuses of the digital world. Federal laws protecting personal data cover some specific areas (like medical information, credit, or financial data), but do not require companies to notify or compensate people if their personal information is shared or sold or exposed to unauthorized parties through cybercrime or data breaches.[14] Many of the laws are outdated for today's digital world.[15] For example, the rules that absolve platforms and social media companies from responsibility from users promoting hate speech and disinformation were implemented during the age of dial-up modems.[16]

There are effectively no regulations overseeing the impact of algorithmic management, and workers have little protection or recourse from digital surveillance on or even off the job.[17] Automated recruiting, hiring, and promotional decisions can have disproportionate or disparate impact on people of color, women, people with disabilities, older people, immigrants, or other protected classes, but the application of civil rights statutes to new and emerging digital technologies remains murky.[18]

The public and the Congress recognize that this Big Tech Wild West is not working for people or society. An increasing majority of the public favors more regulation of technology and technology

---

[12] USMCA Art. 19.11.1 and U.S.-Japan Art. 11.1.

[13] Azmeh, Shamel, Christopher Foster, and Jaime Echavarri. (Azmeh, Foster & Echavarri). "The international trade regime and the quest for free digital trade." *International Studies Review*. Vol. 22. 2020 at 684.

[14] Klosowski, Thorin. "The state of consumer data and privacy laws in the US (and why it matters)." *New York Times*. September 6, 2021.

[15] Kerry, Cameron F. Brookings Institute. "Why Protecting Privacy is a Losing Game Today—And How to Change the Game." July 12, 2018.

[16] The Digital Millennium Copyright Act of 1998. 17 USC §512.

[17] Bernhardt, Annette, Lisa Kresge, and Reese Suliman. (Bernhard, Kresge & Suliman). University of California Berkeley Labor Center. "Data and Algorithms at Work: The Case for Worker Technology Rights." November 2021 at 2; Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. (Ajunwa, Crawford, and Schultz). "Limitless worker surveillance." *California Law Review*. Vol. 105. 2017 at 747 to 749.

[18] Yang, Jenny R. Urban Institute. (Yang). Statement before the Subcommittee on Civil Rights and Human Services. Committee on Education and Labor. U.S. House of Representatives. "The Future of Work: Protecting Workers' Civil Rights in the Digital Age." February 5, 2020 at 8 to 11.

companies, especially related to protecting privacy and curbing monopolistic market power.[19] The House Energy and Commerce Committee passed digital privacy legislation nearly unanimously in July 2022 and released a bipartisan statement flagging the legislation's goal to "rein in Big Tech's power and establish clear, robust protections for people."[20] Bipartisan legislation to address Big Tech's monopolistic and anticompetitive power has passed the Senate and House Judiciary committees but has faced a withering and misleading advertising campaign to derail the legislation.[21] The existing digital trade language would create a very high barrier to implementing and enforcing these laudable congressional efforts.

The existing digital trade provisions constraints on domestic governance harm workers, consumers, and society. The following sections describe how the combination of broad corporate powers for Big Tech companies and stringent regulatory restrictions could lead to increased offshoring of U.S. jobs, make it harder to enforce current labor, employment, and civil rights laws against artificial intelligence algorithmic management and automated decision-making, and prevent governments from adopting safeguards to address emerging technological issues, such as workplace surveillance.

II. Workers harmed by free flow of data and data localization digital trade provisions that accelerate job offshoring and prevent protecting critical data and sectors

The current digital trade model grants broad powers to technology and other companies to control, transmit, process, and store data worldwide, while also shielding their digital systems from regulatory scrutiny. These provisions prohibit any restriction on cross-border data flows — even for sensitive forms of personal information — as well as an absolute prohibition on "data localization" policies. Together, these two provisions grant companies a near unrestricted right to control data and ship it worldwide. The globalization of data has led to the outsourcing and offshoring of U.S. jobs, the increasing privatization of government datasets that reduces public access and raises costs, and the collection of vast troves of personal data compromises the privacy of workers on the job and people at home.

Tech industry demands and existing digital provisions deliver unfettered free flow of data: The technology industry and other big businesses have pressed for digital trade provisions that largely prohibit any impediments to cross-border data flows. The U.S. technology industry has pressed hard for free flow of data because the biggest cloud computing firms are based in the United States.[22] The U.S. Chamber of Commerce listed unfettered cross-border data flows as its top digital

[19] Vogels, Emily A. Pew Research Center. "56% of Americans support more regulation of major technology companies." July 20, 2021; Brenan, Megan. Gallup "Views of Big Tech worsen; public wants more regulation." February 18, 2021.

[20] U.S. House of Representatives. Energy & Commerce Committee. [Press release]. "Bipartisan E&C Leaders Hail Committee Passage of the American Data Privacy and Protection Act." July 20, 2022.

[21] Feiner, Lauren. "Senate committee votes to advance major tech antitrust bill." *CNBC*. January 20, 2022; McKinnon, John D. "Big Tech has spent $36 million on ads to torpedo antitrust bill." *Wall Street Journal*. June 9, 2022; Wheeler, Tom. Brookings Institute. "History repeats itself with Big Tech's misleading advertising." June 15, 2022.

[22] Fefer, Rachel F., Shayerah I. Akhtar, and Michael D. Sutherland. (Fefer, Akhtar & Sutherland). Congressional Research Service. "Digital Trade and U.S. Trade Policy." CRS Report R44565. December 9, 2021 at 17.

trade priority.[23] The industry promotes the unrestricted right for companies to transfer data across borders as a tool to counter authoritarian internet censorship,[24] but that does not mean that all data — including personal, sensitive, or secure — should have no restrictions or requirements when crossing borders.[25]

These industry demands are enshrined in existing digital trade language that provide a nearly unrestricted, unconditional right for cross-border data collection, transmission, and use. The USMCA and U.S. Japan digital agreement both contain nearly absolutist language on data flows: "No Party shall prohibit or restrict the cross-border transfer of information" and it specifically includes "personal information" in this protected right to ship data worldwide.[26] This prioritizes corporate data ownership and control over the privacy rights of workers and consumers.

The USMCA and the U.S.-Japan cross-border data flow provisions contain only narrow caveats for permissible government measures that must be necessary, legitimate, not disguised restriction to trade, or more trade restrictive than necessary.[27] These policy exceptions are borrowed from the WTO, where dispute panels have narrowly interpreted these caveats and constrained governments' right to regulate. The current digital provisions would make it very difficult for governments to maintain or adopt rigorous measures to address the negative impacts of unrestricted data flows on workers or consumers.

Prohibitions on data localization can harm workers, consumers, and the economy: The USMCA and U.S.-Japan digital provisions also contain an absolute prohibition on "data localization" policies. Data localization measures require that data generated within a country must meet certain requirements including domestic data storage.[28] An increasing number of governments are requiring that some kinds of data be stored on domestically to protect digital privacy or secure critical infrastructure.

The USMCA and U.S.-Japan data localization provisions broadly prohibit countries from requiring companies "to use or locate computing facilities in that party's territory as a condition for conducting business."[29] Unlike the prohibition on restrictions to cross-border data flows, neither digital agreement contains a "legitimate public policy" exception, although both agreements exclude financial services from the data localization provisions.[30]

While some data localization policies have been established to foster domestic capacity or protect domestic industries, many "localization policies may be used to achieve legitimate public policy objective, including national security and personal data protection," according to the Congressional

---

[23] U.S. Chamber of Commerce. "The Digital Trade Revolution: How U.S. Workers and Companies Can Benefit from a Digital Trade Agreement." February 2022 at 18.

[24] Cory, Nigel, Robert D. Atkinson, and Daniel Castro. Information Technology & Innovation Foundation. "Principles and Policies for 'Data Free Flow with Trust.'" May 27, 2019.

[25] McCann, Duncan. (McCann). New Economics Foundation. For the International Trade Union Confederation. "Free Trade Agreements, Digital Chapters and the Impact on Labor." 2019 at 16.

[26] USMCA Art. 19.11.1 and U.S-Japan Art. 11.1.

[27] USMCA Art. 19.11.2 and U.S.-Japan Art. 11.2.

[28] Azmeh, Foster & Echavarri. 2020 at 677.

[29] USMCA Art. 19.12; U.S.-Japan Art. 12.1.

[30] USMCA Art. 19.1; U.S.-Japan Art. 12.2.

Research Service.[31] Localization requirements can also prevent companies from moving data to countries with the weakest privacy or financial protections in a digital race-to-the-bottom that could shield information from regulatory oversight.[32]

The combination of the unfettered right to ship data across borders and prohibitions against maintaining domestic data storage to secure some categories of sensitive data or some critical economic sectors can harm consumers, workers, and the economy. For example:

- ***Digital trade provisions compromise personal privacy:*** 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. Privacy issues are inherently tangled with digital trade issues by companies that collect and ship personal data across borders.[33] Tech companies view privacy measures that keep critical data either within national borders or subject to stronger oversight requirements as "impediments to the presence and productivity of their companies in these countries and to international trade," according to companies at a U.S. International Trade Commission forum.[34] The Office of the U.S. Trade Representative (USTR) has identified consumer privacy measures as potential or likely trade barriers and unreasonable impediments to the cross-border flow of data, including laws in Canada, EU, India, Israel, Korea, and Switzerland.[35]

  The USMCA and U.S.-Japan digital provisions explicitly state that even the cross-border transmission of "personal information" cannot be prohibited or restricted.[36] The agreements purportedly permit policies to safeguard personal information but effectively encourage voluntary, corporate self-regulation as a substitute for government privacy regulations.[37] But voluntary, self-regulation is what consumers face today and it is not working. The Big Tech companies that own the personal data already have "privacy" policies but have nonetheless exposed users to cyber-risks while monetizing the data they collect.[38] The digital trade personal information provisions also require regulatory approaches be "necessary and proportionate to the risks,"[39] but do not recognize that consumers, not the companies, bear all the digital privacy risks. This prevents the enactment of any meaningful privacy protection, because it can be difficult to put a financial value on privacy and security from cyber breaches.[40]

---

[31] Fefer, Akhtar & Sutherland. 2021 at 16.

[32] Kelsey, Jane. Public Services International. "Digital Trade Rules and Big Tech: Surrendering the Public Good to Private Power." February 2020 at 14 to 15.

[33] Azmeh, Foster & Echavarri. 2020 at 682.

[34] Horowitz, Jeff. "U.S. International Trade Commission's Digital Trade Roundtable: Discussion Summary." *Journal of International Commerce and Economics*. October, 2015 at 4.

[35] Office of the U.S. Trade Representative (USTR). "2021 National Trade Estimate Report on Foreign Trade Barriers." March 2021 at 89, 209, 266, 289, 332,

[36] USMCA Art. 19.11.1; U.S.-Japan Art. 11.2.

[37] USMCA Art. 19.8.2 footnote 4; U.S.-Japan Art. 15.1 footnote 12.

[38] Warzel, Charlie and Stuart A. Thompson. "Tech companies say they care." *New York Times*. April 10, 2019.

[39] USMCA Art. 19.8.3; U.S.-Japan Art. 15.4.

[40] Estevadeordal, Anton, Marisol Rodriguez Chatruc, and Christian Volpe Martincus. Inter-American Development Bank. "New Technologies and Trade: New Determinants, Modalities, and Varieties." Discussion Paper No. IDB-DP-00746. February 2020 at 25.

- ***Current digital provisions contain no exceptions for critical infrastructure:*** The USMCA and U.S.-Japan data provisions do not exclude critical infrastructure.[41] Failing to exempt critical infrastructure from the cross-border data and data localization provisions could make it harder to protect essential economic sectors from cyberattacks. In 2021, a cyberattack against one of the biggest pipeline systems on the East Coast led to gas lines and threatened to idle downstream industry like chemical companies and refineries.[42] Another 2021 hack of a Florida water system remotely elevated the levels of a dangerous chemical in the water; the operator fortunately noticed the change and quickly prevented the hack from tainting the water supply.[43] The Government Accountability Office has highlighted the environmental and economic risks of the cyber vulnerability of 1,600 U.S. offshore oil and gas rigs.[44] Some companies and countries are moving towards domestic data hosting for critical infrastructure to increase security and accountability for systems like electricity and water delivery.[45]

- ***Digital trade data provisions encourage low-road digital offshoring*:** 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. According to a 2021 report commissioned by Facebook, "If transferring personal data were not permitted, offshoring business services to popular outsourcing destinations would no longer be possible."[46] This kind of digital outsourcing has eliminated U.S. jobs and cost workers their benefits.[47] One call-center outsourcing company promotes a list of nearly 30 major corporations — including financial and telecommunications firms — that outsource their call centers.[48] AT&T shuttered 44 call centers costing 16,000 unionized Communications Workers of America (CWA) jobs from 2011 to 2018, despite record profits.[49] A 2018 Labor Department investigation found that Wells Fargo slashed thousands of U.S. customer service and technology jobs while hiring overseas workers to replace the exact same functions.[50]

  Many of these jobs are going to countries where workers and union activists face severe repression and toil for low wages with few labor protections. For example, many of the CWA call center jobs have been digitally offshored to countries like Mexico and the Philippines.[51]

---

[41] The Comprehensive and Progressive Agreement for Trans-Pacific Partnership, to which the United States is not a party, did exempt critical infrastructure from the agreement's software secrecy provisions. CPTTP Art. 14.17.2.

[42] Sanger, David E. and Nicole Perlroth. "Pipeline attack yields urgent lessons about U.S. cybersecurity." *New York Times*. June 8, 2021.

[43] Margolin, Josh and Ivan Pereira. "Outdated computer system exploited in Florida water treatment hack." *ABC News*. February 11, 2021.

[44] Government Accountability Office. "Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure." GAO-23-105789. October 26, 2022.

[45] "Mitigating risks through sovereign data services." *CRN News*. November 21, 2022.

[46] Kepes, Roze, Josh White, and Aaron Yeater. Analysis Group for Facebook. "The Importance of Cross-Border Data Flows." June 2021 at 4.

[47] Chakraborty, Kalyan and William Remington. "Impact of offshore outsourcing of IT services on the U.S. economy." *Southwestern Economic Review*. 2004.

[48] Magellan Solutions. "List of companies that outsource call centers." Accessed March 2022.

[49] Sainato, Michael. "'They're liquidating us': AT&T continues layoffs and outsourcing despite profits." *The Guardian*. August 18, 2018; Communication Workers of America (CWA). "AT&T 2018 Jobs Report." April 25, 2018.

[50] Moise, Imani. "Wells Fargo moves jobs abroad after U.S. layoffs, government says." *Reuters*. December 20, 2018.

[51] CWA. "Offshoring Security." October 2013; CWA. [Press release]. "CWA uncovers massive Verizon offshoring operation in Philippines." May 13, 2016.

The digital trade data provisions also help maintain a global underclass of low-paid gig workers who transcribe, enter data, label images, and manually tag information that powers the artificial intelligence systems of the biggest tech companies.[52] Many of these millions of ghost workers are in Indo-Pacific Economic Framework countries India and the Philippines where they receive low pay and precarious labor conditions.[53] Companies in the United States are the biggest employers of digital gig workers in the developing world according to data compiled by the University of Oxford.[54]

A worker-centered digital trade agenda would establish critical safeguards for workers, consumers, and the economy: Future digital trade agreements must provide robust public policy space to protect workers, consumers, and the economy. The current digital provisions excessively constrain domestic policy and do not provide necessary flexibility to address emerging and novel technological issues. At a minimum, the cross-border data and data localization provisions of future digital trade agreements or compacts should:

- **Authorize and encourage governments to enact 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 their citizens' personal data. 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 establish stronger requirements for data related to certain sensitive sectors or personal information, including critical infrastructure (energy, water systems, transportation), national security, law enforcement, health care, finance, and other areas where a data breach or disruption risks undermining economic or national security. 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.

III. Workers harmed by source code and algorithm digital trade provisions that set high barriers to address corrosive impacts of boss-ware

Current U.S. digital trade agreements include broad prohibitions on government access to and oversight of the source codes and algorithms behind the automated decision-making and artificial intelligence systems that are increasingly impacting the workplace and society. The provisions purport to be focused on preventing the forced transfer of software secrets as a condition for market access, but the strong, binding source code and algorithm protections pose significant challenges for effective government oversight.[55]

---

[52] Friedland, Julian, David Balkin, and Ramiro Montealegre. "A ghost workers' bill of rights: How to establish a fair and safe gig work platform." *California Management Review*. January 7, 2020.

[53] Royer, Alexandrine. Brookings Institute. "The urgent need for regulating global ghost work." February 9, 2021.

[54] Kässi, Otto and Vili Lehdonvirta. Oxford Internet Institute. University of Oxford. "Online Labour Index 2020 by Country." 2020.

[55] Słok-Wódkowska, Magdalena and Joanna Mazur. (Słok-Wódkowska & Mazur). "Secrecy by default: How regional trade agreements reshape protection of source code." *Journal of International Economic Law*. Vol. 25. 2022 at 107.

Source code is the description of the steps or actions a computer program takes to perform its functions. Software source code is often "black box" technology that is not transparent to software consumers, meaning even the companies that buy and deploy these programs do not know how they work. These source codes and algorithms are also the recipe for how companies extract and commodify personal data and increasingly govern the workplace and oversee workers.

There are many legitimate policy reasons for government authorities to examine source codes and algorithms. For example, financial regulators might want to access source codes and trading algorithms to prevent high-frequency securities trading from engaging in market manipulation.[56] Environmental regulators should be able to determine if pollution-evasion software facilitates increased emissions, as was the case with the Volkswagen diesel emissions fraud.[57]

Ambassador Katherine Tai stated that digital trade provisions need to provide policy space to address "artificial intelligence in a way that safeguards economic security for workers."[58] But the current digital trade provisions create substantial barriers to governments accessing source code and algorithms to protect workers and enforce labor laws, protect privacy, enforce civil rights laws and prohibit discrimination, safeguard consumers, police anticompetitive conduct, and to pursue other legitimate public policy goals.

Digital trade source code and algorithm secrecy provisions constrain legitimate government oversight: The USMCA and U.S. Japan source code provisions impose broad prohibitions on necessary government oversight and lock-in the current weak regulatory oversight of algorithmic management in the workplace leaving workers and people unprotected from the excesses of digitization. These agreements prohibit countries from requiring "the transfer of, or access to, a source code of software […] or an algorithm expressed in that source code" as a condition of distributing or selling that product.[59] The USMCA definition of algorithm (a "defined sequence of steps taken to solve a problem or obtain a result"[60]) might preclude governments from accessing even a description of what data the source code uses, how the data is evaluated, and how the source code operates.[61] The source code provisions shield technology companies and employers from government efforts to monitor and access source codes and algorithms even to achieve needed policy goals to protect the public.

The existing digital agreements provide a narrow exception that allows government oversight "for a specific investigation, inspection, examination, enforcement action, or judicial proceeding."[62] The case-by-case exemption for *specific* enforcement actions precludes broader, industry-wide evaluations of Big Tech to curb the harmful impact of algorithms, artificial intelligence, and machine learning on workers and people.

---

[56] Busch, Danny. "MiFID II: Regulating high frequency trading, other forms of algorithmic trading and direct market access." *Law and Financial Markets Review*. Vol. 10, Iss. 2. 2016.

[57] Dwyer, Jim. "Volkswagen's diesel fraud makes critic of secret code a prophet." *New York Times*. September 22, 2015.

[58] Ambassador Tai. 2021.

[59] USMCA Art. 19.16.1; U.S. Japan Art. 17.

[60] USMCA Art. 19.1; U.S.-Japan Art. 1.

[61] Słok-Wódkowska & Mazur. 2022 at 98.

[62] USMCA Art. 19.16.2; U.S.-Japan Art. 17.

The specific investigation clause also leaves it unclear how governments could initiate an investigation into, for example, employment discrimination and artificial intelligence-driven 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.[63]

Digital source code and algorithm provisions could prevent the protection of workers from the excesses of algorithmic management: Employers are increasingly using artificial intelligence and other software automation applications to screen potential workers, assign tasks, press workers to be more productive, set shift schedules and pay rates, and discipline and terminate workers.[64] Women, people of color, and immigrants are more likely to be employed in lower-wage workplaces where they can bear the brunt of algorithmic management and its potentially embedded racial and social biases.[65] These trends increased during the pandemic shift to remote and hybrid work.[66]

These automated workplace systems harm workers. A 2021 review of 45 studies on algorithmic management found that more than 90 percent of them highlighted the negative impacts on workers, from de-skilling and task variety, lower worker autonomy and increased workplace control, and increased work intensity and job insecurity.[67] Algorithmic management software are "black box" unaccountable systems that hide what data is relied upon and how the data is used to make decisions. The lack of transparency can obscure the harms which are likely to proliferate as these technologies become more widely implemented.

The digital trade source code and algorithm provisions could make it harder for governments to protect workers from unfair and illegal labor practices, to enforce current law, or to address emerging worker protection issues, including:

- ***Enforcing workplace safety laws against productivity-prodding algorithmic management that can increase injury rates:*** Workplace surveillance and algorithmic management can impose productivity targets that can lead to workplace injuries. Amazon warehouse workers are monitored by artificial intelligence-enhanced security cameras and handheld package scanners that track worker movements and evaluate work speed and can even terminate workers based on data collected on workplace productivity metrics.[68] Workers believe that maintaining a high package pick rate is essential to getting permanent or better positions, creating strong incentives to increase work intensity.[69] Workers have been disciplined and even fired for failing to hit pick-rate productivity targets.[70] Amazon's

[63] McCann. 2019 at 15.

[64] AI Now Institute. "2019 Report." December 2019 at 10.

[65] Bernhardt, Kresge & Suliman. 2021 at 2.

[66] Mearian, Lucas. "The rise of digital bosses: They can hire you — and fire you." *Computerworld.* January 6, 2022; Finnegan, Matthew. "EU 'gig worker' rules look to rein in algorithmic management." *Computerworld.* December 15, 2021.

[67] Parent-Rocheleau, Xavier and Sharon K. Parker. "Algorithms as work designers: How algorithmic management influences the design of jobs." *Human Resource Management Review*. May 2021.

[68] Constantz, Jo. (Constanz). "'They were spying on us': Amazon, Walmart, use surveillance technology to bust unions." *Newsweek*. December 13, 2021; Wood, Alex J. (Wood). European Commission. Joint Research Center. "Algorithmic Management: Consequences for Work Organisation and Working Conditions." JCR Working Paper No. 124874. 2021 at 8 to 9.

[69] Wood. 2021 at 7.

[70] Dastin, Jeffrey. "Amazon issued 13,000 disciplinary notices at a single U.S. warehouse." Reuters. July 12, 2022. E

warehouse worker productivity programs have ratcheted up workloads and work speed and are associated with the company's injury rate that is three times the national average, with serious injury rates five times the national average.[71] The Occupational Safety and Health Administration should be able to assess the extent that algorithmic productivity software is increasing workplace injuries.

- ***Algorithmic surveillance of workers personal social media presence stifles right to form unions:*** Some employers are snooping on workers' social media accounts to find unfavorable opinions of the company as well as determine worker discontent and union sympathies. About half of large employers use software to analyze the text of employee social media posts, according to a 2018 survey.[72] A 2022 memo from the National Labor Relations Board general counsel stated that "omnipresent surveillance and other algorithmic-management tools" can "significantly impair" the right to form or join unions.[73] There are many examples of anti-union worker surveillance. Amazon's Whole Foods has used heat maps and predictive algorithms to track locations that were estimated to be high-risk for union activity.[74] McDonalds has operated an intelligence team that monitored the Fight for $15 organizers, which McDonalds employees were active in the campaign, and which workers and locations were interested in forming unions.[75] The meal kit company HelloFresh used software to mine social media posts on Twitter and Instagram looking for content about unionization efforts and identify whether the posts belonged to an employee.[76] The Labor Department should be able to determine whether this kind of algorithmic surveillance violates the right to form or join unions.

- ***Automated scheduling software can lead to violate labor law and short-change workers:*** Retail companies use algorithms to automate just-in-time shift schedules to minimize costs that often leave workers without stable work schedules that reduce economic stability and disrupt family life.[77] Half of retail workers face uncertain scheduling that compounds the economic precarity from low wages.[78] Retail workers under algorithmic scheduling can receive shorter hours, on-call shifts that never materialize, or shift assignments without prior notice.[79] The adoption of one algorithmic scheduling software can convert full-time workers into part-time workers, ending their health care coverage. [80] Algorithmic scheduling software can also encourage managers attempting to meet productivity targets to press workers to work off the

---

[71] Athena Coalition. "Packaging Pain: Workplace Injuries in Amazon's Empire." January 10, 2020.

[72] Gartner. "The future of employee monitoring." May 3, 2019.

[73] Abruzzo, Jennifer A. General Counsel. National Labor Relations Board. Office of the General Counsel. "Electronic Monitoring and Algorithmic Management of Employees Interfering with the Exercise of Section 7 Rights." Memorandum No. GC-23-02. October 31, 2022 at 1.

[74] Constantz. December 13, 2021.

[75] Franceshi-Bicchierai, Lorenzo and Lauren Kaori Gurley. "McDonald's secretive intel team spies on 'Fight for $15' workers, internal documents show." *Vice*. February 24, 2021.

[76] Kaori Gurley, Lauren. "Internal Slack show HelloFresh Is controlling talk of unionization." *Vice*. November 19, 2021.

[77] Finnegan, Matthew. "EU 'gig worker' rules look to rein in algorithmic management." *Computerworld*. December 15, 2021; Wykstra, Stephani. "The movement to make workers' schedules more humane." *Vox*. November 5, 2019.

[78] Schneider, Daniel and Kristen Harknett. University of California Berkeley and Aspen Institute. "Income Volatility in the Service Sector: Contours, Causes, and Consequences." July 2017 at 2.

[79] Kaplap, Esther. (Kaplap). "The spy who fired me." *Harper's Magazine*. March 2015.

[80] Wood. 2021 at 4.

clock, skip breaks, or misattribute paid sick leave that can amount to wage theft.[81] Government authorities need to be able to access source code to assess how algorithmic scheduling can negatively affect workers and potentially violate wage and hour law.

- ***Artificial intelligence recruiting and hiring tools run afoul of civil rights and employment law:*** Employers are increasingly using artificial intelligence-driven tools to recruit, screen, rank, and assess candidates' interview performances which in turn is affecting prospective workers' chances of getting hired.[82] More than two-thirds of human resources leaders and recruiters were using artificial intelligence tools to automate recruiting and hiring.[83] These systems can entrench the existing subjective preferences that perpetuate racial and social biases that contribute to occupational segregation and racial, gender, and economic inequality.[84] The data-driven systems purport to be objective and logical but often have built in biases and rely on faulty data inputs that amplify the detrimental impacts on workers.[85] Some automated applicant screening processes have made it harder for people with non-white sounding or foreign sounding names, women, older people, or people with disabilities to be interviewed and get a chance at a job.[86] As evidence mounts, the discriminatory impact of these artificial intelligence screening and hiring processes are being challenged as potential violations of civil rights and antidiscrimination laws.[87]

- ***Algorithmic management of gig workers suppresses earnings:*** Algorithmic management of gig workers erodes workers' economic security by assigning tasks or suppressing earnings through pricing algorithms that can overwork and underpay gig workers. Gig drivers are often paid under algorithmic rates that use secret calculations to set fares and charges that have tended to suppress earnings.[88] The *Washington Post* reported that changes to pay rate algorithms pushed earnings down by as much as 50 percent for the same number of hours and trips.[89] Platform companies also use algorithms to discipline or block gig workers from jobs. Algorithms can wrongly downgrade workers or suspend their accounts without disclosing the alleged misdeeds or providing a remedy.[90] These platform "deactivations" amount to short-term termination by algorithm that reduces earnings.[91] The combination of platform

---

[81] Kaplap. March 2015.

[82] Yang. 2020 at 3 and 4.

[83] Ajunwa, Ifeoma. (Ajunwa). Cornell University Industrial and Labor Relations School. Statement before the Subcommittee on Civil Rights and Human Services. Committee on Education and Labor. U.S. House of Representatives. "The Future of Work: Protecting Workers' Civil Rights in the Digital Age." February 5, 2020 at 3.

[84] Yang. 2020 at 4 to 5.

[85] *Ibid.* at 1.

[86] Ajunwa. 2020 at 5 to 6; Yang. 2020 at 4.

[87] Opfer, Chris. "AI hiring could mean robot discrimination will head to courts." *Bloomberg Law*. November 12, 2019.

[88] Feliz Leon, Luis. "How gig workers in Canada are fighting for employee rights." *The Real News*. March 8, 2022.

[89] Bhattarai, Abha. "'Don't game my paycheck': Delivery workers say they're being squeezed by ever-changing algorithms." *Washington Post*. November 7, 2019.

[90] Murgia, Madhumita. "Workers demand gig economy companies explain their algorithms." *Financial Times*. December 13, 2021.

[91] Kaori Gurley, Lauren. "Workers need to unionize to protect themselves from algorithmic bosses." *Vice*. December 19, 2019.

algorithmic evaluation and discipline pushes workers to work intensively for long hours without a break.[92]

- ***Automated surveillance of workers undermines privacy and workers' rights:*** Employers are increasingly deploying advanced surveillance to monitor workers on the job and even outside the workplace.[93] The declining cost of worker surveillance has been supercharged by artificial intelligence systems that have made surveillance more prevalent and includes digital cameras, productivity monitoring applications, key card and RFID tracking, wearable electronic monitors, geolocating and heat sensory tracking, keystroke logging, WIFI network logs, wellness programs, biometrics, and monitoring workers' internet search and social media activity.[94] This surveillance is often unknown to workers and companies need not receive workers' consent; the surveillance data is owned by the employer which can share or sell this data without workers' approval.[95]

A worker-centered digital trade agenda must provide meaningful public policy space to address the impacts of automated decision-making and algorithmic management on workers and society: The rise of automated decision-making and artificial intelligence-driven algorithms poses new challenges to enforce current laws and to address emerging and novel issues that affect workers and society. The digital trade source code and algorithm provisions could make it harder for government to take decisive steps to address existing and new problems driven by these technologies. A worker-centered trade agenda would provide sufficient policy space to address these technological challenges. This should include addressing the corrosive effect that social media algorithms are having on democracy, civil discourse, and the mental health of young people as well as the monopolistic power exerted by platform and e-commerce behemoths. The public policy space to protect workers should include, at a minimum:

- **Meaningful oversight of source codes and algorithms to ensure compliance with labor and employment laws:** Governments must be able to examine corporate source codes, algorithms, and other tools of "AI management" to fully understand their impacts and 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.

- **Policy space to address emerging threats to workers' privacy, including employer use of workplace surveillance software:** The digital trade data provisions only protect the personal data of the "users of digital trade,"[96] which in the context of worker privacy is likely the employer that collects and owns the data and information collected by worksite surveillance. Governments must have the policy space to take measures to address digital workplace surveillance and other emerging threats to workers' privacy.

---

[92] Wood. 2021 at 10.

[93] Ajunwa, Crawford, and Schultz. 2017 at 738 to 739.

[94] *Ibid.*; Abril, Danielle. "Your boss can monitor your activities without special software." *Washington Post*. October 7, 2022.

[95] Bernhardt, Kresge & Suliman. 2021 at 18.

[96] USMCA Art. 19.8.2; U.S.-Japan Art. 15.1.

- **Addressing abusive employment practices in the technology sector:** Large technology and platform companies have promoted an exploitative employment model based on rampant employment misclassification and the outsourcing of core job functions. Platform gig workers are employed as precarious contractors without 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 clean up the labor abuses in their own operations and their digital supply chains, including the ghost workers in the developing world.

IV. Other digital provisions present challenges to workers and society

The existing digital trade provisions grant broad rights to technology firms with limited protections for people and workers. Beyond the cross-border data and source code provisions, workers can be negatively impacted by the failure to protect copyrighted material and the weak protections against cyberattacks.

Digital trade provisions fail to protect and promote the economic security of creative professionals in the U.S. motion picture, television, and music industries: The digital trade provisions shield platform companies from responsibility for the third-party content posted on their networks that leaves workers in the creative industries vulnerable to copyright infringement that undermines their economic security. The USMCA and U.S.-Japan agreements both absolve suppliers of interactive computer services from "liability for harms related to information stored, processed, transmitted, distributed, or made available by the service."[97] This language mirrors the Digital Millennium Copyright Act language that excludes internet service providers from being held responsible as a publisher of content on their networks.[98] This absolves platforms and social media companies from responsibility from users promoting hate speech,[99] political disinformation,[100] or other content that has increasingly been associated with negative mental health impacts.[101]

These provisions also harm the more than 4 million people who work in the motion picture, television, and music industries. Many of these workers collectively bargain for payments and contributions to their health insurance and pension plans that are directly tied to the sales and licensing of the copyrighted works that they help create.[102] This content contributes more than $500 billion to the U.S. economy annually and generates a trade surplus.[103] Stolen or unlicensed use of copyrighted content on digital platforms directly harms these workers, severely diminishing the

---

[97] USMCA Art. 19.17.2; U.S.-Japan Art. 18.2.

[98] The Digital Millennium Copyright Act of 1998. 17 USC §512.

[99] Castaño-Pulgarín, Sergio Andrés et al. "Internet, social media and online hate speech. Systemic review." *Aggression and Violent Behavior*. Vol 58. 2021.

[100] Hiaeshutter-Rice, Dan, Sedona Chinn, and Kaiping Chen. "Influencer content: Understanding how audiences and channels shape misinformation online." *Frontiers in Political Science.* May 31, 2021.

[101] Twenge, Jean M. et al. "Increases in depressive symptoms, suicide-related outcomes, and suicide rates among U.S. adolescents after 2010 and links to increased new media screen time." *Clinical Psychological Science*. Vol. 6, Iss. 1. November 14, 2017.

[102] AFL-CIO. Department for Professional Employees. [Fact sheet]. "Creative professionals depend on strong copyright protection." October 4, 2021.

[103] AFL-CIO. Department for Professional Employees. [Fact sheet]. "Intellectual property theft: A threat to working people and the economy." October 25, 2021.

payment and benefit contributions they have bargained for and the ability of their employers to finance future content creation. Digital trade policy must aggressively address the stolen or unlicensed use of copyrighted content on digital platforms that directly harms these workers.

Protect workers and unions from cybercrime by both state and private actors: The USMCA and U.S.-Japan digital agreements recognize the importance of protecting networks and users from cybercrimes to prevent the erosion of confidence in digital trade.[104] Neither provision acknowledges the impact on workers, people, unions, or other organizations that may be harmed by cyberbreaches, malware, ransomware, or other cybercrimes. The digital trade provisions discourage regulatory approaches to bolster cybersecurity and explicitly promote voluntary "risk-based approaches that rely on consensus-based standard and risk management best practices" to protect against cybercrimes and respond to cybersecurity events.[105]

Workers and unions can be significantly impacted by cyberbreaches and ransomware attacks that harm unions, expose workers' personal data, and affect their earnings if employers are temporarily shut down. In 2014, the United States charged members of the Chinese military with hacking U.S.-based companies and the United Steelworkers.[106] In 2019, the International Brotherhood of Teamsters was subject to a ransomware attack demanding $2.9 million that forced the union to rebuild its computer servers.[107] Cyberattacks against employers can leave workers vulnerable to unexpected shutdowns and shift cancellations, as happened to unionized meatpacking workers in 2021.[108] The United Food and Commercial Workers International Union was able to secure pay for workers that lost shifts to the cyberattack, but these types of attacks could cost workers' shifts and income if employers are forced to idle facilities or business locations. A cyberbreach against an entertainment payroll company potentially exposed the personal information and bank accounts of Screen Actors Guild-American Federation of Television and Radio Artists members in 2014.[109] 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.

V. Conclusion

As the Biden administration continues to remake U.S. trade policy, 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 interests of big technology companies.

Too often, the debate over digital trade is framed as a binary choice between authoritarian digital censorship or the unregulated status quo that leaves Big Tech free to collect, control, and commodify workers and consumers' private data as they see fit. The labor movement rejects this

---

[104] USMCA Art. 19.15.1; U.S.-Japan Art. 15.1.

[105] USMCA Art. 19.15.2; U.S.-Japan Art. 1.2.

[106] Miller, John. W. "Pittsburgh-area firms allegedly targeted by hackers." *Wall Street Journal*. May 19, 2014; U.S. Department of Justice. [Press release]. "U.S. chares five Chinese military hackers for cyber espionage against U.S. corporations and a labor organization for commercial advantage." May 19, 2014.

[107] Allen, Jonathan and Kevin Collier. "Ransomware attack hits Teamsters in 2019 — but they refused to pay." *NBC News*. June 11, 2021.

[108] "Fallout and blame: Ransomware attack against world's largest meat producer." *SecureWorld News*. June 1, 2021.

[109] Raman, Jeffrey. "Entertainment payroll firm breached." *BankINfo Security*. December 4, 2014; SAG-AFTRA. [Press release]. "An important announcement about ART Payroll." December 2, 2014.

false choice. Digital trade rules cannot grant broad powers to Big Tech and prevent governments from protecting workers from the downsides of the digital transformation of the economy.

It is time for a strategic re-set on digital trade policy. The public, including workers and labor unions, must decide the rules of the road for technology in the workplace and society. There must be a new democratic, stakeholder-driven approach to data governance that confronts the negative impacts of digitization on workers, consumers, and society.

The Biden administration's call for a 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.