S. HRG. 117–730

PROMOTING COMPETITION, GROWTH, AND PRIVACY PROTECTION IN THE TECHNOLOGY SECTOR

HEARING

BEFORE THE

SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH

OF THE

COMMITTEE ON FINANCE UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

DECEMBER 7, 2021

Printed for the use of the Committee on Finance

U.S. GOVERNMENT PUBLISHING OFFICE

53–261—PDF WASHINGTON : 2023

COMMITTEE ON FINANCE

RON WYDEN, Oregon, *Chairman*

DEBBIE STABENOW, Michigan	MIKE CRAPO, Idaho
MARIA CANTWELL, Washington	CHUCK GRASSLEY, Iowa
ROBERT MENENDEZ, New Jersey	JOHN CORNYN, Texas
THOMAS R. CARPER, Delaware	JOHN THUNE, South Dakota
BENJAMIN L. CARDIN, Maryland	RICHARD BURR, North Carolina
SHERROD BROWN, Ohio	ROB PORTMAN, Ohio
MICHAEL F. BENNET, Colorado	PATRICK J. TOOMEY, Pennsylvania
ROBERT P. CASEY, JR., Pennsylvania	TIM SCOTT, South Carolina
MARK R. WARNER, Virginia	BILL CASSIDY, Louisiana
SHELDON WHITEHOUSE, Rhode Island	JAMES LANKFORD, Oklahoma
MAGGIE HASSAN, New Hampshire	STEVE DAINES, Montana
CATHERINE CORTEZ MASTO, Nevada	TODD YOUNG, Indiana
ELIZABETH WARREN, Massachusetts	BEN SASSE, Nebraska
	JOHN BARRASSO, Wyoming

JOSHUA SHEINKMAN, *Staff Director*
GREGG RICHARD, *Republican Staff Director*

SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH

ELIZABETH WARREN, Massachusetts, *Chair*

RON WYDEN, Oregon	BILL CASSIDY, Louisiana
	RICHARD BURR, North Carolina

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL

COMMUNICATIONS

PROMOTING COMPETITION, GROWTH, AND PRIVACY PROTECTION IN THE TECHNOLOGY SECTOR

TUESDAY, DECEMBER 7, 2021

U.S. SENATE,
SUBCOMMITTEE ON FISCAL RESPONSIBILITY
AND ECONOMIC GROWTH,
COMMITTEE ON FINANCE,
Washington, DC.

The hearing was convened, pursuant to notice, via webex, in Room SD–215, Dirksen Senate Office Building, Hon. Elizabeth Warren (chair of the subcommittee) presiding.

Present: Senators Wyden, Whitehouse, and Cassidy.

Also present: Democratic staff: Michael Evans, Deputy Staff Director and Chief Counsel; Ian Nicholson, Investigator and Nominations Advisor; and Joshua Sheinkman, Staff Director. Republican staff: Lincoln Foran, Policy Advisor; John O'Neal, Trade Policy Director and Counsel; Mayur Patel, Chief International Trade Counsel; Gregg Richard, Staff Director; and Jeffrey Wrase, Deputy Staff Director and Chief Economist.

OPENING STATEMENT OF HON. ELIZABETH WARREN, A U.S. SENATOR FROM MASSACHUSETTS, CHAIR, SUBCOMMITTEE ON FISCAL RESPONSIBILITY AND ECONOMIC GROWTH, COMMITTEE ON FINANCE

Senator WARREN. This hearing will come to order.

Good morning, and welcome to today's hearing of the Subcommittee on Fiscal Responsibility and Economic Growth. I am pleased to be working with Ranking Member Cassidy on this hearing on promoting competition, growth, and privacy protection in the technology sector. Senator Cassidy will be joining us remotely. We are going to do a mixed hearing, with some people in person and some people remote.

Under President Biden's leadership, the American economy is rebounding. The unemployment rate has dropped from a pandemic height of 14.8 percent in April of 2020, to 4.6 percent today; 5.6 million jobs have been added since President Biden's inauguration, more than were added in the first 10 months of any administration since we have been keeping records. Child poverty is projected to plummet by more than 40 percent, thanks to the American Rescue Plan. All of this has occurred despite an ongoing pandemic that has plagued us now for nearly 2 years. Families have tried to adapt, and those changes have echoed throughout our economy.

Demand has shifted as people have consumed fewer services while buying more durable goods like exercise equipment and home appliances. The economy has recovered more quickly than many businesses projected, and all of this is contributing to unexpected bottlenecks in our supply chain and sporadic shortages at warehouses. And these factors contribute to the price increases for many consumer goods. But they are not the only reason that prices have gone up.

Sure, giant companies will raise prices when they have to, but they will also raise prices when they can get away with it. And how do we know this? Because when companies are simply passing along their increases in costs, then profit margins should stay the same. But when companies see a chance to gouge customers, particularly while everyone is talking about inflation, then those companies raise their prices beyond what is needed to cover their increased costs.

Right now, prices are up at the pump, at the supermarket, and online. At the same time, energy companies, grocery companies, and online retailers are reporting record profits. That is not simply a pandemic issue. It is not simply some inevitable economic force of nature. It is greed. And in some cases, it is flatly illegal.

One reason for this price gouging is that fewer and fewer markets in America are truly competitive. When several businesses are competing for customers, companies cannot use a pandemic or a supply chain kink to pad their own profits. In a competitive market, the margin above costs stays steady even in troubled times. But in a market dominated by one or two giants, price gouging is much easier.

For generations, policymakers and regulators under both Democrats and Republicans promoted free-market competition. But starting in the 1970s, our government changed course. For decades now, regulators and courts have looked the other way even as one sector after another has become dominated by one or two giants. They rubber-stamp merger after merger without regard to the consequences. And when small businesses got wiped out, and startups were smothered or bought out, they just did not care.

Today, as a result of increasing consolidation across industries, bigger and bigger corporations have more and more power to charge their customers any price they want. They also wield more and more power to under-invest in things like supply chain resiliency and more and more power to hold down wages and benefits for workers. And it is getting worse.

Earlier this month, Federal Trade Commission Chair Lina Khan noted that by September of this year, our antitrust agencies had already received more merger filings than any other year in the previous decade. In fact, they are on track in 2021 to receive a 70-percent increase above average filings in recent years. Giant corporations are taking advantage of this global crisis to gobble up struggling small businesses and to increase their power through predatory mergers. I introduced my Pandemic Anti-Monopoly Act last year to slow down this trend, and to protect workers and small businesses and families from being squeezed even more by harmful mergers during this crisis. And I will reintroduce it this year, because the need is clear.

The effects of limited competition in our technology sector are particularly severe, and that is why I am interested in exploring today's hearing. Limited competition in tech is having spillover effects across our entire economy. Anticompetitive practices in the semiconductor industry have exacerbated supply chain issues. Big tech firms have used their dominance to inflate prices throughout the online retail market, and to subject their workers to inhumane conditions during the pandemic.

And as Ranking Member Cassidy has rightly highlighted in his own work, tech firms collect and exploit sensitive personal information, often threatening national security, harming our emotional health, and discriminating against vulnerable groups.

It does not have to be like this. With stronger antitrust laws and robust enforcement, we can ensure that our economy works for American families, not just for the wealthiest corporations. Congress could provide better tools to the FTC and the Department of Justice to investigate anticompetitive mergers and break up the companies that have held our economy down. We can also make it easier for the agencies to reject such mergers in the first place. By promoting competitive markets for consumers and workers, we can foster a stronger American economy and a stronger American democracy.

So I look forward to discussing these issues today. I appreciate all of our witnesses who are joining us, and I look forward to hearing about your insights and your experiences.

[The prepared statement of Senator Warren appears in the appendix.]

Next, I am going to turn to Ranking Member Kennedy—Cassidy; sorry, Senator Cassidy—for your opening remarks. Senator Cassidy?

OPENING STATEMENT OF HON. BILL CASSIDY, A U.S. SENATOR FROM LOUISIANA

Senator CASSIDY. No problem, Senator Warner [laughing]—no, Senator Warren. Good morning. Thank you all for being here at today's hearing. And thank you for our witnesses for taking time to testify.

Senator Warren and I have agreed to a bipartisan hearing on promoting competition, growth, and privacy protection in the technology sector. I will focus my time on the privacy aspect of this, and specifically on the data broker industry.

The data broker industry is relatively unknown to most Americans, but its practices and techniques are interwoven into our lives. Data brokers build profiles on individuals about certain attributes, and then sell that information to those whom they see fit, or whoever wishes to purchase.

For example, I am a big fan of LSU football. I frequently search what is related to our new coach, Brian Kelly, upgrading from Notre Dame to LSU. That search data is collected and a profile is made. I then receive ads about buying LSU football tickets, merchandise, et cetera.

We all experience something similar on the Internet. Multiple times a year a company will be the victim of a hack that exposes the data of thousands, if not millions, of customers. While we go

to great lengths to minimize those cyber-incursions, we ignore an entire industry that transacts in much more detailed and sensitive critical information.

You will hear today from witnesses that there is very little information that data brokers cannot sell, and even less data that they are not willing to sell. I believe that few in this room would think it a good idea to sell the profiles of American service members—but that is what is happening.

We should have a conversation about what American data we think is okay to be bought and sold without the knowledge of many Americans; what type of data we think is acceptable to be bought and sold, period. Should we allow a list of military personnel to be sold to foreign adversaries? Should we allow lists of domestic abuse survivors to be sold to domestic abusers? We should have a conversation about what data is appropriate to collect, what limits should be placed on the groups that collect that data, and restrictions on how that data is sold or transferred to others. We should have a conversation about all the things our foreign adversaries can do with this data. That is why we assembled a team of data broker experts to talk about the different aspects of data brokers, what is regulated and what is not, and how best to move forward.

Thanks again to our witnesses, and I am looking forward to discussing the issue.

[The prepared statement of Senator Cassidy appears in the appendix.]

Senator WARREN. Thank you very much. I appreciate it, Senator Cassidy.

So, we have a great set of witnesses here to share their views on promoting competition, growth, and privacy protections in the American technology sector. I appreciate everyone being with us today.

First, joining us virtually, we have Courtenay Brown. Ms. Brown is an Amazon Fresh worker at the company's fulfillment center in Avenel, NJ and a leader with United for Respect. She is also a veteran of the United States Navy.

Second, also joining us remotely, we have the Honorable Karl Racine, the District of Columbia's first elected Attorney General. He is the president of the National Association of Attorneys General and the chair emeritus of the Democratic Attorneys General Association's executive committee. Previously he was a managing partner at Venable Associates, White House counsel for President Clinton, and a staff attorney for the Public Defender Service of the District of Columbia.

Third, we have Barry Lynn, who is the executive director of the Open Markets Institute. His research focuses on threats of the 21st-century monopolies to our democracy, individual liberty, security, and prosperity.

Next, we have Justin Sherman, a co-founder and senior fellow at Ethical Tech, an initiative at Duke University focused on research at the intersection of technology and ethics. Mr. Sherman studies data brokers and the sensitive data that they hold on U.S. individuals.

Following Mr. Sherman, we have Samm Sacks of Yale Law School's Paul Tsai China Center and a cyber policy fellow at the

think tank New America. Ms. Sacks is an expert on cross-border data flows and studies how the Chinese Government collects and uses data.

And finally, we have Ms. Stacey Gray. Ms. Gray is senior counsel at the Future of Privacy Forum. She is a data broker expert, and her research centers on the intersection of emerging technologies and Federal regulation and enforcement.

Increasing consolidation throughout the American economy undoubtedly contributes to higher prices, worsening working conditions, and privacy concerns. The pandemic has not only exacerbated these issues, but has also exposed them more plainly.

We can fix this together. We can make our economy work for all Americans. I want to thank you all for being with us today. I am looking forward to hearing your testimony.

So, Ms. Brown, we are going to start with you. You are recognized for 5 minutes. And tell us what you want us to know.

STATEMENT OF COURTENAY BROWN, AMAZON ASSOCIATE AND LEADER, UNITED FOR RESPECT, NEWARK, NJ

Ms. BROWN. Okay; good morning, everyone. Thank you for inviting me to share my experience with you today, Senator Warren and members of the subcommittee. My name is Courtenay Brown, and I live in Newark, NJ. I am currently working at an Amazon fulfilment center and have been for 4½ years. Before working at Amazon, I served my country as a service member in the United States Navy, and I took the commitment that I made to my country then seriously, as well as the commitment I take seriously now as a member leader of United for Respect.

I am here today, Senators, to raise the alarm about Amazon's business model, because it is a threat to working people, and it is a threat to our economy. One out of every 150 American workers is an Amazon employee, as well as, in that group, there are some former employees. And this multi-billion-dollar corporation grew on the back of its workers by exploiting them. I am looking to you to stand up to corporations like Amazon and protect us.

The job that I do is a much-needed service, especially since the COVID–19 pandemic began. As a process guide, I am in charge of sorting 35,000 to 50,000 groceries daily for delivery to homes in near cities in New Jersey. I am in and out of our cooler constantly, stepping in and out of temperatures as low as negative 10 degrees, and picking up and setting packages down with little to no rest. The work that I do is supposed to be done with 30 to 40 people, but we operate with 25 people or less every day. Because our work is essential, and our workload has increased, we need more hands on deck, not less, so that we can take turns getting breaks and getting much-needed rest. But Amazon can barely retain its workers.

Amazon's multi-billion-dollar wealth is made possible by offering same-day delivery—anywhere from same-day delivery to 2-day delivery—and the corporation has achieved this speed and scale through their sheer brutality, watching, timing, and punishing associates like me and my coworkers for not working fast enough, and not allowing associates to take time off to adequately rest and recover, and to prevent burnout.

From the moment we pull into the parking lot, we are monitored. And that is every step at the facility that we take, and if we fall behind in any way during our 11-hour shift, we risk being disciplined, or even losing our jobs. We are pushed to our limit, to the point where we cannot even take regular bathroom breaks. Often, we have to run to and from the bathroom in under 2 minutes, so we do not get in trouble. On top of that, the bathrooms are usually pretty gross and they are usually broken too.

The constant pressure and surveillance is why Amazon has twice the level of injuries and turnover compared to similar jobs. Research has shown that workplace injury rates are higher at Amazon facilities with more robotic and automated technology. I used to be a trainer, and I saw firsthand how, out of 50 new hires, only five would make it to the 1- or 2-month mark. And many quit soon after due to injuries or over-exhaustion.

We are living in a country where machines are getting better treatment than people. The machines at my facility undergo routine maintenance checks to ensure that they do not burn out. Yet the one time I needed to take off to recover from my mother's passing back in September, I was only given 2 days to do so. Two days to plan a funeral and process my mother's death. So I ended up taking a month off of unpaid time, which was the only option I had at the time. And this unpaid time was only because there was a reduction in the amount of work we had. And my sister, she was not as lucky, because she also works with me, and she had to literally work the day of her death, as well as the day after, come for her funeral, and then return to work 2 days later. So the entire funeral was literally scheduled around me and my sister's work schedule. Imagine going through that while Jeff Bezos made $75 billion last year, thanks to me and my co-workers.

Amazon's high-tech sweatshop caused me to develop plantar fasciitus and tendinitis with debilitating pain in my heel and ankle from having to stand for long periods of time at work with little to no rest. There was once when the pain was so severe that I ended up in the emergency room and, because I was homeless at the time, I did not have enough time to take off. I had to beg doctors and nurses to see me as quickly as possible, because I could not afford to lose my job and the opportunity I had of becoming leadership.

This kind of exploitation is not just happening to me. People have been working through the pandemic nonstop because they will not let us take time off. Often we are so exhausted, we break down and cry. A coworker of mine had to stop breast-feeding her child early due to not receiving the support when she had to pump at work. This is the type of environment Amazon is perpetuating across the country. Amazon associates have been fighting back against these dangerous conditions for years. Instead of fixing the problem, Amazon is only doubling down on exploitative models.

Jeff Bezos himself recently told shareholders that he plans to use more automated control of workers in the warehouse. The worst part is that Amazon is setting up its high-tech sweatshops in Black and Brown communities desperate for work. Amazon is a big-numbers company, and they know that there are people who look like me who have very limited choices, and they know we cannot

afford to complain or refuse bad conditions. Amazon takes advantage of this desperation. The pandemic has closed a lot of businesses in my area, so even someone like me who considers looking for another job, I cannot because there are no jobs available, or the pay is not enough to make rent and put food on the table.

This committee is considering competition and economic growth in the tech sector. When corporations break the rules to maximize their profit, they ensure they win by all means necessary, including exploiting workers and gutting small businesses.

Senators, I am looking to you to stop corporations like Amazon from ruining our economy and dictating the workplace standards for hundreds of millions of workers like me. I am asking you to help me put an end to inhumane, exploitative practices that leave America's workers injured, exhausted, and mentally battered each day. Our country needs elected officials to side with working people—to side with essential workers, not big corporations.

[The prepared statement of Ms. Brown appears in the appendix.]

Senator WARREN. Thank you very much, Ms. Brown. I appreciate your coming in and testifying.

Now we go to Attorney General Racine. You are recognized for 5 minutes.

STATEMENT OF HON. KARL A. RACINE, ATTORNEY GENERAL, DISTRICT OF COLUMBIA, WASHINGTON, DC

Mr. RACINE. Chair Warren, Ranking Member Cassidy, and distinguished members of the subcommittee, thank you so much for the opportunity to testify before you today. As the first independent elected Attorney General of the District of Columbia, and also the outgoing president of the bipartisan National Association of Attorneys General, one of my most important responsibilities is to protect DC consumers from corporate wrongdoing, including investigating and, where appropriate, filing suit against defendants that illegally exercise monopoly power, violate privacy laws, and hurt workers.

We have used our power and authority to sue Amazon in the local DC court for using its overwhelming market power—that is, 50 to 70 percent of all online sales occur on Amazon's platform—to control prices and to restrict agreements with third-party sellers that sell on Amazon's marketplace and wholesalers that feed Amazon's retail business. In its defense, Amazon claims that everything it does in business is all about the consumer. Well, our investigation reveals otherwise. Amazon indeed is focused, and the evidence is compelling, on one thing: its bottom line, even at the expense of consumers like the ones it claims to care so much about. In fact, Amazon is costing all of us more money by controlling prices across the entire electronic mall.

Like you, Senator Warren, I too am a capitalist. People should get paid for their hard work, creativity, and entrepreneurship. People should certainly watch their profits increase as their business increases. But when companies like Amazon unfairly and unlawfully increase the prices on all of us, stifle competition, and take advantage of consumers, the law must step in and say, "enough is enough."

Back in 2019, Amazon was facing pressure from Congress and regulators over anticompetitive behavior, and we know that the concern around Amazon and others is as bipartisan as it gets. To put regulators at ease, Amazon claimed it removed a particular clause in its agreement with third-party sellers that prohibits these third-party sellers from offering their goods for lower prices or on better terms than competing online marketplaces, including the third-party seller's own websites. Again, Amazon claimed that it would remove that particular clause. Here is the spoiler alert: Amazon deceived Congress and consumers with its bait-and-switch, replacing the initial terms of the agreement with different titles and different words that had the same illegal impact.

Let me give an example of how this works. If I am a third-party seller selling, for example, headphones, I do want to list my product on Amazon. Why? Because it reaches so many people—remember, 50 to 70 percent of the entire electronic mall. Well, in order to do so, I have to do the following: sell the headphones at a price on the Amazon marketplace that allows me to still own a reasonable profit, after incorporating Amazon's very high fees and commissions. Then I am barred from selling my headphones on any other platform, including my own website, at a lower price, even though I could earn a fair profit by doing so.

Put another way, I have to build in those high Amazon fees and high Amazon commissions into the price of the headphones that I sell. Why? Because Amazon forced me to agree to that term in order to access its electronic mall. And if they find out, if I sell my headphones even on my own website for a lower price, lower than the built-in fees and commissions that Amazon requires, guess what? You get kicked off of the Amazon marketplace and have sanctions, financial sanctions, imposed on you.

This leaves third-party sellers with two choices. They can sell their product on Amazon under these extremely restrictive terms that guarantee a profit to Amazon and put third-party sellers at risk, or they can only offer their product on other marketplaces. But because Amazon controls so much of the marketplace, third-party sellers have little choice. These agreements impose an artificially high price because, as I have explained, all across the online retail space, consumers lose in this game as a result of Amazon's agreements.

But absent these agreements, third-party sellers could offer their products for lower prices. That is one of the bases for our lawsuits. And Amazon is not just doing this with third-party sellers. They are also doing it with wholesalers as well. So we recently added that count to our lawsuit. First-party sellers sell products to Amazon for Amazon to resell at retail to consumers. If Amazon lowers its retail prices to match or beat the lower price on a competing online marketplace, the wholesalers—listen to this—are forced to pay Amazon the difference between the agreed-upon profit and what Amazon realizes with the lowered retail price. This can lead to wholesalers owing Amazon millions of dollars.

To avoid triggering this agreement, wholesalers have increased the prices on their goods on competing online marketplaces. In other words, they have agreed to do what Amazon wants—that is,

to charge consumers more for products than they ordinarily would have to pay but for Amazon's illegal agreements.

All of these agreements reduce an online marketplace's ability to compete with Amazon's marketplace on price, and result in consumers paying artificially high prices. And even outside this litigation, small businesses of course have complained and complained that Amazon has stolen their business ideas and passed them off as Amazon's own.

Let me give you one brief example——

Senator WARREN. Attorney General, I am going to have to stop you here in just a minute. We have just 5 minutes for each of our witnesses, but we are going to be able to ask you some questions, because I definitely want to hear this. Is that okay?

Mr. RACINE. Absolutely, Senator, and I am happy to stop right here.

[The prepared statement of Mr. Racine appears in the appendix.]

Senator WARREN. Great. Okay, thank you so much. I appreciate it.

And now, Mr. Lynn, you are recognized for 5 minutes.

STATEMENT OF BARRY C. LYNN, EXECUTIVE DIRECTOR, OPEN MARKETS INSTITUTE, WASHINGTON, DC

Mr. LYNN. Chair Warren, Ranking Member Cassidy, members of the subcommittee, thank you for inviting me to speak with you today on this fundamentally important topic. I am Barry Lynn, and I direct the Open Markets Institute, and it is good to see you today.

Political economics is the art of governing how people compete with and exercise power over one another. An essential truth of human society is that competition among people is inevitable. What people can control is whether corporations and markets are structured to promote the liberty and well-being of the individual, the ability of citizens to make wise decisions, and the security and prosperity of individuals and of the Nation.

For two centuries, Americans were masters of engineering competition policies to achieve these ends. American citizens used antimonopoly laws to make themselves the most equal and free people in the world, and the most prosperous, innovative, and powerful. But beginning 4 decades ago, Americans from both parties radically altered how we think about and enforce competition policy.

Rather than aim to promote liberty, democracy, and community prosperity, policymakers embraced a philosophy that said we should aim to promote efficiency only. The result is that today Americans face the gravest set of domestic threats to liberty and democracy since the Civil War. Today in America, as Courtenay made clear, monopolists drive down the people's wages while driving up the prices that people must pay. Monopolists threaten freedom of the press and of expression. Monopolists spy on citizens then use the people's own secrets to misinform, incite, and enrage those same citizens for profit.

Monopolists tax, extort, and steal other people's businesses. Monopolists destroy better technologies and ideas. Monopolists destroy vital industrial capacities. Last year we saw this with face masks, this year, with semiconductors. Monopolists create dangerous dependencies on powerful foreign states. Monopolists strip America's

communities of wealth, opportunity, independence, security, and hope.

None of this is new. I, myself, first warned of how the platform monopolists threaten freedom of expression and democracy more than 11 years ago. I, myself, first warned of the dangers of supply chain concentration 19 years ago. But there is good news. Americans are swiftly awakening to the interlocking set of crises. Today the great majority of Americans from across the political spectrum want to see monopolists stripped of their powers and, better yet, enforcers and legislatures are on the move.

The Justice Department and the FTC have brought lawsuits against Google and Facebook, and in the most democratic anti-monopoly action in U.S. history, Attorneys General from 49 States, Puerto Rico, Washington, DC, and Guam launched investigations of Google and Facebook and filed three additional lawsuits.

Then there are the smart and urgent efforts to strengthen antitrust laws here in the Senate, as with Senator Warren's proposal; in the House; and in Europe and around the world. Perhaps most important, President Biden has personally condemned the pro-monopoly Chicago School of "consumer welfare" philosophy of Robert Bork and Richard Posner and restored our Nation's traditional focus on protecting the American people and the Nation itself from all dangerous concentrations of power and control. And in Lina Khan and Jonathan Kanter, President Biden has appointed law enforcers smart enough and strong enough to get the job done.

Today's hearing marks an especially important step forward in this great struggle. It highlights the pressing need to relearn that competition policy is much more than mere antitrust law. Rather, competition policy is the combination of antitrust with trade policy, corporate governance, Wall Street governance, and industrial strategy. Nowhere is this more obvious than in addressing America's twin supply chain crises. That is why in my written testimony I focus on what lessons we can learn from the role monopolists have played in concentrating so much risk and power in our production and transportation systems, such as with semiconductors.

And I detail how we can rebuild our industrial system in ways that make us truly safe, while also breaking inflation and boosting wages. Our opportunity today is not merely to rebuild what the monopolists have broken these last 40 years, it is to relearn how to use anti-monopoly laws both to imagine and make an America far more democratic, just, and forward-looking than any of us have dared imagine in a generation.

[The prepared statement of Mr. Lynn appears in the appendix.]

Senator WARREN. Thanks very much, Mr. Lynn. I appreciate it.

Mr. Sherman, you are recognized for 5 minutes.

STATEMENT OF JUSTIN SHERMAN, FELLOW AND RESEARCH LEAD, DATA BROKERAGE PROJECT, SANFORD SCHOOL OF PUBLIC POLICY, DUKE UNIVERSITY, DURHAM, NC

Mr. SHERMAN. Chair Warren, Ranking Member Cassidy, and distinguished members of the subcommittee, thank you for the opportunity to testify today about privacy issues facing American citizens. I am a fellow with Duke University's Sanford School of Public Policy, where I lead a research project focused on the data broker-

age ecosystem, a multi-billion-dollar virtually unregulated industry of U.S. companies aggregating, buying, and selling Americans' intimate personal data on the open market.

Data brokers are profiting off the vulnerability and insecurity of the U.S. and its citizens. While comprehensive consumer privacy law is vital, Congress need not wait to resolve this debate to regulate data brokerage. Today I will make three points. Congress can strictly control the sale of data to foreign companies, citizens, and governments; strictly control the sale of data in sensitive categories like genetic and health information and location data; and stop companies from circumventing those controls by inferring data.

Our research at Duke University has found data brokers widely advertising data on hundreds of millions of Americans, their sensitive demographic information, political preferences and beliefs, and whereabouts in real-time locations, as well as data on first responders, students, government employees, and current and former members of the U.S. military. Data brokers contract and sell your race, religion, gender, sexual orientation, income level, how you vote, what you buy, what you search online, and where your kids and grandkids go to school. This harms every American, particularly the most vulnerable. And I will focus on three examples.

Data brokers advertise data on millions of current and former U.S. military personnel. Criminals have bought this data to scam veterans and their families because of the military benefits they get from the Federal Government. Foreign states could acquire this data to profile military personnel, trick them and their families, and undermine national security.

The Chinese Government's 2015 hack of the Office of Personnel Management was one of the worst breaches the Federal Government has suffered. In the future there is no need for the Chinese Government, or any other foreign intelligence agencies, to hack those databases when the data can be bought legally on the open market from U.S. companies.

Data brokers known as "people search" websites aggregate millions of Americans' public records and make them available for search and sale online. Abusive individuals have used this data, including highly sensitive information on individuals' addresses, whereabouts, and family members, to hunt down and stalk, harass, intimidate, and even murder other people—predominantly women and members of the LGBTQ+ community.

There is little in U.S. law stopping data brokers from collecting, publishing, and selling data on victims and survivors of this violence. Data brokers also advertise data on millions of Americans' mental health conditions. Companies can legally purchase this data from other firms and use it to exploit consumers. Criminals already scam senior citizens using data broker data. They could similarly buy data on seniors with Alzheimer's and dementia to steal away their life savings. Foreign governments could even acquire this data for intelligence purposes.

Our research has found that companies selling this data on hundreds of millions of Americans conduct relatively little "know your customer" due diligence. And for those that do, it is unclear how strong it is in practice. Brokers may also make their customers

sign nondisclosure agreements, stopping them from saying where they obtained U.S. citizens' information.

As part of talking about data threats to Americans' civil rights, U.S. national security, and democracy, we must focus on this entire data brokerage ecosystem. There are three steps Congress can take now. First, strictly control the sale of data broker data to foreign companies, citizens, and governments, which currently can entirely legally buy millions of U.S. citizens' data directly or through front companies. Second, strictly control and even consider outright bans on the sale of data in sensitive categories like genetic and health information and location data, which is used now to follow, stalk, and harm individuals. Third, stop companies from circumventing those controls by inferring data, using algorithms and other techniques to predict things they have not technically collected.

Congress can and should act now to regulate the data brokerage ecosystem and its threats to consumers' civil rights and national security. Thank you.

[The prepared statement of Mr. Sherman appears in the appendix.]

Senator WARREN. Thank you, Mr. Sherman.

And now, Ms. Sacks, you are recognized for 5 minutes.

STATEMENT OF SAMM SACKS, SENIOR FELLOW, YALE LAW SCHOOL PAUL TSAI CHINA CENTER, NEW HAVEN, CT; AND CYBERSECURITY POLICY FELLOW, NEW AMERICA, WASHINGTON, DC

Ms. SACKS. Chair Warren, Ranking Member Cassidy, and members of the subcommittee, it is such an honor to testify today. I am a senior fellow at Yale Law School's Paul Tsai China Center and the cybersecurity policy fellow at New America. I have spent the last decade as an analyst of China's technology and data policies, both in the national security community and with the private sector. I also advise corporations on China's policies.

Today I will focus my testimony on China and global cross-border data flows. While my expertise focuses on China—and I will speak specifically about the Chinese Government's efforts to acquire data—my views of the most effective solutions require that the United States put forward a more comprehensive data governance vision with stronger protections for security and privacy for all companies.

Some of these risks are specific to China, but so much of this is much bigger. U.S. lawmakers have an opportunity to address transnational security threats, while also advancing a more secure, ethical, and democratic Internet in its own right.

The Chinese Government has embarked on an ambitious national data strategy with the goal of acquiring, controlling, and unlocking the value of data. My written testimony submitted for the record has more details on recent plans and directives that signal the centralization of Chinese state power of information flows within and beyond China's borders.

The Chinese leadership seeks to control data as both a strategic and an economic asset. There are concerning national security risks. Beijing is already presumed to have sensitive national security information from the theft of personal records of roughly 20

million individuals from the U.S. Office of Personnel Management, as my colleague Justin Sherman has testified. If that location, health, and social media data were to be acquired on the open data market—and combined with what Beijing already has—China could target individuals in sensitive government national security positions and the military for manipulation, coercion, and blackmail.

This is particularly concerning from a counterintelligence perspective. As Chinese online services and network infrastructure grow in predominance around the world, it is possible that the Chinese Government could use this position to monitor data processes abroad, just as the United States had done—as shown by Edward Snowden—in utilizing data transmissions across U.S. intelligence networks.

We simply do not know what value and harm data created now will hold in the future. But we must grapple with the implication of the CCP gaining control of information flows beyond China's closed Internet ecosystem. I have the following recommendations.

First, the analogy of data as the new oil is false and leads to bad policy. It assumes that data is a finite state resource and, as such, efforts by both Beijing and Washington to hoard and wall off data from each other will only lessen national power, not increase it. Instead, Congress should mandate stronger cybersecurity protections and basic standards for what data can be collected and retained in a comprehensive Federal privacy law to protect Americans' sensitive data, not just from sophisticated state hackers, but also from the unregulated industry of data brokers around the world trading in consumer data without transparency or control.

While comprehensive Federal privacy law moves slowly amid much debate, having baseline rules for the data broker industry would close off a prime target for exploitation now. Currently, there is nothing in our regulatory structure that would prevent the Chinese Government from buying American citizens' data. That is why bans on Chinese software applications will not make us more secure or safe. Even if TikTok, for example, were an American-owned company, it could still legally buy that data on the open market.

Given this, American data is shockingly exposed and will remain that way as long as restrictions on data flows only focus on specific companies deemed adversaries. The United States should work with like-minded governments to develop a common set of standards and safeguards, perhaps building off of the initiatives put forward by the Japanese Government, known as "data free flows with trust." And I have some more specific recommendations in my written testimony.

But in conclusion, inaction by the United States in offering an affirmative, compelling vision of U.S. data governance in its own right will only make the United States less secure, less prosperous, less powerful, and allow space for Chinese companies controlled by the CCP to flourish.

Thank you.

[The prepared statement of Ms. Sacks appears in the appendix.]

Senator WARREN. Thank you very much, Ms. Sacks.

And now, Ms. Gray, you are recognized for 5 minutes.

STATEMENT OF STACEY GRAY, SENIOR COUNSEL, FUTURE OF PRIVACY FORUM, WASHINGTON DC

Ms. GRAY. Thank you, Chair Warren, Ranking Member Cassidy, and members of the subcommittee, for the opportunity to testify today. My work at the Future of Privacy Forum is in U.S. law and public policy related to emerging technology and consumer privacy regulations. And specifically, I have been asked to speak to the topic of data brokers.

Privacy advocates, the Federal Trade Commission, and members of this and other Senate committees, have long called for greater transparency and accountability in the data broker industry, and regulation is long overdue. Many of the most influential reports published almost a decade ago have influenced the debate. And since then, much has changed. There have been significant advances in machine learning and artificial intelligence. Adoption of consumer technology has also become universal with 97 percent of U.S. adults using smartphones, and most families having, of course, many additional devices.

The legislative landscape has evolved more slowly and has largely not kept up. Since 2018, California and two other States have passed consumer privacy laws. Three States have established limited data broker-specific regulations. And many of these have focused on transparency to the establishment of data broker registries, while others, such as the California Privacy Rights Act, codify broader consumer rights to opt out of the sale and sharing of data. Much more work remains to be done.

I would like to make two points regarding data brokers and then give recommendations. The first point is that defining the very term "data broker" has been an ongoing challenge, because it encompasses a very broad spectrum of divergent companies and business activities. The leading definition includes any business that collects and sells personal information of a consumer with whom that business does not have a direct relationship. Many hundreds of businesses fall under this definition and use data for a wide range of purposes—as my fellow witness, Mr. Sherman, pointed out—including marketing and advertising, people search data bases, fraud detection, identify verification, and risk scoring. Some of these activities directly benefit consumers, such as the use of data to protect a bank account against fraudulent activity, but others primarily benefit the purchasers or the users of data, such as advertisers, with fewer, or little or no accompanying benefits to individuals or society.

Second, the lack of a direct relationship with consumers, characteristic of the data broker industry, is at the heart of concerns around privacy, fairness, and accountability, but it also presents one of the greatest challenges for crafting effective data privacy regulation, and I will briefly explain why.

Any business with a direct-to-consumer relationship—such as a restaurant, a hotel, a retailer, even a social media network—can collect large amounts of personal information about U.S. consumers today, directly or by purchasing it. And in some cases, those third-party companies can exercise enormous influence in market power, as we have heard. However, there is still some degree of account-

ability to users who are aware that the companies exist and can delete accounts, or raise alarms.

In contrast, a business lacking a direct relationship with consumers typically does not have the same reputational interest, incentives, and in some cases legal requirements, to limit the collection of data and protect it against misuse. However, a lack of consumer relationship also means that businesses engaged even in legitimate data processing, or socially beneficial data processing, cannot rely on traditional historical privacy mechanisms of notice and choice. Meaningful affirmative consent, or opting in, might be impractical or impossible for a business to obtain in some cases, while opting out after the fact tends to be both an inadequate safeguard and impractical for most consumers to navigate.

We know that consumers can become overwhelmed with choices and often lack the knowledge to assess future risks, complex technology, or future potential secondary uses. So what does this all mean? First and foremost, Congress should pass baseline comprehensive privacy regulation that establishes clear rules for both data brokers and first-party companies that process personal information from U.S. consumers. It should address the gaps in the current U.S. sectoral approach to consumer privacy, and it should incorporate, but not rely solely, on consumer choice.

A privacy law should also codify clear limits on the collection of data and apply accountability measures such as transparency risk assessment auditing, limitations on the use of sensitive data, and limits on retention.

In the absence of comprehensive legislation, there are a number of other steps Congress can take to address risks related to privacy and data brokers, including empowering the Federal Trade Commission to continue using its unfair and deceptive trade practices authority to fund and staff the establishment of a privacy bureau; limiting the ability of law enforcement agencies to purchase information from data brokers; enacting sectoral legislation for uniquely high-risk technology such as biometrics and facial recognition; or updating existing Federal laws such as the Fair Credit Reporting Act to more effectively cover emerging uses of data.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Gray appears in the appendix.]

Senator WARREN. Thank you very much, Ms. Gray. I appreciate all of your testimony here.

And now I recognize Senator Whitehouse for 5 minutes of questions.

Senator WHITEHOUSE. Thanks very much, Chair Warren. I appreciate it. This is a fascinating and important hearing, and I am delighted to have these terrific witnesses here.

Facebook and Google have been profiting off some of the worst propagators, I guess you would call it, of climate denial. The Center for Countering Digital Hate finds 10 fringe sites that fuel 69 percent of climate disinformation on Facebook. So with a little bit of focus, they could address this problem if it is only 10 major propagators. Google itself makes millions from Google ads that it runs alongside climate denial content, as if it were legitimate.

Mr. Lynn, can you talk a bit about how our information ecosystem suffers when a handful of companies control what people

see, and how they perceive reality; what a communications monopoly means in a world in which there is so much deliberate climate denial propagated by industry?

Mr. LYNN. Thank you, Senator. It is a fundamentally important issue. And what we see today—one way to answer the question is to understand that Google and Facebook today are the communications corporations of the 21st century. These are the AT&Ts and the Western Unions of the 21st century.

AT&T and Western Union were prohibited by law from manipulating how people spoke to one another. Google and Facebook—their business model is based on manipulation. The reason they take in the data is in order to manipulate you. They are massive manipulation machines. The way they make their money is by renting out the manipulation machines and calling the money that they receive—they call it "advertising." So what we have is, in the midst of our society, rather than sort of networks that connect people and empower people to speak with one another and interact with one another, we have machines that are designed to set people into conflict with one another, to feed them false information, to determine how people vote, and what we have——

Senator WHITEHOUSE. So they are ready, willing, and able tools for false information propagators.

Mr. LYNN. When they were established, I think the idea was that these systems would be used by Proctor & Gamble to sell soap and Tide. What they now do, however, is they rent themselves out to Vladimir Putin, to climate deniers, to the Chinese Communist Party—you know, whoever comes along.

Senator WHITEHOUSE. Let me switch to data that you are talking about, that they have gathered, and ask the witnesses who spoke about data privacy and data brokers, what does somebody listening to this hearing need to know about what companies know about them, what data brokers can extract from what companies know about them to sell, and to what extent that information can be individualized back to them, potentially by foreign bad actors, foreign governments? Mr. Sherman, go ahead.

Mr. SHERMAN. Data brokers know everything about pretty much every American—where you work, where your kids go to school, how much money you make, your race, your religion, your sexual orientation—and their entire business model is that they can target this to individuals. They sell this data. They offer advertising, like Mr. Lynn mentioned, for the purposes of targeting specific individuals. And so these profiles are out there on the open market for sale.

Senator WHITEHOUSE. And if you were running a psychological warfare operation involving American public officials, or American CEOs, or various kinds of decision-makers in American society, how valuable a tool would that be if you were a foreign government, to be able to look into people's lives and understand not only what you directly know, but what conclusions you can realistically draw about what their shopping habits are and so forth?

Mr. SHERMAN. Incredibly valuable for that. You can buy databases right now for what people search online, how they vote, what they think. And so it is all out there on the open market.

Senator WHITEHOUSE. My time is up. Thank you, Chair Warren.

If I could, I would just add one question for the record so as not to take up too much time. But one of the things we hear in the Finance Committee a lot—our chairman has joined us, Chairman Wyden, and he is very active on this subject—is that if we make big American companies pay a fair share in taxes, that will make them uncompetitive against foreign companies. And that is the argument our Republican friends always make. What they ignore is that when the big American companies do not pay a fair tax burden, that gives them competitive advantage over smaller American companies. And obviously that plays out in this tech world, because you have Apple and Google, who have come up with, you know—what do they call them?—the double Irish and the Dutch sandwich, and all these peculiar tax tricks that they use to avoid paying their fair share. And I would be interested in your views, again in writing and not now because my time has expired, on how that creates competitive disadvantage with potential competitors against them for competitive advantage in the U.S., and to what extent it locks in, financially, some of their monopolistic power because, frankly, they put themselves into a place where they do not have to pay taxes, but all their competitors have to—well, all their smaller competitors have to.

Thank you very much. I appreciate the attention to that question in writing.

Senator WARREN. Thank you, Senator Whitehouse; a very thoughtful question.

And now, Senator Cassidy, I think you are up.

Senator CASSIDY. Thank you, Madam Chair. Thank you all for testifying.

Mr. Sherman, I cannot help but note we are on Pearl Harbor Day, and our country has come to venerate this day, but also to honor the service men, women, others in the clandestine services, et cetera, who offer themselves to protect us. And we rightly make tremendous investment in the VA hospitals and other services to include a suite of benefits to help these folks who have offered so much.

But I am struck when you speak about how a data broker can sell personal information on active military personnel—I assume on veterans as well—to allow a company to basically rip them off of these benefits that they would ordinarily receive.

How and where—how does someone get such information? What is the price of one military profile? And is it safe to say that companies are getting rich off of using this data to trick our service folks into giving their benefits over to the company, a marginal benefit for the service person or the veteran, but a great benefit for the company, and the taxpayer gets ripped off? I have at least three questions in there.

Mr. SHERMAN. Data brokers are absolutely profiting off the vulnerability and insecurity of the U.S. and its citizens. That includes veterans. That includes members of the military. I do not have a figure in front of me for the cost of one of those profiles, though I can follow up on that, but I will say it is very, very easy to find this information online and to purchase it.

Our research has shown that many of these companies offering this data—whether it is military personnel, low-income individuals,

whatever it is—do not do much customer vetting. They are basically willing to sell to most entities with a check and an email address. And so at the end of the day, it is all too easy for people to use this, as they have, to scam veterans and to create risks to national security.

Senator CASSIDY. Now how do they get this information? How do they know that someone is active military, et cetera?

Mr. SHERMAN. Because the collection and buying and selling of this information is so unregulated, it is very easy for these companies to put pieces of information together to figure out who you are, much like they might track where you go during the day, and what you spend, to figure out how much money you and your household make. They might look at where you travel to figure out if you are in the military.

Senator CASSIDY. Would the data brokers themselves have location data that would obviously indicate that I am spending my night on base every night, except for an occasional deployment in some place which seems to be a military zone, or are they buying this location data from others?

Mr. SHERMAN. Likely both. Many companies collect this data directly from people's phones, whether you are working on the Hill, or in the military, or even in an intelligence agency, and they also buy this data from other companies.

Senator CASSIDY. Now I am a physician, so let me toss this out, and if one of the other witnesses on data brokers wishes to address it, please do. The thought has occurred to me that we have HIPAA penalties if I, as a physician, would reveal that someone was HIV positive, or had a mental illness. But one of you specified that the mental illness is actually well known, which makes total sense to me. If you have location data that shows that somebody goes to work every day at a place which is known to be a mental health clinic or an HIV clinic, a treatment clinic, that would mean the person is probably employed there. But if they go every 2 weeks, or every month, and then they go to a pharmacy afterwards, they could infer that the patient has either got HIV or a mental health issue, or some other illness. Those are often stand-alone clinics, and so they could infer this.

Is this kind of a correct kind of guess at how all this is done? And does this not kind of violate, certainly, the spirit that seems almost the letter of the HIPAA regulations? Mr. Sherman, please start, and I will ask Ms. Sacks and Ms. Gray to comment.

Mr. SHERMAN. That is exactly the problem with data brokers, Senator. They can basically dance around the very few, very limited privacy laws we do have, by proxy data, by running algorithms to get that information anyway.

Senator CASSIDY. So this would be what you were speaking of as "inferring." They can infer, even if they do not directly collect.

Mr. SHERMAN. That is correct.

Senator CASSIDY. And they sell that data to those who might be interested in marketing to someone who has mental illness or HIV, or something such as that?

Mr. SHERMAN. Yes, they do that.

Senator CASSIDY. Ms. Gray or Ms. Sacks, do you have any further comments on that? Because as a physician, that greatly of-

fends me, because the idea that we can infer that which is otherwise restricted is—again, it just violates that which I always kind of had in my DNA as a physician in terms of protecting patient privacy.

Ms. GRAY. I would characterize that the same way, Senator. And in fact, this is one of the major problems that needs to be addressed through nonsectoral comprehensive privacy regulations, because data collected increasingly through apps, wearable devices, and fitness devices, and devices like bicycles and electric vehicles, can all lead to the types of information sharing that you are describing. Some of it is directly collected from consumers, and some of it would refer to large data sets.

Senator CASSIDY. Your answer implied that my car, which is connected to the Internet, theoretically at least could have an app that could—theoretically at least, a data broker could purchase the information related to my location data from a car which is, quote/unquote, "a smart car," although I do not know why you would have to do it from an app that was on somebody's cellphone. But is all that true?

Ms. GRAY. All of that is true. Much of the commercial location data that is in the industry, some from mobile apps and some from cars, is tied to device IDs. For example, some of it is actually from apps when it claims to measure things like driving behavior, and all of that information is very valuable for a number of purposes, some of them benign like transportation analytics in urban planning, and some of them more harmful.

Senator CASSIDY. I will have a second round, but I yield back, Madam Chair.

Senator WARREN. All right. Thank you very much, Senator Cassidy.

Senator Wyden?

Senator WYDEN. Thank you, Senator Warren. And I want to thank you and Senator Cassidy for getting into these issues. Senator Cassidy just mentioned the modern car, and the modern car is a computer on wheels. And I have been investigating now for years, as chairman of this committee, the sleazy, unregulated world of these data brokers. And in several instances we blew the whistle on government agencies that were too-eager consumers for this information, and we pushed Apple and Google to finally get some of the sleaziest data brokers out of their stores, and out of their businesses. And I am glad we are making progress, but we have a lot more to do.

I want to start with you, Mr. Sherman. You made an important point with respect to how foreign governments can acquire Americans' data to run disinformation campaigns, identify undercover government personnel, blackmail government employees—and I have been working on legislation for some time now to deal with this threat, which will be introduced shortly.

My first question to you, Mr. Sherman: do you agree that Congress should enact legislation to strictly limit the exports of Americans' personal data to high-risk foreign nations and companies to address what, in my view, are demonstrable national security threats?

Mr. SHERMAN. There is a huge—a huge—national security threat here, and Congress does need to control the sale of data to foreign companies, citizens, and governments. As you referenced, it is all too easy to get that on the open market.

Senator WYDEN. Very good.

Ms. Gray, we have also been looking at this whole issue of how U.S. Government agencies bypass the courts by buying American data from data brokers. And so I have introduced bipartisan legislation, The Fourth Amendment Is Not for Sale, to close these loopholes.

Do you agree that the governments' exploitation of these loopholes is a serious problem? And do you agree that Congress ought to close these ever-yawning loopholes by passing our legislation?

Ms. GRAY. Absolutely, Senator. The Fourth Amendment Is Not for Sale Act is a very strong model. That is exactly what is needed right now.

Senator WYDEN. And tell us, if you would, how this connects with privacy issues? Because I have also introduced another piece of legislation, the Mind Your Own Business Act. Had that become law, I am of the view Mr. Zuckerberg would have already faced major sanctions for behavior connected to privacy violations.

But how does this whole area connect with privacy? Because on the Finance Committee, we are increasingly looking at privacy issues. For example, we feel very strongly that the wealthy tax cheats right now are about as likely to get audited by the government as getting hit by a meteor. We have to do more to root out that corruption, but we can do it in a way that is consistent with protecting people's privacy. I am a privacy hawk. I will put my privacy credentials up against anybody in the United States Senate.

Tell us how this whole field connects with the broader expanse of making sure that we protect people's privacy.

Ms. GRAY. Sure. Well, one of the issues is the sheer scale and volume of the modern commercial data ecosystem. And it is becoming increasingly untenable, I think, to separate the related fields of law enforcement and national security uses of data and commercial collection and uses of data that originate for a particular purpose but end up being used for secondary purposes, and being used by government agencies.

Senator WYDEN. It is striking, because I am also on the Intelligence Committee, and I have come to the conclusion that privacy is a massive economic and national security issue. And you cannot just separate these all out in separate boxes. And this question on economics and national security and privacy are directly linked. I want to thank all of you for your good work. I appreciate Senator Cassidy's interest in this. Senator Warren has been a long-time leader of making sure that we hold these major economic forces in our country, our largest companies, accountable.

And by the way, I was in Sisters, OR, and people were asking me about these issues. Being successful and ensuring that there is accountability are not mutually exclusive. We can do both. Of course we want our businesses to do well. Of course we want them to be profitable. But they can also be accountable to key American values like protecting people's privacy. And I want everybody to

know I am so pleased that Senator Warren has given us this chance.

These sleazy, unregulated data brokers, I want to put them on notice today: we are going to stay at it until there are serious consumer protections. Whether it is The Fourth Amendment Is Not for Sale, or other kinds of measures, there is going to be accountability in this field.

Thank you, Senator Warren.

Senator WARREN. And thank you, Senator Wyden. And thank you for your long-time leadership in this area. This is how we are going to make changes, so thank you. Thank you for all you have done.

I want to talk about another aspect of the issues that we have raised today, and that starts over 100 years ago when Congress passed our first antitrust laws to protect both local businesses and to protect our democracy from powerful dominant corporations that would undermine competition, crush workers, and gouge consumers.

But starting in the 1970s, our government reversed course. Corporate CEOs and lobbyists pushed the idea that mega-mergers and corporate behemoths were actually good. Economists used complicated models to say, gee, if we just let big corporations get even bigger, they would be more efficient, they would lower prices for everyone, and they would compete better on the world stage.

Unfortunately, too often that is not what happened. Take the semiconductor industry for an example. Hedge fund managers took over our biggest chip manufacturer, Intel. Intel grew its market size, cemented its dominant position through anticompetitive and predatory practices. Then, having killed the competition, the managers were free to weaken Intel's fundamentals with impunity. I will give you just one example.

From 2001 to 2010, instead of spending more money on innovation—remember, we are talking about the semiconductor industry, right? You have to stay up. Instead of spending more money on innovation, on new ideas, on more efficient manufacturing here in the United States, Intel's managers spent $48 billion on stock buybacks. They boosted share prices and executive pay, while they hollowed out a once-great company.

So, Mr. Lynn, let me start with you. You know a lot about the semiconductor industry. Did consolidation, particularly the growth of Intel, lead to greater efficiency?

Mr. LYNN. No, Senator, the opposite.

Senator WARREN. Did it lead to lower prices?

Mr. LYNN. Absolutely not, Senator.

Senator WARREN. Then did it at least make Intel a stronger competitor on the world stage?

Mr. LYNN. The opposite, Senator.

Senator WARREN. So in your assessment, what exactly did happen as a result of Intel's growing dominance in its sphere?

Mr. LYNN. First, one of the things—you mentioned $48 billion that Intel paid out between 2001 and 2010. The dominance allowed them to pay out much more between 2010 and 2020—actually $130 billion over the last 10 years. So the looting and sacking of this cor-

poration grew much faster and more aggressive over the last 10 years.

But this results in higher prices for the chips. It results in more power—you know, concentration of power over workers. And it is not just the people on the assembly line, but it is also scientists. It is also the engineers. And these are the people that we count on to develop a better future, and we have concentrated power over them. So we see less innovation as another effect. The other effects include this extreme concentration of capacity that we have seen in corporations like TSMC in Taiwan. And this extreme concentration—here you have all of a certain kind of chip, you have all your eggs in one basket—means that the system itself is fragile and subject to catastrophic failure.

What you have is a system that gives other powerful countries like China power over the people who depend on that capacity—for instance, by threatening to disrupt shipments in and out of Taiwan. It leads to these massive shortages, these structural shortages that we see that are leading to the shutdown of assembly lines all around the world—not just in America, but we are talking about Ford, a 50-percent decline in production of cars in Q2. We are seeing Toyota, a 40-percent decline in production of cars in Q3. This equals vastly higher prices for newer cars, vastly higher prices for used cars, vastly higher prices for rental cars, and a lot of dirtier cars on our streets because we cannot replace them with newer, cleaner cars.

Senator WARREN. So consolidation clearly did not strengthen our semiconductor industry, but consolidation, or lack of competitors in this field, did create this supply chain crisis that the pandemic has exposed. And now, as you rightly point out, without semiconductor chips, other manufacturers like auto companies cannot meet demand. They are furloughing workers at the same time that orders are stacking up, all because they cannot get the chips that U.S. manufacturers once supplied all around the globe.

And what has been management's response to this? The same executives who exacerbated this crisis by failing to properly invest in their operations in infrastructure, now are asking Congress to bail them out so they can make the investments that they should have been making years ago.

Excessive concentration is a real problem. It is also a problem in our domestic logistics and supply chain operations, and it applies, obviously, to big tech firms.

Ms. Brown, I would like to go to you, if I can. During the 4½ years that you have worked at Amazon, Amazon has grown bigger and bigger. Its profits have skyrocketed. So let me ask. In your personal experience, have Amazon's logistical operations improved, or have things just gotten worse, and particularly with the COVID crisis? Can you speak to that?

Ms. BROWN. Yes, absolutely. It has definitely gotten worse as the years have gone on, especially with the pandemic. It is all about this pushing out as much as possible frame of mind. It used to be about the quality that we are giving our customers. That was the number one thing. But now Amazon really does not care very much. They do not care about how their workers are trained. It is all about speed and quantity. So when it comes to my facility with

delivering food, you know, we deliver broken eggs, crushed bread. We end up sending out a lot of spoiled food and everything.

So a lot of us want to do good work, but it is like really frustrating because, you know, we are at a limit for doing such things. And for Amazon, they are getting rich. They preach the customer obsession, but it is not good for customers at all. And it is not good for hardworking people at the facility centers either. Workers cannot do their jobs well because Amazon wants to make more money, and that is the bottom line for them—about as much product as they can get out, and more money. And if you attempt to try and do these things like giving customers good quality, actually practice customer obsession, you end up actually getting written up and then eventually terminated. So the bottom line for them is all profit.

Senator WARREN. Thank you so much, Ms. Brown.

Amazon's profits have exploded during the pandemic, even though deliveries have been significantly delayed and services have become more expensive. In a competitive marketplace, Amazon's rivals would be able to compete on these factors—providing more reliable service, or lower prices, or a better work environment. But because there is no competition, consumers get higher prices and worse services, while Amazon gets even richer.

Markets can produce lower prices. Markets can produce more reliable products. Markets can produce robust supply chains, but only if there is competition. When giants are allowed to dominate an industry, everyone else pays. Thanks very much.

Senator Cassidy, I recognize you.

Senator CASSIDY. Thank you.

Ms. Gray, I will have a series of questions for you right now. I finished in my last line of questioning speaking about how location data could establish somebody as being HIV positive, or having mental illness, or being military personnel, et cetera. I understand the organization with which you work considers location data to be personal information that should be regulated. Can you kind of comment upon that, please?

Ms. GRAY. Certainly. Commercial location data of the nature of the data that is frequently bought and sold in the data broker industry is often tied to, not necessarily name and contact information, but device identifiers such as a device ID related to a mobile phone. That has led many in the industry to claim at times that the data is not personally identifiable, that it has been anonymized, or de-identified to a certain extent. And while the risk may have been lessened, the facts remain that persistent, precise location information over time is very straightforward to relate back to an individual person because our behaviors and our movements are unique over time. And so that is one of the unique challenges specific to the commercial location data industry.

Senator CASSIDY. I am sorry. I had to stop my video. My computer is about to die. I apologize for that.

Secondly, related to that, what is the difference between suppressing data—I call my data broker. I contact him. I say I do not want my data to be marketed, et cetera. How do I ask them to get rid of it? And I am told that oftentimes they do not get rid of it.

They suppress, but suppression is different than deletion. Can you elaborate on that, please?

Ms. GRAY. Sure. Sure, Senator. Suppression is an industry term that is frequently used for the purpose of describing when a company maintains a list of consumers or individuals or devices for the purpose of excluding those individuals or devices from their products and services, but not necessarily deleting the underlying data.

And there can be a range of reasons to do that. One of them, for example, is to comply, in an ongoing manner, with deletion or opt-out requests that are required by some of the emerging privacy laws. For example, data brokers that automatically collect large amounts of information from public records may receive a request to delete data from an individual, actually delete that data, but be unable to continue to delete data on that individual in the future unless they retain a limited suppression list.

Senator CASSIDY. In that case, you suggest that that is actually a positive thing in which they would be using the suppression list to mark this. So is it a positive or a negative that data is merely suppressed as opposed to eliminated?

Ms. GRAY. I would say, Senator, it depends on the use case. There are other higher-risk marketing and advertising use cases related to suppression lists. As we heard, for example, some marketers wish to exclude certain segments of the population from receiving advertisements that may be deemed offensive. For example, a list of households associated with the loss of a child, or the loss of a pregnancy, may be a list that a marketer uses to exclude those households from receiving marketing and advertising related to baby products. That is an example.

So it depends on the use. And there is some risk associated particularly with those more sensitive categories of information just by the maintenance of a suppression list.

Senator CASSIDY. So there is clearly a nuance here. And frankly, if we are going to attempt to address that in legislation, we would need someone such as you and your organization to help elaborate on that nuance. Because it actually sounds like it could be a positive thing, although you suggest that there is a potential negative as well.

So with that said, let me ask you about the next thing, because I think this is another nuance. In your written testimony—I believe it was you who spoke of the fact that this big data can be very helpful. You wish to look at, just to give an example—I am not sure it ever came to full fruition, but it has in other countries—using location data to establish who may have been at a conference at which COVID is known to have infected people, and so therefore you can do that.

I know after Mardi Gras in March of 2020, people used location data to figure out where everybody went back to from New Orleans after Mardi Gras and where people had come from, and they were able to establish that COVID came to New Orleans from both the Northwest and the Northeast.

So clearly people are using data in another sense. So what is the nuance between using the data appropriately for public health purposes, as an example, maybe to let me know how congested the

highway is, and should I take this route or should I take another, as opposed to using it somewhat nefariously, if you will?

Ms. GRAY. You are right, Senator, to point out that there are essentially good uses and bad uses of this data. For example, in the early stages of the COVID–19 pandemic there were large commercial data sets held by both first parties, including Google, and members of the commercial location data broker industry, that provided aggregate analyses of how people were moving around to help assist public health efforts.

So, there are both good and bad use cases. One of the nuances here is that, when we talk about fair information practices and privacy and having a realm of private life, there are increasing concerns around the fact that data is collected in the first place—even when it might be later used for good or beneficial purposes. There is, nonetheless, a zone of private life that I think most agree should not be intruded upon.

In other cases, most consumers are aware that they are sharing location data—for example, for a particular service—and not aware that it may be re-used for a secondary or incompatible purpose. And things like commercial research and public health purposes are technically incompatible purposes, because that is not the reason that the data was necessarily provided. And so crafting nuanced exemptions here related to sources of data, sensitivity of data, risk related to harms to individuals and groups and society, are all part of crafting effective regulation here.

Senator CASSIDY. Thank you.

And I will finish with this and turn it back to you, Madam Chair. But I sincerely think, observationally, it cannot be disputed, that we can come up with better legislation from a hearing such as this that takes information from those who are stakeholders and academics and others who analyze and try and get those nuances down.

Again, I ask you to contact my staff afterwards with some idea of those nuances. And that is an open invitation to everybody on the panel.

Madam Chair, I turn it back to you.

Senator WARREN. Thank you, Senator Cassidy.

So, as Attorney General Racine pointed out, Amazon controls 50 to 70 percent of the $430-billion online market for consumer goods. Prices for everything from light bulbs to mattresses to motor oil are going up on Amazon. And the question is, why is that happening? A huge part of the reason is Amazon's deliberate exploitation of its market dominance to squeeze more dollars out of consumers and third-party sellers alike. In other words, Amazon is taking a big bite out of the middle.

So one of our witnesses, Attorney General Racine, filed a lawsuit this year against Amazon for this very reason. And a particular focus of the lawsuit is the impact of something that Amazon calls its "fair pricing policy."

And if I can, Attorney General Racine, I would like to follow up on the example you gave to illustrate this policy. So, let's say if I make earphones and sell them for $100 on my own website—I just want to make sure we are clear on all this—if I want to sell them on Amazon to access this huge marketplace online and extend my

reach, I have to pay Amazon's fees and agree to their terms. And my understanding is that Amazon's fees can be as high as 40 percent of the cost of these goods.

So, thanks to these fees—let's just pick that example—I have to increase my prices to ensure that I can still turn a profit. So now instead of charging $100 for these earphones, I may now have to charge $140. But the worst part is, I now also have to charge $140 on my own website, and on every other platform where I am trying to sell my headphones. These inflated prices crush American consumers.

So, Attorney General Racine, I want to return to your opening remarks. I want to go back over the example you talked about, but you also mentioned how Amazon forces wholesalers to pay more as well. So I did the consumer part. Can you say a little more about how they are doing this with their wholesalers as well?

Mr. RACINE. Sure. And you have captured it exactly right, Senator, which of course is no surprise to me. With respect to wholesalers, Amazon again forces these first-party sellers, I will call them, to reach an agreement with them in regards to what the price is going to be. And here is the deal. If Amazon lowers its retail prices to match or beat a lower price for that initial good on the online marketplace, the wholesaler is forced to pay Amazon the difference between the agreed-upon profit that they made with Amazon and the money that Amazon realizes after it lowers the retail price.

In short, Amazon has profit protection at the cost of the first-party seller. I do feel compelled to also mention—and do not take my word for it; look at the April 23, 2020, *Wall Street Journal* article written by Dana Mattioli that talks about how Amazon has scooped up data from its own sellers, these first-party sellers, to launch competing products. So not only are they crushing these first-party sellers with these unlawful agreements—that is what we allege—but they are also using data around the popularity and selling of these products to launch competitive products against these first-party sellers.

Amazon cannot win enough without cheating, and that is why we are suing them.

Senator WARREN. So this just knocks me out. In a typical collusion case like price-fixing, competitors illegally agree to charge higher prices. And when they get caught, they can actually go to jail under Federal law. But Amazon accomplishes the same thing in-house. And its higher fees are inflating prices on its own platform as well as in stores and on other websites through these anti-competitive contract provisions with third-party sellers. And the result is, prices go up for millions of Americans, and Americans cannot see it because there is no place else to do the price comparison to see what is happening here.

This price increase is entirely hidden from consumers because it looks the same wherever they go. And it just shows up as inflation.

Mr. RACINE. Can I give you numbers?

Senator WARREN. Please.

Mr. RACINE. I think it is going to make your point. So between 2014 and 2020, Amazon's revenue from third-party seller fees and charges grew from $11.75 billion to over $80 billion. This year,

Amazon is estimated to reap over $121 billion in fees from third-party sellers. They are doing this because it is extremely profitable. They do not care that consumers are paying far too much for goods, and they are not doing what they say they are doing, which is focusing 100 percent on consumers. They are focused 100 percent on utilizing their market power to extract every bit of profit that they can.

Senator WARREN. So the question, obviously, you have to ask is, how do they get away with this? And what I would like you to focus on, if you can, Attorney General Racine, is how Amazon's dominant market position contributes to this kind of pricing power that has been felt throughout our economy.

Mr. RACINE. I think the example with the headphones that I gave, and that you accentuated, frankly, and made better, is the best example. And that is, that what Amazon does is, it artificially builds its commissions and fees into a product that ensures that that embedded profit that it has, frankly, continues throughout the electronic mini-mall or major mall in such a way that no one, not even you, nor me, the creator of my own headphones, can sell my headphones for cheaper than what Amazon and we essentially were forced to agree to sell them at.

And why do we engage in that agreement? Because they own 50 to 70 percent of the marketplace. Look at it as a toll booth keeper. The road only leads to the toll booth. The toll booth keeper can raise those prices, and you as the driver have no choice but to pay whatever they are asking if you are trying to get down that road.

And we think that is illegal. We appreciate the work of this great committee. We are going to make law in the courts, and we look forward to helping with respect to legislation.

Senator WARREN. Well, I very much appreciate that. I appreciate your point about 50 to 70 percent of the marketplace that they already own. And yet, Amazon keeps growing. And they do not just grow by sales, they continue to acquire.

So back in May, Amazon announced its proposed acquisition of MGM Studios. That would be an $8.45-billion deal. Now I wrote a letter to the FTC Commissioners asking them to review the deal thoroughly and to evaluate how the deal might affect workers and prices in other markets in the Amazon ecosystem.

Mr. Lynn, even if the FTC wanted to oppose this huge merger, it would be a challenge to successfully block it—notwithstanding everything that we have already heard from the Attorney General, and that others have testified about. Can you explain why that is?

Mr. LYNN. Yes, thank you, Senator.

Well, first it is going to be very expensive in terms of the time, you know, for this limited staff that the FTC has. They are going up against the richest corporation in the world, the most powerful corporation in the world, a corporation that can throw wrench after wrench after wrench into the mechanism.

It is also very expensive in terms of the expertise they have to pay for—economic expertise. They have to put millions and millions of dollars, often, into the kitty to pay for economists. And this is even with President Biden's renunciation of the Bork consumer welfare philosophy. The legacy—because of the nature of the law—of the consumer welfare philosophy and its focus on efficiency con-

tinues to shape how the judiciary is going to look at this issue. And they have to be ready with this very expensive expertise.

The third reason is, it is just very difficult to communicate with judges in the stylized language of consumer welfare, of efficiency. You know, this is an issue of power. It is an issue of democracy. It is an issue of human liberty. And they are being told that we have to talk about this in terms of efficiency.

Judges are trained to use common sense to enforce the law, to ensure the rule of law. And when you are using consumer welfare framing, you are speaking nonsense.

Senator WARREN. Well, I really appreciate that.

You noted earlier that President Biden has selected two outstanding experts, Lina Khan and Jonathan Kanter, to lead the antitrust efforts at the FTC and at DOJ. These are people who believe in competition. And they are going to build strong cases. But Congress needs to do its part. We need to make sure that they have the resources, and we need to make sure that they have the tools to be able to wage these battles. Otherwise, we are just going to continue to see companies like Amazon squeeze consumers, no matter who is President or no matter whatever crisis of the day we are dealing with.

So, I think it is important that we step up on our side too. Thank you.

Senator Cassidy, back to you.

Senator CASSIDY. Thank you. It appears 5-minute limits are off, so I may go a little bit longer.

Senator WARREN. I apologize. Please go as long as you need to, Senator Cassidy.

Senator CASSIDY. I have a series of questions for you, Ms. Sacks. First, your testimony speaks of the need to have kind of a comprehensive arrangement between countries, or blocks, if you will, to take the EU as a block, in order to have some sort of agreement. I think I am summarizing, although I am sure you would find nuance there.

Now the reason I say this is that I have been told that the general data protection regulation of the EU risks making the EU a digital colony to the U.S. or China. It is so restrictive that the big data sets that are required to enhance research on AI are almost impossible to construct. I do not know if that is true. You know far more than I do. But nonetheless, that is what I am told.

So, there is something here. How do we allow those sort of data sets required for AI to be constructed, the big data sets—if you agree that that is the case—and then how do we have a governance that would exclude bad actors—and I think folks see China, with all their cyber-espionage, as being a bad actor—but nonetheless get the fruits of this big data?

And you had mentioned specifically the Japanese with the "data free flow with trust" paradigm. So I think I have given you kind of a lot of directions to go in your answer, and I will turn it back to you.

Ms. SACKS. Thank you, Senator Cassidy.

I think you put out a key point here, which is that U.S. security and prosperity relies on access to large international data sets. But

as with other areas of the data broker legislation that you mentioned with Ms. Gray, this one will have nuance to it.

So how do we allow global data flows, but with the right safeguards in place, both at home and internationally? And I think that a big, important step here is making sure that we get our own house in order first. The transatlantic data flow relationship will be key, and it is important that the U.S. put forward its own vision of data privacy first, but this should not be a copy-and-paste of GDPR. And the topic of this hearing focused on antitrust, I think gets at the challenge, which is that one of the most important critiques of GDPR is that it may only end up serving those companies that are wealthy enough to comply with a very heavy burden that comes along with it.

So it reinforces the concentration of power in big tech, while there still may be limitations on meaningful privacy protections. I think that the Japanese "free flow with trust" model is a compelling way to think about how like-minded countries can come together to put in place certain standards that would allow data to flow with certain conditions in place. And perhaps there can be a certification regime drawing on some of the privacy protections already outlined in the OECD guidelines.

So there are a number of directions, and this will require nuance as well, and I look forward to helping support efforts of the committee to do that.

Senator CASSIDY. Now, does that require an international treaty? I mean, you are not—I am assuming you may not be an international trade attorney, but can we just basically pass legislation which is in alignment with others without having a formal treaty? Or do you have a sense of how we would go about this OCED kind of a collaboration?

Ms. SACKS. You know, I think this is one that I am going to need to get back to you on, on the specific nuts and bolts of the various tools that are in place. If it is all right, I will follow up with you and your staff after.

Senator CASSIDY. I appreciate that.

Now, Ms. Sacks, tell me—we have learned that the Chinese Government, as an example, could purchase information on U.S. military personnel, and presumably location data as well. It would be kind of interesting to see where people are deployed, would it not, just to see the concentration of force, et cetera, what type of force, if you know from other information what branch of the military they are in?

But do other countries have that same sort of lax attitude regarding allowing the legal purchase of information upon their security forces? So, for example, what about China?

Ms. SACKS. The Chinese Government is actually moving rapidly ahead to lock down more kinds of data that are deemed vital to national security, even in the commercial sector. For example, they put in place a data security law this fall which seeks to put forward a data classification scheme where they will move across sectors to define what kind of data would be vital to national security. They did this first in the auto sector, for example, and data being vital to national security has new higher-bar security obligations as

well as localization requirements around who that data can be shared with.

Senator CASSIDY. Now I think it was you who suggested that it could be counterproductive if you wall off your data, and that indeed the free flow of data—again, a nuance here—a free flow of data is essential to ascending economic power for a Nation as a whole, with the economic power, of course, being somewhat linked to national security.

So in your mind, is what they are doing counterproductive? I mean, is that something we should also do, or is it counterproductive?

Ms. SACKS. The Chinese Government is shooting itself in the foot by, I think, over-classifying the kind of data that it deems vital to national security. But in theory, what they are trying to do is say that certain kinds of data are vital to national security and need to be locked down and other kinds of data should flow and circulate in the economy.

Now, how that is going to happen in practice is another story. But I think that there could be something we could learn here in terms of defining what is the most sensitive kind of data. And Mr. Sherman and Ms. Gray have mentioned location data, for example.

President Biden put forward an executive order in June in which he called for creating a framework to assess what the security risks are of transactions involving Americans' sensitive data and what should be restricted. And in that executive order, he said not all data has the same level of sensitivity.

So I think one thing we can do is have a more thoughtful process, following on that executive order, around what kind of data is vital to national security and should be subject to higher protections, and what kind of data is less sensitive and should be subject to more international flow and sharing.

Senator CASSIDY. Let me finish with this. Mr. Sherman, is there any sort of data that cannot be relinked? So, of course, we say we are going to have location data, and we are going to be using it for X, Y, and Z purpose; it will be anomymized, it will be delinked, because it is very important. Maybe you just want to use it to establish crowd flows within a city for city planning, et cetera. But is there any data that cannot be relinked if you have a robust enough data set by which to compare it to?

Mr. SHERMAN. As Ms. Gray mentioned, there is a difference between data with someone's name or Social Security number attached, and data that does not have that attached. But at the end of the day, you can re-identify anything.

As myself and others have now testified, there is so much data out there on Americans hoarded by different companies that it is all too easy to combine it to identify people by name.

Senator CASSIDY. Okay.

Madam Chair, I am going to sign off now, because I have to transition to come in for votes. But I thank all the witnesses for your testimony, including Senator Warren's witnesses whom I might have not asked questions of, but I found their testimony very interesting. And, Madam Chair, I look forward to collaborating with you on such future events.

Senator WARREN. And thank you for being such a great partner on this. I really appreciate it, Senator Cassidy. And like you, I am delighted with the witnesses that you have invited today, to learn from them, and I hope we will have many follow-up questions for the record here. So, thank you for your partnership. This is just the opening round, and we will keep going on this.

I have one more round of questions I would like to be able to ask right now. What I would like to do now is focus a little bit on market dominance and the impact on workers.

For too long our antitrust policies have focused on prices and consumers, which are important, but the Amazon example shows that we have had weak enforcement of those policies, and that has let these big companies increase prices across the board.

We have also talked about how consolidation creates other problems, particularly for American workers. You know, whenever these companies merge, the corporate executives like to talk about the new efficiencies. And what they usually mean by that is they are going to lay off workers and cut wages. So, as companies grow more dominant, they have more and more power to lay off workers and to cut wages with no real consequences for themselves, because they know that as industries become more consolidated, workers have fewer alternatives. This means that employees who are subject to increasingly harsh, dehumanized working conditions cannot just move to a better job if there is no other available employer. This is called monopsony power, and our antitrust laws need to better address this.

So, Ms. Brown, if I can, I would like to ask you a couple of questions here. You work for Amazon Fresh. And lots of people order their groceries for delivery within a few hours and never think anything more about it. But there is a grueling process that happens behind the scenes to accomplish this feat.

Can you explain how conditions at your warehouse have changed during the pandemic?

Ms. BROWN. Absolutely. So, I am going to paint a picture for you about what the process looks like. So as soon as you go on the website and you click the "place your order" button, it causes a chain reaction of people running around the warehouse to gather everything. So, it is a small team of those who will eventually be looking at the numbers and everything and passing it down to another slate of people who are then running around a warehouse that is bigger than a football field, to then gather those items.

Then it goes to an even smaller team that is usually like about five people, to package those items out. And then it goes to an even smaller amount of people who are responsible for sorting everything, depending on where it is going, on the conveyor belt. And then it goes to my people—we work on the dock—and we are responsible for sorting thousands of those orders every day for 11 hours, making sure they get on the truck and making sure they get to the customers as fast as possible.

So now, the human toll in all of this is, basically, we have very few to no breaks. We work until our bodies are basically past the emergency stop. We delay bathroom breaks. We miss lunch. You know, we cannot miss work. And during the pandemic, you have a lot of us that—you know, we are burned out. So a lot of us, my-

self included, we would literally take like 30 seconds to kind of cry it out for a little bit, and then get right back to it. Then when you go home, you do not even have the energy to take care of your family, if you have kids, or you have family members who are dependent on you. Things such as cleaning the house or cooking for yourself basically become nonexistent on days that you have to work.

Senator WARREN. So this sounds really grueling. And I know that during these challenging times, many people across a lot of different industries have considered quitting their jobs and finding better employment. However, Amazon is continuing to grow like no other company, especially while small retailers and small local businesses are closing.

So let me ask, Ms. Brown, if conditions are this bad at the Amazon warehouse, what other employment options do you and your coworkers have to be able to support yourselves and your families?

Ms. BROWN. Well, Black and Brown people in my particular neighborhood, a lot of my coworkers do not really have very many options open to us out here in New Jersey. So most other jobs out here are warehouse jobs, or retail. And those do not pay enough. Amazon pays just a bit more than them. So we are stuck being taken advantage of in warehouses like this.

And this is what they bank on. So they know we have no other choice. So they continue with the lack of regulation and everything to protect us.

Senator WARREN. So you're right: it is not an accident. You know it is the largest employer in your industry, equipped with massive power. Amazon can pressure other companies to follow suit with its poor labor standards, or they just put those companies out of business.

Now, it was announced last week that the Amazon facility in Bessemer, AL, that workers there are entitled to hold a new union election. And if that election is successful, this would be Amazon's first union ever in the United States. But I want to ask about the other side of that: what it is like to negotiate with Amazon if you do not have a union on your side.

Amazon claims—and for this one, I actually want to quote Amazon on it—they claim that "direct connection between managers and associates is the most effective way to understand and respond to the wants and needs of Amazon employees."

Now it is certainly effective for Amazon's bottom line, but, Ms. Brown, can you tell us how effective this "direct connection" that Amazon talks about, negotiating with Amazon without a union, has been for you and for your fellow workers?

Ms. BROWN. So, okay, my colleagues and I have been fighting for change at Amazon for years. And instead of listening to us and working with us to find solutions, they tend to double-down and continue to exploit us. So that is why we continue to speak out to try to improve working conditions, and for executives to take us seriously.

So going to Amazon, especially when, say you are going to be written up or something, is kind of like trying to defend yourself in court. It is usually not going to go too well.

Senator WARREN. Well, I am very concerned that the workers who are most at risk during this pandemic are more likely to be

women, are more likely to be people of color—and of course it varies depending on the job.

And so if I can—this is the last thing I want to ask you, Ms. Brown—as a Black woman, what have you observed about Amazon's treatment of racial minorities and women?

Ms. BROWN. So now Amazon, they will hire any and everyone. That is true. But, depending on what race you are, that is going to determine whether you can get promoted, and sometimes what you are going to be doing. Most of the workers are Black and Brown, and very few of us hold high positions in the company. And it shows in the promotion process. They will promote only enough Black and Brown people so that it looks okay, but mostly they hire White managers out of school who have never actually worked for Amazon versus hiring, you know, the majority of their workforce that is Black and Brown, promoting us upwards, in the process. They really do not—when they do promote you, the pay is definitely different from those who get hired from outside.

So, if you are a Black or Brown worker, usually when you make manager, your internal promotions, you get a lower wage compared to one who is going to be coming from outside who is going to be getting a higher wage. And for women, you know, it is even more scarce to really see us in any kind of leadership role, with any of the same responsibility and respect. They would rather promote usually a White guy over someone who looks like me.

Senator WARREN. Well, I appreciate your testimony and your coming in to talk to us about this.

You know, all of this suggests to me that if we really tackle the dominant power issue by fighting abusive employer practices, by limiting mergers that would harm workers, and by empowering workers to unionize, we could accomplish two important goals at the same time. We could strengthen the American labor force and the middle class, and we could advance racial and gender equity. Vigorous competition enforcement would be better for all Americans who work, and better for all Americans who purchase goods.

So, thank you very much for your testimony, Ms. Brown. I really do appreciate it.

And I now ask for unanimous consent that the statement received by the subcommittee from the International Brotherhood of Teamsters and the Strategic Organizing Center on the importance of strong antitrust policy for workers, including in the tech sector, be entered into the record.

[The statement appears in the appendix on p 77.]

Senator WARREN. Without objection, so ordered.

I think at this moment, the United States is at an inflection point. Wealth and income disparities are at levels that we have not seen in our lifetimes. The government's lax enforcement of antitrust laws during the past few decades is a huge part of this problem. Regulators and judges have allowed merger after merger, and the result is too little competition in the U.S. market.

Dominant firms in technology are free pretty much to do as they please, including on data collection. They raise prices, they reduce wages, they threaten our privacy, all so that they can boost their profits to their shareholders and make their CEOs richer. I am encouraged that the Biden administration is committed to stronger

enforcement actions across agencies, and committed to promoting competition. But Congress has to step up and do its part too.

It is time for Congress to finally update our antitrust laws. We should ban all mergers involving huge corporations. The biggest companies need to compete on the merits. They need to offer better products, better prices, better service, not just buy up their rivals and then gouge consumers. And second, we have to give our antitrust agencies better tools to break up the anticompetitive deals that are most harmful to our economy, like Facebook's acquisition of Instagram. And finally, our competition policy must safeguard our workforce. Those deal synergies that reduce corporate costs often come out of the hides of American workers—real people with families to support who deserve to work with dignity and are paying a huge cost when mergers reduce competition.

More than 100 years ago, our antitrust laws were not designed to promote efficiency or to increase consumer welfare. They were designed to protect people from being at the mercy of economic kings who could exploit workers and customers at their whims. Those laws were also designed to protect our democracy from the corrupt influence of giant corporations. Congress needs to do its part once again to make our economy more competitive.

So I want to say again, thank you to all of our witnesses. I appreciate your being here today. Your testimony has been very valuable, and I appreciate your answers.

For any Senators who wish to submit questions for the record, those are due 1 week from today. That is Tuesday, December 14th. For our witnesses, you will have 45 days to respond to any questions.

I want to thank you all again.

And with that, this hearing is adjourned.

[Whereupon, at 11:33 a.m., the hearing was concluded.]

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

PREPARED STATEMENT OF COURTENAY BROWN, AMAZON ASSOCIATE AND LEADER, UNITED FOR RESPECT

Thank you for inviting me to share my experience with you today, Senator Warren and members of the committee. My name is Courtenay Brown, and I live in Newark, NJ. I'm currently working at an Amazon fulfillment center and have been for 3½ years.

Before working at Amazon, I served my country as a service member in the U.S. Navy. In my time of service, I vowed to uphold the core values of the Navy, which included the commitment to care for the safety, professional, personal, and spiritual well-being of our people. It was my duty, and that of my fellow Navy men and women, to work together as a team to improve the quality of our work, our people, and ourselves.

I took seriously the commitment I made to my country then, and I take it seriously now as a member leader with United for Respect.

I'm here today, Senators, to raise the alarm about Amazon's business model, its threat to working people, and its threat to our economy. One out of every 153 American workers is an Amazon employee [1] and this multi-billion-dollar corporation grew on the back of its workers by exploiting them. I'm looking to you to stand up to corporations like Amazon and protect us.

The job I do is a much-needed service, especially since the COVID–19 pandemic began. As a process guide, I sort 35,000–50,000 groceries for delivery to homes in New York City and New Jersey every day. I'm in and out of our cooler constantly, picking up and setting down items as heavy as a TV monitor with little to no rest. The work that I do is supposed to be done with a team of 30–40 people, but we are operating with 28 people or less. Because our work is so essential, we need more hands on deck, not less, so that we can take turns getting breaks and much-needed rest. But Amazon does not retain its workers.

The work is physically and mentally exhausting, and on top of that, we are monitored every single second as we scan items. So pausing even to wipe the sweat off our forehead can lead to a write-up as managers monitor our locations and times we spend doing work. If we fall behind in any way during our 11-hour shift, we risk being disciplined. We are pushed to our limit to the point where we can't even take regular bathroom breaks. Often we literally have to run to and from the bathroom in under 2 minutes so we don't get in trouble. The constant pressure and surveillance is one reason why Amazon has twice the level of injuries and turnover compared to similar employers.[2]

Very few people survive Amazon for more than 6 months. I used to be a trainer at Amazon and I saw firsthand how, out of 50 new hires, for example, only 5 would make it to the 6-month mark, and many quit soon after due to injuries and overexhaustion. Unfortunately, many are often so bruised and battered that they have to turn to disability or unemployment because they can't work anymore.

---

[1] *https://www.businessinsider.com/amazon-employees-number-1-of-153-us-workers-head-count-2021-7.*

[2] *https://revealnews.org/article/behind-the-smiles/; https://www.seattletimes.com/business/amazon/amazons-turnover-rate-amid-pandemic-is-at-least-double-the-average-for-retail-and-warehousing-industries/.*

We are living in a country where **machines** are getting better treatment than people. The machines at my facility undergo routine maintenance checks to ensure they don't burn out. Meanwhile, research has shown that workplace injury rates are higher at Amazon facilities with more robotic and automated technology.[3]

Yet the one time I needed time off to be with my family to recover from my mother's passing, I was told I wouldn't be able to get the allotted 3 days off for bereavement; I was only getting 2. As you can imagine, 2 days to plan for funeral arrangements and process **my mother's death** was not nearly enough, so I had to take a month off unpaid because that's the only option I had. A month of unpaid time off, while Jeff Bezos made $75 billion[4] last year thanks to me and my coworkers.

Amazon's multi-billion-dollar wealth is made possible by offering 1- and 2-day delivery, and the corporation has achieved this speed and scale through sheer brutality—watching, timing, and punishing associates like me and my coworkers for not working fast enough and not allowing associates to take time off to adequately recover, rest, and prevent burnout.

Amazon's high-tech sweatshop caused me to develop plantar fasciitis—a debilitating pain in my heel—because I'm having to stand up for long periods of time at work with little to no rest. The burning sensation around my heels is so painful that I take what little time I have to run to the bathroom just to cry. One time the pain got so intolerable I broke down and went to the emergency room. I begged the doctors not to keep me longer than a few hours because I had to go back to work. I was more concerned that I'd get punished at work for calling out than prioritizing my own health. This kind of exploitation isn't just happening to me—I know a coworker of mine who wasn't provided the accommodations needed to pump her breast milk at work after giving birth to her child. *This* is the type of work environment Amazon is perpetuating across the country.

Amazon associates have been fighting back against these dangerous conditions for years. Instead of fixing the problem, Amazon is only doubling down on its exploitative model. Jeff Bezos himself recently told shareholders that he plans to use *more* automated control of workers in the warehouses.[5] As Amazon associates, we know what more automated control looks like—dehumanizing tactics designed to break our bodies.

Amazon has built an empire on our backs, and now other employers, like Walmart, are racing to copy it's inhumane, exploitative model that demands we work nonstop.

The worst part of all is that Amazon is setting up its high-tech sweatshop in Black and Brown communities desperate for work. The pandemic has closed a lot of businesses in my area, so even someone like me who has considered looking for another job—I can't because there are no jobs available or the pay isn't enough to make rent and put food on the table.

This committee is considering competition and economic growth in the tech sector. When corporations write the rules to maximize their profit, they ensure they win by all means necessary—including exploiting workers and gutting small businesses.

Senators, I'm looking to you to stop corporations like Amazon from ruining our economy and dictating the workplace standards for hundreds of millions of workers like me. I'm asking **you** to help me put an end to inhumane, exploitative processes that leave America's workers injured, exhausted, and mentally battered each day.

Our country needs elected leaders to side with working people—to side with essential workers—not big corporations.

Thank you.

---

[3] *https://humanimpact.org/wp-content/uploads/2021/01/The-Public-Health-Crisis-Hidden-In-Amazon-Warehouses-HIP-WWRC-01-21.pdf.*

[4] *https://www.businessinsider.com/amazon-ceo-jeff-bezos-net-worth-explodes-in-2020-chart-2020-12.*

[5] *https://www.aboutamazon.com/news/company-news/2020-letter-to-shareholders.*

Appendix I

Public Hearing on: Promoting Competition and Economic Growth in the Technology Sector

United for Respect, December 2021

We cannot have a thriving economy or democracy when the most powerful tech corporations in the world profit, grow, and outcompete small businesses by finding innovative ways to exploit working people. When success is the result of low-road labor practices, workers, communities, and responsible businesses are undermined and left facing the consequences.

Over the past decade, Amazon has grown from a company with 56,000 workers to one with 1.47 million.[6, 7] Amazon is now the second largest employer in the United States, and relies on thousands more third-party contractors to complete its distribution network.[8] Today, Amazon dominates multiple markets and industries: it's projected to capture 41.4 percent of U.S. retail e-commerce in 2021, 40.8 percent of the cloud computing market through Amazon Web Services, and 21 percent of the streaming market with Prime Video.[9, 10, 11] Recently, Amazon's CEO of World Consumer predicted that by early 2022, Amazon would surpass UPS and FedEx to become the U.S.'s largest package delivery service.[12]

Amazon has achieved this growth and dominance by creating a high-turnover, high-pressure system that offloads the costs of injuries, employment precarity, and deskilling onto the public, workers, and their families. This is Amazon's great innovation. Monitored at every minute, Amazon warehouse workers and drivers report running to the bathroom or even peeing in bottles, suffering from mental stress and fatigue, workplace injuries, and being driven to unemployment. With turnover of 150 percent, or higher, Amazon itself worries that it will churn through the entire workforce in some regions.[13]

Amazon's extensive worker surveillance and productivity metrics, commonly known as *rate* and *time off task,* have been repeatedly linked to the high injury rates at its warehouses.[14, 15] In 2020, Amazon reported 27,178 workplace injuries, of which 90 percent were serious enough that workers were unable to perform their regular duties or were forced to miss work entirely.[16] Studies have found that not only are serious injuries more frequent at Amazon warehouses—nearly 80-percent higher than for all other employers in the warehouse industry—but that they are more severe as well, with injured Amazon workers taking, on average, a week longer than the recovery time for workers injured in the general warehouse industry.[17, 18] A study by Human Impact Partners also found that injury rates at Amazon warehouses were higher during the peak rush seasons associated with holidays, Cyber Monday, and Prime Day.[19] Similarly, elevated injury rates were found at Amazon facilities with higher levels of robotic and automated technology.[20]

---

[6] *https://s2.q4cdn.com/299287126/files/doc_financials/annual/269317_023_bmk.pdf.*
[7] *https://ir.aboutamazon.com/news-release/news-release-details/2021/Amazon.com-Announces-Third-Quarter-Results/.*
[8] *https://www.nbcnews.com/business/business-news/amazon-now-employs-almost-1-million-people-u-s-or-n1275539.*
[9] *https://www.cnbc.com/2021/06/18/as-e-commerce-sales-proliferate-amazon-holds-on-to-top-online-retail-spot.html.*
[10] *https://www.wsj.com/articles/amazons-cloud-boss-is-girding-to-defend-turf-in-the-field-company-pioneered-11636300800.*
[11] *https://www.tvtechnology.com/news/amazon-apple-hbo-max-grow-us-streaming-shares-in-q3.*
[12] *https://www.cnbc.com/2021/11/29/amazon-on-track-to-be-largest-us-delivery-service-by-2022-exec-says.html.*
[13] *https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html.*
[14] *https://humanimpact.org/wp-content/uploads/2021/01/The-Public-Health-Crisis-Hidden-In-Amazon-Warehouses-HIP-WWRC-01-21.pdf.*
[15] *https://thesoc.org/wp-content/uploads/2021/02/PrimedForPain.pdf.*
[16] *https://thesoc.org/wp-content/uploads/2021/02/PrimedForPain.pdf.*
[17] *https://thesoc.org/wp-content/uploads/2021/02/PrimedForPain.pdf.*
[18] *https://thesoc.org/wp-content/uploads/2021/02/PrimedForPain.pdf.*
[19] *https://humanimpact.org/wp-content/uploads/2021/01/The-Public-Health-Crisis-Hidden-In-Amazon-Warehouses-HIP-WWRC-01-21.pdf.*
[20] *https://humanimpact.org/wp-content/uploads/2021/01/The-Public-Health-Crisis-Hidden-In-Amazon-Warehouses-HIP-WWRC-01-21.pdf.*

Amazon has also come to dominate the logistics industry by undercutting wages.[21] A study by Bloomberg found that when Amazon opens new facilities, the average warehouse industry wages fall in that county, reaching their pre-Amazon level only after 5 years.[22] The same study found Amazon's employee promotion rate to be far below that of the industry average, reflecting the high turnover rate and lack of advancement opportunities facing most associates.[23]

Black workers disproportionately bear the brunt of Amazon's model. At one of Amazon's largest warehouses in New York, Black workers were 50-percent more likely to be fired than their White peers.[24] And during the pandemic, Amazon fired several Black workers who spoke out about unsafe conditions.[25] This mirrors findings that Black people are more likely to have dangerous jobs, less likely to have their concerns heard, and more likely to be retaliated against.[26] Further, Amazon actively discourages the promotion of hourly workers in warehouses, the majority of whom are Black and Brown.[27]

Meanwhile, other employers are forced, lest they be undercut, to compete using the same methods that economist Daron Acemoglu calls "so-so" tech innovation.[28] This so-so or low-road innovation contributes little to economic growth, while destabilizing the lives of working people and lowering wages. This race to the bottom wastes our enormous shared technological potential, while exacerbating economic inequality.

This is not a natural outcome of progress in the tech sector, but a reflection of economic policy decisions that we have the power to change. Our current policies incentivize the wrong kind of innovation and growth, and we must turn that around.

States are already beginning to take action in this direction. Recently, California passed a State bill regulating warehouse performance metrics such as those utilized by Amazon.[29] In 2020, Washington State, citing the high workplace injury rates at Amazon warehouses, raised the company's Worker Compensation premium rates by 15 percent and proposed placing fulfillment centers in a risk class of their own.[30] Worker surveillance practices like those Amazon uses to monitor associates and drivers, have also led to introduced legislation in Massachusetts and Illinois.[31, 32] Meanwhile, as Reuters reported last month, Amazon has used its massive lobbying and policy team to kill or undermine over 36 State bills that would impact the company.[33]

As this committee studies actions to ensure we have a healthy tech sector, it should consider a new generation of economic policies and labor rights that prevent tech corporations like Amazon from leveraging worker exploitation into growth, and outcompeting rivals by taking the low road. Establishing robust worker protections and rebalancing power between workers and employers would not only benefit hundreds of thousands of Amazon workers, but could reorient the economy and tech innovation toward more equitable and sustainable outcomes that lead to productive growth. In order to do this, we must establish policies that prioritize worker health and safety, protect against predatory surveillance and automated management practices, fortify the rights of workers to speak out and organize, guard against low-road

---

[21] *https://www.bloomberg.com/news/features/2020-12-17/amazon-amzn-job-pay-rate-leaves-some-warehouse-employees-homeless?sref=AuDcg4ag.*

[22] *https://www.bloomberg.com/news/features/2020-12-17/amazon-amzn-job-pay-rate-leaves-some-warehouse-employees-homeless?sref=AuDcg4ag.*

[23] *https://www.bloomberg.com/news/features/2020-12-17/amazon-amzn-job-pay-rate-leaves-some-warehouse-employees- homeless?sref=AuDcg4ag.*

[24] *https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html?referring Source=articleShare.*

[25] *https://sahanjournal.com/business-economy/amazon-shakopee-minnesota-protest/.*

[26] *https://www.nelp.org/publication/silenced-COVID–19-workplace/.*

[27] *https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html.*

[28] *https://fairgrowth.house.gov/sites/democrats.fairgrowth.house.gov/files/documents/Acemoglu%20Testimony.pdf.*

[29] *https://www.latimes.com/business/story/2021-09-08/california-bill-ab701-passes-senate-warehouse-work-metrics-algorithims-regulation.*

[30] *https://www.seattletimes.com/business/because-of-injury-claims-state-wants-amazons-automated-warehouses-to-pay-higher-workers-comp-premiums-than-meatpacking-or-logging-operations/.*

[31] *https://www.bostonglobe.com/2021/10/07/opinion/massachusetts-has-chance-clean-up-our-national-privacy-disaster/.*

[32] *https://inthesetimes.com/article/at-will-just-cause-employment-union-labor-illinois.*

[33] *https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/.*

business models, and incentivize innovation that enhances worker well-being and shared economic prosperity.

Appendix II

Worker Letter to Shareholders

United for Respect and Warehouse Worker Resource Center

November 29, 2021

Dear Amazon Shareholder,

We are Amazon associates and leaders with United for Respect (UFR) and the Warehouse Worker Resource Center (WWRC). We are part of a multiracial movement of working people advancing a vision of an economy where our work is respected and our humanity recognized. We write to you today to share an important letter from Human Impact Partners and over 200 public health practitioners calling on Amazon CEO, Andy Jassy, to end the inhumane and unsafe workplace quotas and surveillance that are currently ubiquitous throughout Amazon's logistics network.

Based on the findings of a study by Human Impact Partners and the WWRC, this letter outlines the dangerous reality we experience going to work every day. The high productivity quotas at Amazon facilities, commonly known as *rate* and *time off task,* have led to injury rates twice that of the general warehouse industry, and three times that of the average private employer. During peak rush times, and in Amazon's most automated facilities, workplace injury rates are even higher.

As the very people at risk from Amazon's unsafe warehouse practices, we urge you to read the letter and consider the included recommendations. Common-sense improvements such as doing away with *rate* and *time off task,* adopting ergonomic standards, and strengthening COVID–19 precautions would not only make Amazon facilities safer workplaces, but might lessen the worker shortage and high turnover rate seen presently at Amazon warehouses. As an Amazon shareholder, you can help mitigate any short-sighted mismanagement of human capital at the company and support any shareholder proposals that seek to review workplace health and safety issues.

In our capacity as Amazon, UFR, and WWRC worker-leaders, we would also welcome the chance to speak directly with you, answer any questions, and share our vision of a better and safer Amazon.

Sincerely,

United for Respect Member Leaders and the Membership of WWRC

Appendix III

Joint Statement

Stop Amazon's Injury Crisis: End Amazon's Dangerous and Punitive Worker Surveillance

June 21, 2021

Amazon injures and discards[34] warehouse workers and delivery drivers at double the industry average. There were a record[35] 24,000 serious injuries at Amazon facilities last year. It is time for lawmakers and regulators to step in and end the punitive system of constant surveillance that drives the dangerous pace of work at Amazon.

Amazon's business model is a calculated exploitation of workers, the majority[36] of whom are Black and Brown. Amazon's punishing[37] system monitors workers'

---

[34] *https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html?referringSource=articleShare.*

[35] *https://thesoc.org/amazon-primed-for-pain/.*

[36] *https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html?referringSource=articleShare.*

[37] *https://logicmag.io/bodies/surviving-amazon/.*

speed or *rate,* tracks their movements each second with a metric called *time off task,* and imposes a constant threat of termination. Amazon claims to simply monitor workflow—but in reality, *rate* and *time off task* are used to control[38] physical movements and discipline workers, dictate when or if they can use the bathroom, and have been used to retaliate[39] against worker organizing. A recent investigation in Washington State concluded[40] that this high-pressure system violates the law.

Discarding workers after they are injured or too exhausted, Amazon churned[41] through over half a million workers in 2019. Amazon's model breaks people's bodies, taking their health and sometimes livelihoods. The cumulative costs of this exploitative business model are offloaded[42] onto workers, their families, and the public.

Black workers disproportionately bear the brunt of Amazon's model. At one of Amazon's largest warehouses in New York, Black workers were 50 percent[43] more likely to be fired than their White peers. And during the pandemic, Amazon fired[44] several Black workers who spoke out about unsafe conditions. This mirrors findings[45] that Black people are more likely to have dangerous jobs, less likely to have their concerns heard, and more likely to be retaliated against. Further, Amazon actively[46] discourages the promotion of hourly workers in warehouses, the majority of whom are Black and Brown.

Warehouse workers and delivery drivers cannot wait for Amazon to fix its broken system. To ensure Amazon's model does not become the standard for our entire economy, regulators and lawmakers must intervene:

- **End *rate* and *time off task* tracking:** State and Federal electeds should enact laws that ban this surveillance-driven discipline and control to ensure that workers are protected from abusive conditions.
- **Update OSHA standards and enforcement to end *rate* and *time off task:*** As evidence mounts that Amazon's model creates an unsafe workplace, State and Federal OSHA programs should enforce existing standards and create new rules that address practices like *rate* and *time off* task that monitor workers and increase the pace of work.
- **Investigate Amazon's abuses:** Agencies tasked with safeguarding workers should investigate Amazon for these widespread and longstanding abuses, including: injuries, retaliation, and discrimination.

For years, workers have spoken out and protested[47] against these conditions. Most recently, in Bessemer, AL, Black warehouse workers[48] led a unionization effort, citing[49] the punishing conditions created by Amazon's system of surveillance, control, and threat of termination.

Last year, civil society organizations stood with workers and called[50] upon Congress to ban this type of punitive worker surveillance, citing the dangerous impacts on workers' physical and mental health, potential to undermine workers' right to organize, and long-term deskilling and wage decline of these jobs.

Finally forced to admit to ongoing injury problems, Amazon is nevertheless doubling down on its extractive model. In his final letter[51] to shareholders, Jeff Bezos stated that Amazon would begin to use artificial intelligence to direct workers from

---

[38] *https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.*
[39] *https://www.nbcnews.com/business/business-news/fired-interrogated-disciplined-amazon-warehouse-organizers-allege-year-retaliation-n1262367.*
[40] *https://www.seattletimes.com/business/amazon/amazons-relentless-pace-is-violating-the-law-and-injuring-warehouse-workers-washington-state-regulator-says/.*
[41] *https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html.*
[42] *https://www.nelp.org/publication/amazons-disposable-workers-high-injury-turnover-rates-fulfillment-centers-california/.*
[43] *https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html?referringSource=articleShare.*
[44] *https://sahanjournal.com/business-work/amazon-shakopee-minnesota-protest/.*
[45] *https://www.nelp.org/publication/silenced-COVID–19-workplace/.*
[46] *https://www.nytimes.com/interactive/2021/06/15/us/amazon-workers.html.*
[47] *https://www.theverge.com/2019/10/3/20897119/amazon-workers-walk-out-protest-part-time-work-minnesota.*
[48] *https://www.vox.com/the-highlight/22320009/amazon-bessemer-union-rwdsu-alabama.*
[49] *https://www.vox.com/the-highlight/22320009/amazon-bessemer-union-rwdsu-alabama.*
[50] *https://athenaforall.medium.com/end-worker-surveillance-d99aa7cd3850.*
[51] *https://www.vice.com/en/article/z3xeba/amazons-new-algorithm-will-set-workers-schedules-according-to-muscle-use.*

one task to the next. But using technology to maintain absolute control over workers' tasks and workflow will only escalate Amazon's injury crisis. Decades of research show that when workers do not have autonomy and control at work, they are more likely to be injured and experience mental strain [52] and depression.[53] Later, Amazon announced wellness programs and funding for injury research, but it refuses [54] to do the one thing that would stop widespread injuries: eliminate *rate* and *time off task.*

Amazon will soon [55] be the largest private employer in the United States, and if lawmakers and regulators fail to take action, its dangerous and extractive model will become the standard in warehousing, logistics, and retail. As other retailers implement similarly exploitative strategies,[56] this dangerous trend will further degrade working conditions for tens of millions of people across the country. The result will be a punishing, untenable reality for all working people, and Black and Brown people will pay [57] the highest cost.

We call on lawmakers and regulators do everything in their power to end *rate* and *time off task,* ensuring Amazon cannot use this punitive system of surveillance to cycle through entire workforces in communities throughout the country.

In Solidarity,

Athena Coalition
Action Center on Race and the Economy (ACRE)
Awood Center
AI Now
Civil Liberties Defense Center
Color of Change
Constitutional Alliance
Demos
Fight for the Future
Free Press
New York Communities For Change
OLE
Open Markets Institute
Partnership for Working Families
Presente.org
Public Citizen
Restore the Fourth Minnesota
Secure Justice
Government Accountability Project
Green America
Institute for Local Self-Reliance
Jobs With Justice
LAANE
Make the Road New York
Make the Road NJ
MediaJustice
Movement Alliance Project
MPower Change
National Employment Law Project
Stand Up Nashville
Surveillance Technology Oversight Project (STOP)
SumOfUs
Transit Riders Union
United for Respect
Warehouse Worker Resource Center
Warehouse Workers for Justice

Appendix IV

Joint Statement

Put Workers over Profits: End Worker Surveillance

October 14, 2020

Farhiyo Warsame, a warehouse worker, was targeted, surveilled, and fired by Amazon after speaking up about unsafe conditions at work, according to the Awood Center. Amazon tracked Farhiyo's time in between each small task and used the accumulated extra seconds to justify threats for her eventual termination. Through this "rate" and "time off task" tracking system, Amazon would have you believe it monitors work productivity—but in reality, this system is used to control the physical movements of workers, dictate when or if they can use the bathroom, discipline workers and, in the end, has been used repeatedly to retaliate against workers. It

[52] *https://www.jstor.org/stable/2392498#metadata_info_tab_contents.*
[53] *https://www.researchgate.net/publication/324557829_Job_Strain_Long_Work_Hours_and_Suicidal_Ideation_in_US_Workers_A_Longitudinal_Study.*
[54] *https://www.seattletimes.com/business/amazon/amazon-to-maintain-pace-of-warehouse-work-despite-regulators-citation/.*
[55] *https://www.cnbc.com/2021/06/11/amazon-to-overtake-walmart-as-largest-us-retailer-in-2022-jpmorgan.html.*
[56] *https://www.techtimes.com/articles/261243/20210609/walmart-free-phones-employees-used-surveillance-workers-expert.htm.*
[57] *https://www.epi.org/blog/workers-of-color-are-far-more-likely-to-be-paid-poverty-level-wages-than-white-workers/.*

enforces an unreasonable pace of work that leads to the unusually high number of injuries at Amazon.

Today, workers are subjected to an unprecedented level of workplace surveillance and control. From voice monitoring to tracking applications, these systems are being introduced into workplaces that are already stacked against low-wage workers, creating an environment ripe for exploitation. Surveillance gives corporations more power over workers. When combined with automation that dictates the pace and type of work, it results in a more dangerous, punishing, and precarious workplace. It can also lead to lower wages, deskilling of jobs, mental health stresses, the potential for racial discrimination, and a chilling effect on organizing. Workers urgently need legal protections that prevent these harms and end exploitative practices, including Amazon's rate and time off task monitoring.

The use of surveillance to exploit workers has a long history in the United States, going back to the plantation and then in manufacturing, where Taylorism and other systems of "scientific management" established control over workers' every move. The trend has worsened dramatically in recent years, and laws and regulatory agencies have failed to catch up.

Meanwhile, with few protections for workers, corporate employers have been able to grow profits by demanding and enforcing dangerous speeds, controlling each physical movement of a worker, and maximizing opportunities to make workers replaceable and expendable.

New technologies that monitor and control workers represent a radical transfer of power from workers to corporations. At Amazon warehouses, workers report that a scanner tells you exactly where to go, gives you seconds to get there, and then orders you what to do next. Your entire workload and every task you complete is managed in seconds. If you take longer than the seconds you are given, the time is added to your time off task. If you go to the bathroom or take a rest, this is also added to time off task. At the end of the day, if your productivity falls below a moving threshold, you are disciplined, and eventually fired.

Amazon's contract delivery drivers face similar monitoring, with dispatchers pressuring drivers to deliver increasing volumes of packages in a single shift—even if that means drivers must speed or skip bathroom breaks to meet delivery quotas. At Amazon, this is paired with intelligence systems and practices to monitor potential organizing activity outside of work.

This level of monitoring and control has no place in our economy. Corporate employers say that these technologies make workplaces more efficient and are necessary to be competitive, but those claims do not hold up to scrutiny. Instead, we find:

Individual productivity monitoring is used to enforce a dangerous pace of work. Within Amazon warehouses, the pervasive and punitive nature of tracking rate and time off task for each worker results in nearly double the injury rate and greater job precarity, as compared to the sector. While Amazon claimed that they stopped disciplining workers for productivity during the pandemic, the practice continued. This type of monitoring is designed for workers to fail.

Worker surveillance disproportionately harms Black and brown workers. Black and Brown workers are more likely to be in low-wage jobs, less likely to be listened to when they raise concerns, and more likely to face retaliation. Additionally, algorithmic decision-making can dramatically reinforce and exacerbate racial disparities, particularly where people impacted have no recourse or power. For many of these workers, the level of monitoring is akin to discriminatory police surveillance in their communities.

Surveillance is being used punitively, rather than to keep workers safe. Corporations are adopting new workplace technologies for the sole purpose of disciplining individual workers, even in areas where technology could be used to improve working conditions. When Amazon developed new technologies to determine if workers were within six feet of one another, they then immediately used this information to discipline and then fire workers.

Surveillance is being used to retaliate against workers and undermine their protected rights to speak out and take collective action. With limitless surveillance at an employer's fingertips, targeting a particular worker is trivial—illegal retaliation is easily obscured. Amazon has used monitoring of time off task and social distancing to retaliate against workers after they spoke up about safety concerns. Surveillance of workers is not limited to the workplace, and it was recently reported

that Amazon monitored private social media groups of Amazon Flex drivers, and tried to recruit an intelligence analyst to investigate labor organizing activities.

Pervasive surveillance and automated control increase corporate profits on the backs of workers, by reducing wages and deskilling jobs. While some technologies, such as supermarket scanners, allow companies to raise profits by using workers more efficiently, surveillance technologies raise profits by the cruder mechanism of increasing the exploitation of workers. The supermarket scanner allows each worker to serve more customers with the same level of effort, but surveillance technologies can dangerously accelerate the pace of work. The costs of injury and burnout are then offloaded onto families and the workers compensation system, rather than being internalized by the company.

During the pandemic, corporate employers have expanded workplace surveillance in ways that can compromise worker privacy and autonomy, and are using those tools for worker discipline and control. Employers have a legal duty to provide a safe working place (*e.g.,* by slowing work speeds and providing handwashing breaks). Instead, Amazon developed a punitive social distance surveillance system that it gave to other corporate employers.

In response, State and Federal Governments should enact protections against workplace surveillance—ending predatory practices, such as Amazon's rate and time off task monitoring. These protections should prioritize worker health and safety, fortify the rights of workers to speak out and organize, guard against low-road business models, require transparency in the use of new technologies, protect against new forms of tech-driven racial discrimination, and incentivize innovation that enhances worker well-being. Workers deserve better than models of exploitation developed on plantations and in factories over 100 years ago.

In Solidarity,

Athena
Action Center on Race and the Economy
The Awood Center
Center on Privacy and Technology at Georgetown Law
Civil Liberties Defense Center
Color of Change
Constitutional Alliance
Council on American-Islamic Relations (CAIR)
Coworker.org
Demand Progress
Demos
Fight for the Future
Free Press
Government Accountability Project
Greater New York Labor-Religion Coalition
Instituto de Educacion Popular del Sur de California
Jobs With Justice
Just Futures Law
LAANE
Make the Road New York
Media Mobilizing Project
MediaJustice
MPower Change
National Employment Law Project
New America's Open Technology Institute
New York Communities For Change
Open Markets Institute
Our Data Bodies
Partnership for Working Families
Public Citizen
Restore The Fourth Minnesota
RootsAction.org
Secure Justice
SEIU California
Stand Up Nashville
SumOfUs
Surveillance Technology Oversight Project (S.T.O.P.)
United for Respect
Warehouse Worker Resource Center
Working Partnerships USA
X-Lab

Appendix V

Joint Statement

Silencing of Whistleblowers in the Workplace Is a Threat to Public Health

Given the immediate public health risks, we are calling for an urgent expansion and improved enforcement of legal protections for workers who speak out and take collective action against dangerous workplace conditions that risk exacerbating the spread of COVID–19 in communities. Workers themselves are in the best position to raise health and safety concerns, and if these concerns are ignored, or worse, if

workers are retaliated against, it not only impacts those workers and their families, but risks accelerating the current public health crisis.

Over the last few weeks, Amazon fired at least six workers who had spoken out about unsafe working conditions in warehouses. In addition to these firings, other workers at Amazon have reported receiving arbitrary work-related warnings as a result of speaking out or participating in walkouts, and they fear that they are being set up for termination. Given that Amazon is the second largest private employer in the United States and is significantly expanding its workforce during the crisis, this apparent pattern of retaliation is alarming.

Thousands of warehouse, delivery, and grocery workers are on the front lines of this fight, risking contracting and spreading COVID–19 every day in order to provide essential goods. This risk disproportionately falls on communities of color, who are more likely to hold these jobs and more vulnerable to the virus, as a result of the systemic racism that undermines health in these communities. These essential workers are calling for common-sense measures in line with CDC guidance: implementation of 6 feet of distance between all individuals in the facility, personal protective equipment for all, time for handwashing, temporarily closing and cleaning exposed facilities to allow for quarantine, independent and transparent reporting, and paid leave policies to help exposed and sick workers to stay home.

Instead of adopting policies to protect workers, corporations are increasingly adopting invasive surveillance technologies to penalize and monitor lower-wage workers. This already predatory surveillance could too easily be turned against protected concerted activity and workers voicing concerns. We know that the mere presence of pervasive surveillance is likely to silence dissent, but not to protect health.

People who take action and speak out are not only exercising their legally protected right to protest and organize collectively for safe working conditions, but also acting in the national interest and protecting public health. Large facilities like warehouses, factories, and meatpacking plants employ thousands of people and grocery stores are major points of social interaction—if necessary precautions are not taken, COVID–19 could easily spread throughout communities. The right to demand better health and safety measures needs to be protected in order to limit the spread of COVID–19.

The current crisis has elevated workplace whistleblowing and collective action to a matter of national health and additional protection and enforcement measures are urgently necessary.

In solidarity,

Athena Coalition
Access Now
Action Center on Race and the Economy
AI Now Institute
Alternate ROOTS
Black Alliance for Just Immigration
Center on Privacy and Technology at Georgetown Law
Color of Change
Community Justice Exchange
Constitutional Alliance
Council on American-Islamic Relations (CAIR)
Defending Rights and Dissent
Demand Progress Education Fund
Ella Baker Center
Fight for the Future
Freedom of the Press Foundation
Global Action Project
Government Accountability Project
Instituto de Educacion Popular del Sur de California
Just Futures Law
Line Break Media
Make the Road New Jersey
New America Center on Education and Labor
New America's Open Technology Institute
New York Communities for Change
Ohio Valley Environmental Coalition
Open Markets Institute
Open MIC (Open Media and Information Companies Initiative)
Partnership for Working Families
People Demanding Action
People for the American Way
PeoplesHub
Project Censored
Project on Government Oversight
Public Citizen
RootsAction.org
RYSE Center
Secure Justice
Surveillance Technology Oversight Project (STOP)
The Awood Center
The Civil Liberties Defense Center
The Tully Center for Free Speech
United for Respect

Make the Road New York
Media Mobilizing Project
MediaJustice
MPower Change
Muslim Advocates
National Employment
United We Dream
Warehouse Worker Resource Center
Whistleblower and Source Protection Program at ExposeFacts
Law Project (NELP)
Woodhull Freedom Foundation
XLab
National Immigration Law Center

PREPARED STATEMENT OF HON. BILL CASSIDY,
A U.S. SENATOR FROM LOUISIANA

Good morning, and thank you all for being here for today's hearing. Thank you to our witnesses for taking time to testify today.

Senator Warren and I have agreed to a bipartisan hearing on promoting competition, growth, and privacy protection in the technology sector. I will be focusing my time on the data broker industry.

The data broker industry is relatively unknown to the common American, but its practices and techniques are interwoven into many aspects of their lives. Data brokers build profiles on individuals about certain attributes and then sell that information to whom they see fit. For example, as a big fan of LSU football, I frequently search topics related to LSU football; that search data is collected. A profile is made to say I am a fan of LSU football, and I will then receive ads about buying LSU football tickets, merchandise, and more. We have all experienced something similar to this, and we experience it almost everyday.

Multiple times a year a company will be the victim of a hack that exposes the data of thousands of customers. While we go to great lengths to minimize these cyber incursions, we ignore an entire industry that transacts in much more detailed and sensitive personal information. As you will hear from some of our witnesses, there is very little information data brokers can't sell and even less data that they aren't willing to sell. I believe that few people in this room would think it is a good idea to sell the profiles of millions of American service members, but that's just what they are doing.

We should have a conversation about what American data we think is okay to be bought and sold without the knowledge of many Americans, and what type of data we think is acceptable to be bought and sold period. Should we allow a list of military personnel to be sold to foreign adversaries? Should we allow lists of domestic abuse survivors to be sold to domestic abusers?

We should have a conversation about what data is appropriate to collect, what limits should be placed on the groups that data is collected on, and restrictions on how that data is sold or transferred to other parties.

We should have a conversation about all of the things our foreign adversaries can do with this data.

That's why we have assembled a team of data broker experts to talk about the different aspects of data brokers: what's regulated, what's not, and how to best move forward.

Thanks again to our witnesses. I'm looking forward to discussing these issues.

PREPARED STATEMENT OF STACEY GRAY, SENIOR COUNSEL,
FUTURE OF PRIVACY FORUM

Chair Warren, Ranking Member Cassidy, and members of the subcommittee, thank you for the opportunity to testify today on the important issue of consumer privacy in the technology sector. Specifically, I've been asked to discuss the subject of data brokers and consumer privacy, an important and highly relevant topic as Congress continues to work towards enacting a Federal comprehensive data privacy law.

As a senior counsel at the Future of Privacy Forum,[1] I work on public policy related to the intersection of emerging technologies, business practices, and U.S. consumer privacy regulation. The Future of Privacy Forum is a 501(c)(3) non-profit organization, based in Washington, DC, specializing in consumer privacy and dedicated to helping policymakers, privacy professionals, academics, and advocates around the world find consensus around responsible business practices for emerging technology.

Let me begin by observing that attention to this topic is not new. Privacy advocates, the Federal Trade Commission, and members of the Finance Committee and other Senate Committees[2] have long called for greater transparency, accountability, and regulation of the data broker industry. This includes reports from the Government Accountability Office (GAO) in 2013,[3] the Federal Trade Commission (FTC) in 2014,[4] and the research and advocacy of academic scholars and leaders, including Pam Dixon of the World Privacy Forum,[5] and my fellow witnesses here today.

Since many of these reports were published almost a decade ago, much has changed. There have been significant advances in machine learning, the ability of systems to learn, adapt, and generate inferences from large datasets, with varying accuracy. Adoption of consumer technology has also become nearly universal, with 97 percent of U.S. adults now owning a smartphone,[6] and most adults owning several additional devices—a fact which has led to fragmentation in marketing industries, and incentives for many businesses to collect even more data to attribute and measure behavior across devices.[7]

The legislative landscape is also evolving. Since 2018, California and two other States have passed non-sectoral consumer privacy legislation,[8] and three States have established limited data broker-specific regulation—California,[9] Nevada,[10] and Vermont.[11] Some State efforts have focused on transparency, through the establishment of Data Broker Registries, while others, such as the California Privacy Rights Act, codify consumer rights to opt out of the sale of data and limit the use of sensitive information. Much more work remains to be done.

In the context of this evolving landscape, I'd like to make two substantive points regarding the data broker industry, and then provide three recommendations.

1. **First:** Defining the term "data broker" is a challenge for many regulations, because it encompasses a broad spectrum of divergent companies and business activities. The GAO has used the phrase "information resellers,"[12] and the leading definition from current State law includes any commercial entity that "collects and sells

---

[1] *https://www.fpf.org.* The views expressed in this testimony are my own, and do not represent the views of FPF's supporters or Advisory Board. *See* Future of Privacy Forum, Advisory Board, *https://fpf.org/about/advisory-board/;* Supporters, *https://fpf.org/about/supporters/.*

[2] Majority Staff Report for Chairman Rockerfeller, "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes," Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations (December 18, 2013), available at *http://educationnewyork.com/files/rockefeller_databroker.pdf.*

[3] Government Accountability Office, "Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace," GAO–13–663 (September 2013), *https://www.gao.gov/assets/gao-13-663.pdf.*

[4] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability" (May, 2014), *https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.*

[5] World Privacy Forum, *https://www.worldprivacyforum.org/.*

[6] Pew Research Center, "Mobile Fact Sheet" (April 7, 2021), *https://www.pewresearch.org/internet/fact-sheet/mobile.*

[7] Jules Polonetsky and Stacey Gray, Future of Privacy Forum, *Cross-Device: Understanding the State of State Management* (2015), *https://fpf.org/wp-content/uploads/2015/11/FPF_FTC_CrossDevice_F_20pg-3.pdf.*

[8] *See* California Consumer Privacy Act, Cal. Civ. Code § 1798.100 (2018); California Privacy Rights Act, Cal. Civ. Code § 1798.100 (2020); Virginia Consumer Data Protection Act, Va. Code Ann. § 59.1–571 (2021); Colorado Privacy Act, Colo. Rev. Stat. § 6–1–1301 (2021).

[9] Data Broker Registration, Cal. Civ. Code §§ 1798.99.80–88 (2020).

[10] In 2021, Nevada updated its existing law governing operators of online services, providing consumer rights specific to qualifying data brokers. *See* Heather Sussman and David Curtis, Orrick, "Nevada Expands Online Privacy Law; Goes for Brokers" (July 1, 2021), *https://www.orrick.com/en/insights/2021/07/Nevada-Expands-Online-Privacy-Law-Goes-for-Brokers.*

[11] Vermont Data Broker Regulation, 9 V.S.A. § 2430 (2018).

[12] Government Accountability Office, "Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace," GAO–13–663 (September 2013), *https://www.gao.gov/assets/gao-13-663.pdf.*

[or licenses] the personal information of a consumer with whom the business does not have a direct relationship."[13]

Businesses that fall under this definition, including the 170 businesses registered and currently "active" in Vermont's Data Broker Registry,[14] or the 490 businesses currently registered in California,[15] use data for a wide range of purposes. Some of the information these businesses collect and sell is quite sensitive and closely linked to individuals, while other information is less sensitive or de-identified to some degree. Both registries, and most current definitions of data broker, exclude business activities that are regulated by the Fair Credit Reporting Act (FCRA)[16] (*i.e.,* consumer reporting agencies and the use of credit reports for eligibility decisions in employment, insurance, and housing) or the Gramm-Leach Bliley Act (GLBA)[17] (*i.e.,* financial institutions).

Commercial purposes that can fall outside of FCRA and GLBA include, but are not limited to:

- **Marketing and advertising**—Likely the largest category of typical "data broker" activities by revenue is for marketing and advertising,[18] including direct mail, online, and mobile advertising. Advertisers have long had the ability to purchase and curate lists of audiences (such as by demographics, zip code, or inferred interests).[19] Increasingly, data brokers and other large tech companies are interested in using web, mobile, and offline data to generate detailed predictions related to consumer purchasing intent, future behavior, psychological profiles,[20] lifestyle,[21] or sensitive information such as political affiliation or health conditions.[22] Many advertising technology (ad tech) providers also use data to offer measurement for ad attribution, conversion, and related metrics.
- **Appending and matching services**—Many businesses provide matching services that allow companies to link, or append additional information, to their existing lists of customers.[23] In some cases, businesses offer specialized, isolated matching services, or "clean rooms," that allow for external partners to link datasets without sharing underlying data, often for reasons of data ownership or protecting privacy. For example, a health-care institution might use a matching service to send information about clinical trials to patients with specific health conditions, without disclosing patient information to researchers.
- **People Search Databases**—People search databases are online search tools that provide free or paid access to information that can be found in public

---

[13] Under the Vermont Data Broker Regulation, a Data Broker is "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." 9 V.S.A. § 2430(4)(A).

[14] Vermont Secretary of State, Corporations Division, "Data Broker Search" (last visited December 3, 2021), *https://bizfilings.vermont.gov/online/DatabrokerInquire/DataBrokerSearch.*

[15] State of California Department of Justice, Office of the Attorney General, "Data Broker Registry" (last visited December 3, 2021), *https://oag.ca.gov/data-brokers.*

[16] Fair Credit Reporting Act, 15 U.S.C. § 1681.

[17] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.

[18] *See* Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability" (May 2014) at 23, *https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.*

[19] In many cases, risks related to data depend on its use. For example, an audience list associated with "Interest in Motorcycles" could be used to send direct mail discounts from a local motorcycle repair shop, but could also be used by an insurance company to infer that individuals or households engage in risky behavior. *Id.* at vi.

[20] *See, e.g.,* AnalyticsIQ, "What We Do: Consumer Data" (last visited December 3, 2021). *https://analytics-iq.com/what-we-do.*

[21] *See, e.g.,* Experian's Mosaic ® USA (December 2018) (last visited December 3, 2021), *https://www.experian.com/assets/marketing-services/product-sheets/mosaic-usa.pdf.*

[22] Justin Sherman, "Data Brokers and Sensitive Data on U.S. Individuals" Duke Sanford Cyber Policy Program (August 2021), *https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.*

[23] *See* 2020 NAI Code of Conduct (Network Advertising Initiative), page 8–B, "audience matched advertising," *https://thenai.org/wp-content/uploads/2021/07/nai_code2020-1.pdf.*

records, such as a person's home address, previous addresses, names of family members, DMV information, court records, and criminal records.[24]

- **Fraud detection**—Many companies offer commercial fraud detection services to institutions such as banks, health-care institutions, and online retailers, to protect consumers and businesses against fraudulent activities.[25] Such services typically rely on a wide variety of data from public and private records, such as purchasing behavior, online behavior, or real-time behavioral data from devices.[26]
- **Identity verification—**The ability to accurately verify identity, or that an individual is who they say they are, is a key component of digital services across many sectors.[27] Including for the estimated 1 billion people globally who do not have proof of identity and are thus prevented from accessing government services or excluded from basic financial services, individual "digital footprints" can offer opportunities for alternative approaches to digital identity verification.[28]
- **Alternative risk scoring**—Historically, credit scores provided by consumer reporting agencies (CRAs) include predictions of creditworthiness based on past loan repayment history and related information. A growing number of fintech and data broker companies have begun using data from other sources, such as rental history or payment of utility bills, to make similar predictions about risk.[29] Sometimes known as "alternative risk scoring," this can be used to extend lines of credit to consumers that are "thin-file," or have little to no formal credit history. However, such risk scoring has raised concerns about privacy, fairness, bias, and accuracy, when it involves predictions from data such as web browsing, search history, or social media. Alternative risk scoring is governed by FCRA when used for individual eligibility decisions, such as firm offers of credit, but in some cases may fall outside of the protections of FCRA, for example when involving household data or lead generation.[30]

---

[24] Examples of people search companies include Whitepages *(whitepages.com);* Truthfinder *(truthfinder.com),* BeenVerified *(https://www.beenverified.com/),* and Spokeo *(https://www.spokeo.com/). See also,* Adi Robertson, "The Long, Weird History of Companies that Put Your Life Online," Wired (March 21, 2017), *https://www.theverge.com/2017/3/21/14945884/people-search-sites-history-privacy-regulation,* and Yael Grauer, "How to Delete Your Information From People-Search Sites," Consumer Reports (August 20, 2020), *https://www.consumerreports.org/personal-information/how-to-delete-your-information-from-people-search-sites-a6926856917.*

[25] According to data released by the Federal Trade Commission, more than 2.1 million fraud reports were filed by consumers in 2020. Consumers reported losing more than $3.3 billion to fraud in 2020, up from $1.8 billion in 2019. Nearly $1.2 billion of losses reported last year were due to imposter scams, while online shopping accounted for about $246 million in reported losses from consumers. Federal Trade Commission, "New Data Shows FTC Received 2.2 Million Fraud Reports from Consumers in 2020" (February 4, 2021), *https://www.ftc.gov/news-events/press-releases/2021/02/new-data-shows-ftc-received-2-2-million-fraud-reports-consumers.*

[26] *See, e.g.,* Tax N. et al. (2021), "Machine Learning for Fraud Detection in E-Commerce: A Research Agenda." In: Wang G., Ciptadi A., Ahmadzadeh A. (eds.) *Deployable Machine Learning for Security Defense.* MLHat 2021. *Communications in Computer and Information Science,* vol 1482. Springer, Cham. *https://doi.org/10.1007/978-3-030-87839-9_2.*

[27] *See* Noah Katz and Brenda Leong, Future of Privacy Forum, "Now, on the Internet, Everyone Knows You're a Dog: An Introduction to Digital Identity" (August 3, 2021), *https://fpf.org/blog/now-on-the-internet-everyone-knows-youre-a-dog/.* Notably, identity verification can also be an important responsibility for businesses in responding to consumer requests to access, delete, and control data under emerging consumer privacy laws. *See, e.g.,* Jennifer Ellan and Steven Stransky, "The new CCPA draft regulations: Identity verification," International Association of Privacy Professionals (June 30, 2020), *https://iapp.org/news/a/the-new-ccpa-draft-regulations-identity-verification.*

[28] Vyjayanti T. Desai, Anna Diofasi, and Jing Lu, "The global identification challenge: Who are the 1 billion people without proof of identity?", World Bank (April 25, 2018), *https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity.*

[29] *See generally,* Consumer Financial Protection Bureau, "CFPB Explores Impact of Alternative Data on Credit Access for Consumers Who Are Credit Invisible" (February 16, 2017), *https://www.consumerfinance.gov/about-us/newsroom/cfpb-explores-impact-alternative-data-credit-access-consumers-who-are-credit-invisible/.*

[30] For an exploration of the boundaries of the Fair Credit Reporting Act, see generally, Testimony of Pam Dixon Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs: Data Brokers, Privacy, and the Fair Credit Reporting Act (June 11, 2019), *https://www.banking.senate.gov/imo/media/doc/Dixon%20Testimony%206-11-19.pdf;* and Sahiba Chopra, "Current Regulatory Challenges in Consumer Credit Scoring Using Alternative Data-Driven Methodologies," 23 *Vanderbilt Journal of Entertainment and Technology Law* 625 (2021), *https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1044&context=jetlaw.*

- **Socially Beneficial Research Initiatives—**Commercial data contributes to a growing number of research initiatives that seek to harness data in support of socially beneficial goals, such as public health tracking, humanitarian efforts, disaster relief, and medical research. In 2020, FPF established an annual Award for Research Data Stewardship, recognizing collaborations between company and academic researchers that allow researchers to access commercial data with privacy and ethical safeguards.[31]

Some data broker activities provide clear benefits to consumers, such as the use of data for public health, or to protect financial accounts against fraudulent activity. Others primarily benefit the purchasers or users of the data, such as advertisers, with little or no accompanying benefit (or perceived benefit) to individuals. A key to effective regulation will be to draw nuanced distinctions based on sources of data, purposes of processing, limitations on sharing and sale, data sensitivity, and the potential for risk and harm to individuals and groups.

2. Second: The lack of a direct relationship with consumers that characterizes most "data brokers" is both at the heart of concerns around privacy, fairness, and accountability, while also presenting the greatest challenge for data privacy regulation.

Any business with a direct-to-consumer relationship, big or small, such as a retailer, restaurant, hotel, or social media network, can collect personal information about U.S. consumers directly, indirectly, or through purchasing and appending it. In some cases, those "first-party" companies can exercise enormous influence and market power.[32] However, there is still a degree of public accountability to users who are aware of who such companies are and can delete accounts or raise alarms when practices go too far. In addition, first-party companies can directly present users with controls and tools to manage their data in an app, on a web site, through direct email communications, or other means.[33]

In contrast, a business lacking a direct relationship with consumers does not always have the same reputational interests, business incentives, or in some cases legal requirements, to limit the collection of consumer data, process it fairly, and protect it against exfiltration. In States such as California, where privacy law codifies the right to access, delete, or opt out of the sale or sharing of data, consumers typically are not aware of what companies within the "data broker" category may process their information, how to reach them, or how to manage the hundreds of opt-out requests that would be necessary to control the disclosure of their information.[34]

At the same time, a lack of a consumer relationship means that businesses engaged in legitimate or socially beneficial data processing often cannot rely on traditional mechanisms of notice and consent. Affirmative consent, or "opt-in," may be impossible or impractical for a business to obtain, while "opting out" after the fact tends to be impractical for consumers to navigate. For this reason, consumer advocates and academics have long observed the problems of legal regimes that rely solely on consent: consumers can become overwhelmed with choices, and may lack the knowledge to assess future risks, complex technological practices (such as predictive analytics, machine learning, or AI), or future secondary uses.[35] These risks are especially acute in the data broker industry.

What does this mean? In some cases, consumer choice remains an appropriate component of consumer privacy frameworks; a lack of consent should prevent data

---

[31] *See* Future of Privacy Forum Blog, FPF Issues Award for Research Data Stewardship to Stanford Medicine and Empatica, Google and Its Academic Partners (June 28, 2021), *https://fpf.org/press-releases/fpf-issues-2021-award-for-research-data-stewardship/*.

[32] Charlotte Slaiman, "Data Protection Is About Power, Not Just Privacy," Public Knowledge (March 3, 2020), *https://www.publicknowledge.org/blog/data-protection-is-about-power-not-just-privacy*.

[33] In some cases, the ability of advertisers to purchase data from data brokers can undermine the efforts of first-party platforms to create greater transparency and control for users. *See, e.g.,* Privacy Risks with Facebook's PII-based Targeting: Auditing a data broker's advertising interface (FTC PrivacyCon), *https://www.ftc.gov/system/files/documents/public_events/1223263/panel05_privacy_risks_fb_pii.pdf*.

[34] *See* Maureen Mahoney, "California Consumer Privacy Act: Are Consumers' Digital Rights Protected?", *Consumer Reports* (October 1, 2020), *https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf*.

[35] *See e.g.,* Neil Richards and Woodrow Hartzog, "The Pathologies of Digital Consent," 96 *Wash. U. L. Rev.* 1461 (2019), available at *https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11*.

processing in many circumstances. But choice cannot be the sole safeguard in consumer privacy rules. In other cases, data processing should not occur even *with* a person's consent, for example if the processing is inherently high-risk or harmful.[36]

In some circumstances, we should recognize there are socially beneficial uses of large datasets that cannot, for reasons of practicality or accuracy, hinge on consumer choice. For example, commercial research in the public interest may include allowing independent researchers to evaluate the effect of large platforms on mental health; understanding the effect of COVID–19 and public health efforts; enabling disaster relief, and mitigating bias and discrimination in AI.[37]

In these cases, privacy law can offer other tools for protecting consumers, including: limits on collection of data; transparency; accountability; risk assessment and auditing; limitations on the use of sensitive data; and limitations on high-risk automated processing for making important decisions regarding individuals' life choices.

3. Recommendations:

First and foremost, Congress should pass baseline comprehensive privacy legislation that establishes clear limitations and rules for both data brokers and first-party companies that process individuals' personal information. Its primary purpose should be to address the gaps in the current U.S. sectoral approach to consumer privacy, which has resulted in incomplete legal protections. Currently, personal information collected within certain sectors, such as credit reporting, finance, and health care, are subject to longstanding Federal safeguards, while commercial data outside of these sectors remains largely unregulated even when the data may be equally sensitive or high-risk.[38]

In the absence of comprehensive legislation, there are a number of steps Congress can take to address risks related to consumer privacy and data brokers. Legal protections specific to the industry (alone or as part of a comprehensive law) could play a useful role, for example, through a national registry or opt-out system that would build on, or standardize the work of California and Vermont. In practice, however, a comprehensive law that is not specific to particular technologies or business models will be most effective, fair, and interoperable with global frameworks such as the General Data Protection Regulation.

Other legal approaches include: (1) limiting the ability of law enforcement agencies to purchase information from data brokers, including information purchased as a workaround to evade the constitutional limitations on those agencies when seeking information directly; (2) enacting sectoral legislation for uniquely high risk technologies, such as facial recognition; or (3) updating existing laws, such as the Fair Credit Reporting Act, to more effectively cover emerging uses of data, for example in alternative consumer risk scoring.

Second, Congress should empower the Federal Trade Commission to continue using its longstanding authority to enforce against unfair and deceptive trade practices, through funding of enforcement, research, and consumer education; greater numbers of staff and the establishment of a Privacy Bureau, and civil fining authority to effectively police businesses.

---

[36] Many proposals for Federal privacy frameworks advanced by both industry and consumer advocacy groups have included categories of "prohibited" data practices that organizations processing personal information would be barred from engaging in, even with individual consent. *See e.g.,* Center for Democracy and Technology, CDT's Federal Baseline Privacy Legislation Discussion Draft (December 13, 2018) (last visited December 3, 2021), *https://cdt.org/insights/cdts-federal-baseline-privacy-legislation-discussion-draft/* (proposing that Federal law prohibit per se "unfair data processing practices," such as certain forms of biometric information tracking, precise geospatial information tracking, and probabilistic cross-device tracking); compare to, *e.g.,* Privacy For America, "Principles for Privacy Legislation" (last visited December 3, 2021), *https://www.privacyforamerica.com/overview/principles-for-privacy-legislation/* (an industry-led proposal containing prohibitions on data misuse that would include (1) banning the use of data to make certain eligibility decisions outside outside existing sectoral laws, (2) banning the use of data to charge higher prices for goods or services based on certain personal traits, and (3) outlawing the use of personal information for stalking or other forms of substantial harassment).

[37] *See* Future of Privacy Forum and Anti-Defamation League, "Big Data: A Tool for Fighting Discrimination and Empowering Groups" (July 2014), *https://fpf.org/wp-content/uploads/2014/09/Big-Data-A-Tool-for-Fighting-Discrimination-and-Empowering-Groups-FINAL1.pdf.*

[38] For example, medical records held by hospitals and covered by the Health Insurance Portability and Accountability Act (HIPAA) are subject to Federal privacy and security rules. However, equally sensitive commercial information or inferences about health conditions is largely unregulated when processed by app developers, search engines, or marketing and advertising firms, outside of the Federal Trade Commission's longstanding section 5 authority.

And finally, legislators should ensure that, within reasonable limits, privacy regulation does not prevent the use of data for socially beneficial purposes that are in the public interest, such as identifying bias and discrimination, contributing to a fair and competitive marketplace, holding large platforms accountable through independent research, and contributing to generalizable scientific, historical, and statistical research and knowledge.

Thank you for this opportunity, and I look forward to your questions.

PREPARED STATEMENT OF BARRY C. LYNN, EXECUTIVE DIRECTOR, OPEN MARKETS INSTITUTE

AMERICA'S MONOPOLY CRISIS—DEMOCRACY AND SECURITY AT RISK

Five and a half years ago, Senator Warren awakened Americans to the extreme and fast-growing threat posed by the concentration of power and control across almost all sectors of the U.S. economy. "Consolidation and concentration are on the rise in sector after sector," Senator Warren said in the June 29, 2016, speech, when she became the first leading policymaker to recognize America's monopoly crisis. "Concentration threatens our markets, threatens our economy, and threatens our democracy."

Since then Americans have witnessed a long series of real advances in the fight against concentration and consolidation. These include:

- Learning how monopolization lies at the root of most of the great problems we face today—including low wages, high prices, broken health care, sharp declines in entrepreneurship, and political extremism.
- Getting leading journalists and policymakers in both parties to recognize the problem and to propose legislation to fix it.
- Getting law enforcers in Washington and in almost every State of the Nation to bring powerful lawsuits against Google and Facebook, perhaps the most powerful and far-reaching corporations in human history.
- Relearning how to use traditional antimonopoly tools such as common carrier law and other rules designed to ensure that monopolists treat every American the same.

Then in July President Joe Biden resoundingly restored antimonopoly law to its necessary and original role as one of the main tools we use to protect our democracy and individual liberties. And in doing so, the President also bluntly renounced the "Chicago School" philosophy of Robert Bork and other "Neoliberal" radicals, with its focus solely on restricting the use of antimonopoly law solely increasing efficiency theoretically to promote the "welfare" of the "consumer." Further, President Biden then demanded that all agencies and departments of government—not merely those with traditional antitrust authorities—join the fight against today's extreme and dangerous concentration of power and control in the hands of a few.

What we are witnessing is one of the most important intellectual and political awakenings in American history, on a par with the awakening that took place in the years just before and after the Declaration of Independence. Or rather, we are witnessing a reawakening to the true promise, purpose, and principles of our democratic republic.

In place of the dangerous determinism of the Neoliberal Chicago School philosophy, with its insistence on the necessity, scientific inevitability, and fundamental goodness of bigness and concentrated control, Americans are returning to our traditional common-sense approach to regulating power and competition in ways that help us build a more democratic, just, sustainable, and innovative society. This in turn is empowering us to develop our own selves, families, and communities more fully and completely, which was one of the essential goals of the Founding.

Unfortunately, the task before us remains immense and daunting. The power and control that has been concentrated in the hands of Google, Facebook, Amazon, and other autocratic corporations over the last 40 years poses perhaps the most extreme threat to our democracy that we have faced since the Civil War. And the rise of the Internet and other new technologies over this period means our task today is not merely to restore the approaches of the past, but to adapt them to new structures and ways of communicating and doing business.

The good news is that Senator Warren's hearing today provides us with a vitally important chance to speed and broaden our efforts to reestablish the basic balances and controls that are essential if we are to preserve our democracy and fundamental liberties. The opportunity lies in the fact that today's hearing is the first to focus on the role that monopolization has played in creating the complex supply chain and production crises that so threaten our economic and industrial security today.

This focus on the supply chain crisis is important in three key ways.

First, the extreme and growing nature of the threats posed to our production systems illustrate in an easy-to-understand way how monopolization directly threatens the security of our Nation, our communities, and our families, not only by cutting jobs and creating higher prices but by creating the potential for a catastrophic breakdown of vital production systems and/or various forms of conflict with China and other nations.

Second, the fact that the supply chain crisis is the result of radical neoliberal changes to multiple regulatory regimes in the 1980s and 1990s—including antimonopoly, trade, corporate governance, and finance and banking—demonstrates clearly the need to strategically integrate multiple regulatory regimes into a single coherent whole.

Third, the fact that all of these threats we face today were predicted 15 or even 20 years ago demonstrates the costliness of delay and the urgency to take radical and comprehensive action immediately.

Properly studied and embraced, the lessons of our supply chain crises will also teach us how to speed and expand all of our antimonopoly efforts—including those aimed at the platform monopolists—to a point where we can assure ultimate victory. The lessons of our supply chain crises can also help to teach us how to integrate our efforts here in the United States with those of our closest industrial and political allies, in ways that will further empower us to establish the foundations for a safe and sustainable international system able to support our democracies and prosperity through the long haul of the 21st century.

THE ORIGINS OF THE SUPPLY CHAIN CRISIS

The first step to understanding today's supply chain crises, is to recognize that the structures of the production systems on which the United States relies today differ radically from the structures of the production systems that served our Nation in the past.

For most of the decades after the Second World War, right until the last years of the 20th century, most production of products and components around the world was widely distributed in multiple locations around the world.

First, production was compartmentalized within the borders of the nation-state. In the case of products such as automobiles, electronics, metals, and chemicals, for instance, every industrial nation largely produced what it consumed, and then competed with other industrial nations to sell finished goods to smaller nations, and to nations that were less industrialized.

Second, within most industrialized nations, manufacture of products such as automobiles, electronics, metals, and chemicals was separated into multiple vertically integrated corporations. In the United States, for instance, antimonopoly practice aimed to ensure that at least four corporations competed to make any particular product. Much the same was true of Japan and of Europe as a whole.

Production within corporations was then often further compartmentalized by the distribution of the capacity to manufacture of key components and end products among two or more different factories.

As a result, for most of the 20th century, when something went wrong in one factory or one industrial region somewhere in the world, the overall effects of the disruption were limited to one of many companies. Further, the widespread distribution of manufacturing capacity and skills meant that when one company experienced a major problem, it could turn to its competitors for help in keeping its own assembly lines moving and in repairing whatever damage it had suffered.

Then on September 21, 1999, an earthquake in Taiwan revealed that in at least one industry—semiconductors—the structure of production had been changed in revolutionary ways.

The 7.3 magnitude earthquake killed more than 2,500 people and disrupted life and business across Taiwan. But for the first time in human history, the efforts of an earthquake in one nation were felt almost immediately all around the entire world. The quake disrupted power at Taipei's international airport, which in turn prevented the Just-in-Time shipment of semiconductors from the industrial city of Hsinchu to factories around the world. As a result, within just a few days, computer assembly plants in California, Texas, and elsewhere began to shut down. The quake, in other words, had triggered the world's first industrial crash.

Luckily the Taiwanese foundries where the semiconductors were produced had suffered only minor damage and both production and transportation of semiconductors were swiftly restored. But the quake demonstrated in blunt fashion that at least with the manufacture of one important type of semiconductor, production was no longer compartmentalized in any real way. On the contrary, production was now concentrated in a single place in the world, largely under the control of a single corporation.

Looked at another way, all the industrial nations of the world, and all the industrial corporations, had allowed all of this one particularly "egg" to be put in a single basket.

In the years that followed, such extreme industrial concentration swiftly went from being the exception to the rule. Under the trading rules established in the mid-1990s by the Uruguay Round of the GATT, industrial nations began to offshore more and more capacity to other nations, in a process that at the time was called globalization. At the same time industrial corporations that had long insisted on producing in house the basic components that went into their finished products began to outsource production to other companies.[1]

Within a relatively short time, this combination of outsourcing and offshoring resulted in the concentration of production of many other vital goods in one or two places on the globe, much in the way the production of certain semiconductors had been concentrated in Hsinchu. Today we see such concentration in the production of many if not most of the components that go into computers and other electronics, but also in products ranging from pharmaceutical ingredients to Vitamin C to piston rings to pesticides to silicon ingots. In many instances we have also seen extreme concentration of the capacity to assemble the components into finished products.

Beginning 20 years ago, I and a few other students of the international production system began to warn about a suite of dangers posed by this revolutionary shift from a highly distributed and compartmentalized system of production to a system marked by extreme concentration of both capacity and of control. We warned that this concentration of capacity was making the production system as a whole ever more subject to catastrophic cascading failure, due to the loss of access to one industrial region or even just one factory.

We also warned that this new concentration of capacity had created the opportunity for nation-states or even factions within nation-states to exercise various forms of coercion over other nations and individual corporations that depended on the production that had been concentrated within their borders.

We also warned that this extreme concentration of capacity and monopolization of control would likely result in higher prices, lower quality, and lower levels of overall production of many individual goods and components, as the new monopolists became less focused on serving their customers and more focused on extracting outsize profits. And we warned that that concentration and monopolization threatened to result in less innovation in key products and processes.

During these same years, however, many leading economists, journalists, and policymakers began to defend the new concentration of production as a more efficient way to manufacture products. Some also defended this new concentration of production as a way to ensure that nation-states did not go to war with one another. And thus the warnings were ignored, for more than 20 years.

THE ORIGINS OF THE TRANSPORTATION AND DISTRIBUTION CRISIS

Today in America we also face a second, distinct crisis, closely related to the first. This is the breakdown of the main transportation systems on depend on for the shipment of both finished products and components to factories and stores around

[1] *https://prospect.org/features/detroit-went-bottom-up/*.

the world. The origins of this crisis lie in the same neoliberal intellectual revolution that overthrew America's antimonopoly laws, back in the 1980s and 1990s.

For most of U.S. history, the Federal, State, and local governments devoted great attention to ensuring the safety, efficiency, reliability, and affordability of transportation and distribution services. The goal was to ensure that individuals always got what they needed when they needed it. And that companies would always be able to get the supplies they needed and be able to deliver finished goods.

One result was a set of highly sophisticated systems to regulate the private corporations that handled America's ocean shipping, railroads, and air service. A second result was direct oversight of the construction of highways, canals, inland waterways, ports, and airports, and of such supporting infrastructures as pipelines and fuel depots. It also included extensive and complex systems for regulation of food marketing, processing, and warehousing.

In the 1980s and 1990s, however, U.S. regulators at all levels retreated in often dramatic fashion from these long-time tasks. They did so under pressure from the same laissez faire arguments used to overthrow antimonopoly law; *i.e.,* that it was more efficient just to let the "market" regulate investment in transportation and the behavior of transportation corporations.

The result, when combined with the revolutionary changes taking place during these same years in the international system of production, was a revolutionary reordering of every one of the transportation and distribution systems that tie Americans to one another and to the other nations of the world. This reordering played out largely as a concentration of power and control over America's transportation system in the hands of a few giant corporations and foreign nation-states, and the concentration of physical risk through the construction of super large ships, super long rail trains, and super large ports and inland shipping facilities.

Beginning about 15 years ago, I and a few others began to warn about the radical concentration of capacity and ownership in steamships, railroads, warehousing, trucking, food processing, and retail was undermining the stability of the systems we rely on for the transportation, processing, storage, and distribution of many of the goods and foods on which we depend. We said the concentration of capacity and control was making our food and fuel systems ever more subject to potentially catastrophic cascading failure.

Over these years, the United States and other nations also experienced a number of events that demonstrated that the "deregulation" of transportation and distribution services was indeed creating a variety of new threats to the security of the American people and the proper functioning of the American economy as a whole.

These events include massive and long lasting disruptions to rail service in the United States after the merger of the Union Pacific and Southern Pacific railroads in 1996 and after CSX and Norfolk Southern divvied up control of Conrail beginning in 1999. It also includes a series of disruptions caused by strikes and lockouts of stevedores at West Coast ports. And it includes the hyper consolidation of the steamship industry itself into three closely interlocking cartels, in ways that have made it far easier for these foreign-controlled corporations to exploit the American public and U.S. businesses.

Perhaps the single most dramatic warning took place in late 2012 when Hurricane Sandy flooded automobile and rail tunnels running between Manhattan and New Jersey and also disrupted fuel supplies to the region as a whole. For centuries, warehouses and other storage centers within the boundaries of the city had kept weeks of food within near reach of the people it was destined to feed. Within 24 hours of Sandy's passage, however, it became clear that this was no longer true. The extreme consolidation of food service, food warehousing, and food transportation over the preceding decades—combined with the introduction of Just-In-Time practices in food warehousing—had stripped out most of this buffer. The result was that New Yorkers had become almost entirely dependent on an uninterrupted flow of trucks from facilities located as much as 200 miles away, and now that flow had been interrupted.[2]

Luckily, in the days after Sandy, New Yorkers did not panic and major disruptions were averted. But in the decade since, no one at the city, State, or Federal governments have taken a single step to address this danger.

---

[2] *https://www.reuters.com/article/idUS417782027820131028.*

On the contrary, over these same years, those few economists and policymakers who looked at these issues largely defended the new concentration of capacities, power, and control as a more efficient way to serve American people.

SYSTEMIC BREAKDOWNS AND CASCADING EFFECTS

Since the beginning of the COVID–19 pandemic nearly 2 years ago, both the production system and the transportation system have broken down, in ways that have created widespread disruptions to our economy and to our lives. Although distinct from one another, the breakdowns in the production and transportation systems have, time and again, also interacted in ways that greatly exacerbated the overall effects.

In the case of our production systems, the concentration of manufacturing capacity for key inputs and final products has repeatedly resulted in the breakdown of the ability to ensure that we have what we need, when we need it. We saw this in dramatic fashion in the early days of the Pandemic when there was a shocking lack of sufficient N95 masks and other personal protection equipment to protect even the most vulnerable of front line workers. This despite the fact that Americans had often first developed these products and had long led the world in manufacturing them.

The lack of sufficient masks and other PPE resulted in a cascading series of problems. It resulted in unnecessary deaths, including among health-care workers. It resulted in widespread panic and a general sense of dysfunction and confusion, as governments and institutions fought over what supplies existed. It led to the unnecessary disruption in the production of other vital goods. One dramatic example was the widespread shutdowns of processing within America's highly concentrated livestock industries—resulting in severe shortages of beef, chicken, and pork at different times and in different places around the country.

Perhaps single best illustration of the far-reaching nature of the threats posed by today's extreme concentration of industrial capacity is in semiconductors.

Over the course of the 22 years since the earthquake in Taiwan first revealed the extreme concentration of the capacity to produce certain types of semiconductors, the problem has become only worse. As was true in 1999, the world today remains just as vulnerable to disruption by earthquake or other disaster, as there has been no effort whatsoever to distribute capacity or ownership. Worse, monopolistic manufacturers like Taiwan Semiconductor Manufacturing Corporation (TSMC) have become increasingly tempted to exploit their chokepoint for profit.

The result, which has played out across the industrial world over the last 18 or so months, has been a slow but steady choking off of production in an ever widening range of industries.

In the United States, the failure by TSMC to invest sufficient funds to meet demand for its products has resulted in shortages of goods ranging from appliances to farm machinery to medical devices. The most far-reaching disruptions have take place within the automobile industry, where the shortages of semiconductors has forced automakers around the world to radically cut production. In the second quarter of 2021, for instance, Ford reported that it has lost about 50 percent of planned production for the period.[3] In October, Toyota reported that third quarter production was down nearly 40 percent compared to a year earlier,[4] and Volkswagen reported that production had fallen 30 percent below projections.[5] In recent days, the problems appear to have spread into iPhone production.[6]

Such massive shortfalls in production, in turn, trigger a variety of other harms across the industrial system. These include fewer jobs and smaller paychecks at vehicle manufacturers; higher prices for new cars, used cars, and rental cars; less work for suppliers and dealers and their employees, and more pollution as individuals are unable to replace older cars.

Meanwhile, a largely separate set of events has triggered massive disruptions within the transportation and distribution systems on which we rely to keep our

---

[3] *https://techcrunch.com/2021/07/28/ford-expects-semiconductor-rebound-new-vehicle-demand-to-increase-2021-profits/.*

[4] *https://www.reuters.com/world/asia-pacific/global-supply-constraints-deal-heavy-blow-japanese-firms-2021-10-28/.*

[5] *https://www.reuters.com/business/autos-transportation/europes-top-carmakers-count-cost-chip-crunch-2021-10-28/.*

[6] *https://www.barrons.com/articles/apple-stock-chip-shortage-iphones-51638543940.*

shelves stocked and our factories running. This includes the disruption to shipping through the Suez Canal earlier this year when the container ship Everclear got stuck. And it includes the backing up of container shipping across the Pacific when the Union Pacific railroad ran out of space to offload containers at its yards in Chicago.

Here too the result of extreme concentration of capacity and control was a dangerous series of secondary effects, including empty shelves in stores, factories that have been slowed or even shut down, higher prices, and fewer jobs.

COMPETITION POLICY AS INDUSTRIAL POLICY

Many people contend that America's supply chain crisis is nothing more than a temporary effect of changes in consumption during the pandemic, with people spending less on restaurants and more on the purchase of manufactured goods and building supplies. The economist Paul Krugman, for instance, recently made the case that the supply chain crisis is the result of nothing more than a temporary surge in demand for particular goods, and that the problem will soon ease. Or as he put it, "Why the skew? It's not a mystery: We've been afraid to indulge in many of our usual experiences and bought stuff to compensate."[7]

There is certainly some truth to the idea that the COVID–19 pandemic has resulted in large changes to what we buy and when. But to contend that America's twin supply chain crises will simply work themselves out is embarrassingly naive. In the case of both the production system and the transportation and distribution system, we see overwhelming evidence that the problems derive foremost from the concentration both of physical capacity and of control.

The monopolists who control these systems have stripped out all the slack, and then some. As a result, when something goes awry, the effects are swiftly amplified and transmitted across the economy as a whole.

Our first task in addressing America's industrial crisis is, therefore, to recognize that we are dealing with two separate but interlinking problems. Our second task is to identify what is common to both the choke pointing of production and transportation, and what makes the two problems unique.

What is common is that both problems derive from the same radical changes in thinking about how to regulate the U.S. and international political economies, beginning in the early 1980s. The Neoliberals of the 1980s and the 1990s aimed foremost at concentrating control and profits in the hands of the few. And they pursued this same basic goal in both the production and transportation systems.

What separates the two problems from one another are the particular regulatory regimes that neoliberals altered to achieve their ends, and the particular regulatory regimes we must now alter if we are to solve the problems.

In the case of the production system, the revolutionary restructuring was the result of radical changes to four distinct regulatory regimes—antitrust, trade, corporate governance, and finance. It was the combination of these four that cleared the way for the extreme concentration of production in one or a few places that we see today.

A recent article in the *Washington Monthly* by Open Markets reporter Garphil Julien provides a good description of how these four changes combined in ways that resulted in the severe degradation of the U.S. semiconductor industry. Julien reports, for instance, how Intel executives extracted almost $180 billion from the corporation—in the form of stock buybacks and dividends—between 2001 and 2020.[8]

In the case of the transportation and distribution systems that serve the United States, today's problems derive mainly from radical changes in how we regulate these essential networks, as the Neoliberal era changes aimed to achieve what, in essence, was a de facto privatization of industries that had been largely governed to serve the public interest. The problems that have resulted were then made worse by the radical relaxation of antitrust enforcement in retailing and food processing, which led to an ever more extreme concentration of reach, power, and control in corporations such as Walmart and Tysons.

---

[7] *https://www.nytimes.com/2021/10/19/opinion/vaccine-mandates-us-ports-supply-chain.html.*

[8] *https://washingtonmonthly.com/2021/12/01/to-fix-the-supply-chain-mess-take-on-wall-street/.*

A recent article in the *Washington Monthly* by Open Markets policy director Phillip Longman provides a good example of how this process played out in the U.S. railroad industry. As Longman details, railroad executives have cut services dramatically over the last decade.[9] And as Martin Oberman, chair of the Surface Transportation Board made clear recently, during this same period these railroads extracted more than $190 billion in stock buybacks and dividends from the railroads, much of which should have been reinvested in maintaining and improving service.[10]

Another good example of who the deregulation of the transportation and distribution systems was designed to serve is the recent surge in profits among members of steamship cartel. According to the maritime consultancy Drewry, container lines are on course to earn as much as $100 billion in profits this year, which is 15 times their profits in 2019.[11] What looks like a crisis to the American people looks like a fantastic opportunity to those who engineered the problem.

Solving the monopoly crisis within the production system that serves the United States will therefore require integrating antitrust with trade, corporate governance, and financial policy. Solving the monopoly crisis within the transportation and distribution industries, meanwhile, will require radical changes to how the United States regulates the steamship, railroad, warehousing, and distribution industries, as well as far more aggressive antitrust enforcement in retailing and food processing to break dangerous concentrations of capacity and control.

Perhaps most important is to recognize that there are no easy fixes, that at least some of the disruptions we are experiencing today will continue for years. Indeed, it is vital to approach this challenge as a long-term project that will require the government to develop a coherent and sophisticated industrial strategy that aims to rebuild the capacity, resiliency, skills, and innovation systems within such industries as semiconductors and railroads, and that then carefully protects such investments from being appropriated by Wall Street raiders.

ON THE PRECIPICE—AFTER A 20-YEAR FAILURE TO ACT

Today's twin supply chain crises were easily foreseeable 15 even 20 years ago. Time and again the U.S. Government was warned. Time and again the U.S. Government failed to take action. It is vital that we view the disruptions of the last 2 years as our last warning, and move immediately to take comprehensive and radical action to restructure both how we make the goods we need, and how we move them from factory to home.

Because as bad as the present set of problems is, we can imagine far worse crises. This includes the sudden and catastrophic seizing up of the system as a whole. And it includes attempts by foreign powers—China most likely—to exploit these dependencies and fragilities in ways that allow these nations to concentrate power over individual American businesses and over the American people as a whole.

This is an issue I have lived, in a very personal way, for 20 years.

In June 2002, I published a long essay in *Harper's* titled "Unmade in America: The True Cost of a Global Assembly Line." In that essay I detailed how the September 1999 earthquake in Taiwan demonstrated how the extreme and growing concentration of capacity within the international system had made our international assembly lines subject to catastrophic collapse and was fast giving the government in China dangerous levels of control over the production of goods vital to the security of the American people and the Nation as a whole.

That article immediately caught the attention of the U.S. national security community, and was cited extensively in the first annual report of the U.S.-China Security Review Commission, released in July 2002. The *Harper's* article also changed perceptions in the business community, when Yale School of Management Dean Jeffrey Garten, writing in *BusinessWeek,* called on the Bush administration to investigate the dangers I described.

In 2005 I expanded my reporting on the twin supply chain crises into a mainstream book for Doubleday, titled "End of the Line: The Rise and Coming Fall of the Global Corporation." That book was widely debated, including in the *Financial Times* and *The Wall Street Journal*, and in a special section of *The Economist.* It

[9] *https://washingtonmonthly.com/magazine/november-december-2021/amtrak-joe-vs-the-modern-robber-barons/.*
[10] *https://ajot.com/insights/full/ai-stbs-oberman-says-u.s-railroads-reduced-service-raised-rates-and-derived-191-billion-in-dividends-and-buybacks-since-2010.*
[11] *https://maritimemag.com/en/drewry-forecasts-80-billion-profit-in-2021-for-container-lines/.*

also led to direct conversations with high-level officials within the Treasury and Commerce Departments; the CIA; the Department of Defense; the White House; the U.K. Ministry of Defence; Japan's Ministry of Economy, Trade, and Industry; with multiple leading members of Congress; and with think tank scholars and academics around the world.

During this period, my own warnings were supplemented by those of other close students of the industrial system, including Intel's then CEO Andy Grove, Xilinx Semiconductor CEO Willem Roelandts, and the epidemiologist Michael Osterholm.

Over the years, these initial warnings were repeatedly borne out by real world events. This includes disruptions caused by the shutdown of borders after September 11th, the SARS epidemic, the explosion of a volcano in Iceland, the great financial crash of 2008, and most dramatically by the massive Tohoku earthquake in northern Japan in March 2011.

During these years, I further developed my own analysis of the origins and nature of the problem, in my 2010 book *Cornered: The New Monopoly Capitalism and the Economics of Destruction,* and in a series of articles for mainstream publications and specialized journals. Recently my team at the Open Markets Institute cohosted an event with the Organisation for Economic Co-operation and Development to discuss the early lessons of the disruptions caused by the early stages of COVID in 2020.

Yet until the Biden administration, every U.S. Government of the last 2 decades has failed to develop a coherent plan to address these risks. As a result, 5 years after the Trump administration first began to impose tariffs on Chinese and other imports and embargoed shipments of key components to Huawei and other Chinese corporations, the concentration of capacity in a few places continues to worsen.

Despite all the headlines about America "decoupling" from China, the fact is that U.S. corporations continue to shift more key capacity into China than out of China. This is true of leading manufacturers such as Apple.[12] And it is true of the wider array of manufacturers generally, as Nick Lardy of the Peterson Institute made clear recently.[13]

THE OPPORTUNITY

Last summer, I published an article in *Foreign Affairs* magazine, titled "Antimonopoly Power: The Global Fight Against Corporate Concentration."[14]

In that piece I describe how to use competition policy principles to guide the construction of an entirely new system of production for the United States and our industrial and democratic allies. I described how we can construct international industrial and transportation systems that distribute all risk and all power in ways that ensure that no natural or political disaster can ever again break the supply of the goods and services we need to live safely and happily here in America, and cooperatively with the other nations of the world.

I am sure there are other ways to achieve these same goals.

I look forward to working with Senator Warren and the other members of this subcommittee to do so swiftly. And to do so in ways that reinforce our democracy, liberty, and community here in America.

Thank you for this opportunity. I look forward to working with you in the days to come.

ADDITIONAL READING

- *End of the Line: The Rise and Coming Fall of the Global Corporation,* Barry Lynn, Doubleday, New York, August 2005.
- *Cornered: The New Monopoly Capitalism and the Economics of Destruction,* Barry Lynn, Wiley, 2010.
- "Built to Break: The International System of Bottlenecks in the Era of Monopoly," Barry Lynn, *Challenge Magazine,* March/April 2011.

---

[12] *https://www.theguardian.com/technology/2021/jun/03/apple-uses-more-suppliers-from-china-than-taiwan-for-first-time-data-shows.*

[13] *https://www.piie.com/blogs/china-economic-watch/foreign-investments-china-are-accelerating-despite-global-economic.*

[14] *https://www.foreignaffairs.com/articles/world/2021-06-22/antimonopoly-power.*

- "Systemic Supply Chain Risk," Yossi Sheffi and Barry C. Lynn, *The Bridge,* Fall 2014. The first article in which an engineer recognized the systemic nature of international production arrangements and the potential for cascading crashes.
- "War, Trade, and Utopia," Barry Lynn, *The National Interest,* Winter 2006. A straightforward discussion of the politics of industrial interdependence and dependence in a system marked by extreme concentrations of industrial capacity.
- "The New China Syndrome: American Business Meets Its New Master," Barry Lynn, *Harper's,* November 2015.
- "Unmade in America: The True Cost of a Global Supply Chain," Barry Lynn, *Harper's,* June 2002.
- "How the United States marched the semiconductor industry into its trade war with China," Chad P. Bown, Peterson Institute for International Economics, December 2020.
- "How Detroit Went Bottom-Up: Outsourcing Has Made the Automotive Industry So Co-Dependent and Fragile that One Company's Downfall Is Every Company's Concern," Barry Lynn, *The American Prospect,* September 2009.
- "Amtrak Joe vs. the Modern Robber Barons," Phillip Longman, *Washington Monthly,* November 2021.
- "To Fix the Supply Chain Mess, Take on Wall Street," Garphil Julien, *Washington Monthly,* December 2021.
- "New York's Looming Food Disaster," Sidhartha Mahanta, *Atlantic City Lab,* October 21, 2013.
- "A Year After Sandy, Food and Fuel Supplies Are as Vulnerable as Ever," Sidhartha Mahanta, *Reuters,* October 28, 2013.
- "The Old-School Answer to Global Trade," Beth Baltzan, *The Washington Monthly,* April 2019.
- "Preparing for the Next Pandemic," Michael T. Osterholm, *Foreign Affairs,* July/August 2005.
- "The Fragility That Threatens," Barry Lynn, *Financial Times,* October 17, 2005.

QUESTIONS SUBMITTED FOR THE RECORD TO BARRY C. LYNN

QUESTIONS SUBMITTED BY HON. SHELDON WHITEHOUSE

Question. Big tech companies have been among the most aggressive tax dodgers, pioneering offshore tax tricks with names like the "double Irish" and "Dutch sandwich."

What is the relationship between market power and large-scale tax avoidance?

Answer. Bigness equals the ability to reach into more locations and to play those locations off one another. Bigness equals more complexity, hence more ways to hide or disguise profits. Bigness equals greater ability to force governments to bend to your will.

Question. Many big tech companies—with the help of armies of lawyers and accountants—have exploited our tax laws to avoid paying their fair share. Smaller domestic companies that cannot avail themselves of these tax avoidance strategies may face a proportionally larger tax bill.

How might the abuse of tax loopholes by big tech companies put smaller domestic companies at a competitive disadvantage?

Answer. Big corporations already have many huge advantages over smaller businesses. They have more cash on hand to weather hard times. It's easier for them to get credit. They pay less for their supplies. They control more information. They have more power over government at the local, State, and Federal levels. For independent businesses in America, having to pay higher taxes relative to income is but one more disadvantage. But sometimes it is the factor that finally breaks the back of those enterprises.

Question. Before the passage of the Trump tax law, a handful of giant tech companies collectively stashed hundreds of billions in profits in offshore tax havens. The

Trump law rewarded this offshore tax avoidance by allowing companies to pay less than half of the tax rate they would have previously owed on those profits.

Instead of using the Trump tax windfall to invest in their workers, their businesses, or research and development, many businesses rewarded wealthy shareholders with massive stock buybacks. One study found that, in the year the law took effect, corporations spent 154 times as much to buy back stock as they spent on worker bonuses and wage hikes.

How might market concentration and monopoly profits have contributed to the decision by companies to choose stock buybacks over productive investments in their businesses and workers?

Answer. In a competitive market, companies have to deliver. If not, they lose their customers to a rival who offers a better good or service. This means that in competitive markets, most companies will invest more in their factories and stores, in their workers, and in innovation. But Monopoly means never having to say you're sorry, no matter how badly you fail. Monopolists, in other words, don't have to deliver because their customers can't leave them for a rival. This frees monopolists from the need to invest in their factories and stores, in their workers, and in innovation. Instead, monopolists can charge their customers monopoly profits for bad service, then turn all that money over to financiers in the form of dividends and stock buybacks.

Question. The Build Back Better Act includes critical reforms to level the playing field for domestic businesses by reversing incentives from the Trump tax law to shift profits overseas.

How might other aspects of our current tax laws encourage market concentration?

Answer. Over the years, Americans have devised many tax strategies to weaken or break the incentive to create a monopoly. The first such strategy was to tax the estates of the wealthy at a higher rate than smaller estates, and to require families to divide inheritances equally among all their children. Another simple approach is to tax large corporations at higher level than smaller corporations in the same line of business. In recent years, however, many of the taxation strategies designed to level the playing field for smaller companies have been overturned, making it easier for monopolists to pull ahead of their independent rivals. This in turn increases the incentive to make and keep a monopoly.

PREPARED STATEMENT OF HON. KARL A. RACINE,
ATTORNEY GENERAL, DISTRICT OF COLUMBIA

Chairwoman Warren, Ranking Member Cassidy, and distinguished members of the subcommittee, thank you for the opportunity to testify before you today to discuss how my office is enforcing antitrust laws and stopping anti-competitive behavior from tech giants.

As the first independently elected Attorney General of the District of Columbia—and also the outgoing president of the bipartisan National Association of Attorneys General—part of my job is to bring creative and novel lawsuits in the public interest.

That is why we were the first Attorney General office to bring an antitrust lawsuit against Amazon alleging that it is illegally controlling prices through restrictive agreements with third-party sellers that sell on Amazon's marketplace and wholesalers that feed Amazon's retail business.

Amazon claims that everything it does in business is about the consumer. Well, even just a cursory look—and certainly our investigation—reveals otherwise. Amazon is focused on one thing only: its bottom line, even at the expense of consumers—like the ones it claims to care so much about. In fact, Amazon is costing all of us more money by controlling prices across the entire market.

As you have said before, Senator Warren—I too, am a capitalist. A fair profit is more than fair. A great profit is more than fair. And people should get paid for entrepreneurship and hard work. But when companies use their market power to reduce competition and take advantage of consumers under the guise of creating efficiencies, regulators must step in.

Right now, many families are hurting. They're trying to keep a roof over their heads, food on the table, and clothes on their back. And if they're lucky, maybe af-

ford a few Christmas presents. But Amazon's pricing policies contribute to making that unattainable.

Now, let me give you a little bit of background on how we decided Amazon isn't acting fairly, why we're suing them, and why consumers deserve better.

Back in 2019, Amazon was facing pressure from Congress and regulators over anticompetitive behavior. To put regulators at ease, Amazon claimed it removed a clause in its agreements with third-party sellers known as its Price Parity Provision (or PPP)—that prohibited third-party sellers from offering their goods for lower prices or on better terms on competing online marketplaces, including the third-party sellers' own websites.

Spoiler alert: Amazon did a bait-and-switch by replacing the Price Parity Provision with something nearly identical. Amazon called it the Fair Pricing Policy (or FPP), which was incorporated into Amazon's agreements with third-party sellers.

The Fair Pricing Policy, like the original Price Parity Provision, effectively prohibited third-party sellers from offering their products for lower prices or under better terms on a competing online platform—including their own—by allowing Amazon to impose sanctions on those third-party sellers that did so.

Let me give an example of how this works. If I'm a third-party seller selling headphones and I want to list my product on Amazon, I must do the following: sell the headphones at a price on the Amazon marketplace that allows me to still earn a reasonable profit after incorporating Amazon's high fees and commissions. Then, I'm barred from selling my headphones on any other platform, including my own website, at a lower price, even though I could earn the same profit by doing so. And if I do, I—the third-party seller—could get kicked off of Amazon or have other significant sanctions imposed on me.

This leaves third-party sellers with two choices. They can sell their product on Amazon under these restrictive terms. Or they can only offer their product on other marketplaces. But because Amazon controls between 50–70 percent of all online sales, third-party sellers have little choice but to accept Amazon's terms.

These agreements impose an artificially high price floor across the online retail marketplace. By charging such high fees—as much as 40 percent of the product price—Amazon is inflating the prices for consumers on its platform and competing platforms. For example, if I'm selling a pair of headphones for $100 on Amazon, up to $40 dollars of that price is to cover Amazon's fees. Plain and simple, this is inflation.

And consumers lose in this scheme. As a result of Amazon's agreements, consumers *think* they're getting the lowest prices on Amazon's marketplace because they don't see any lower prices on other online marketplaces. But, absent these agreements, third-party sellers could offer their products for lower prices on other online marketplaces.

And Amazon isn't just doing this with third-party sellers, they're doing it with wholesalers as well—so we added that to our lawsuit too. First-party sellers sell products to Amazon for Amazon to resell at retail to consumers. And we've found that Amazon requires wholesalers to guarantee a certain minimum profit to Amazon on those products. This agreement is called the Minimum Margin Agreement (MMA).

This is how it works: if Amazon lowers its retail prices to match or beat a lower price on a competing online marketplace, the wholesalers are forced to pay Amazon the difference between the agreed-upon profit and what Amazon realizes with the lowered retail price. This can lead to wholesalers owing Amazon millions of dollars.

To avoid triggering this agreement, wholesalers have increased the prices to and on competing online marketplaces. The Minimum Margin Agreement, like the Price Parity Provision and the Fair Pricing Policy, reduce competing online marketplaces' abilities to compete with Amazon's marketplace on price and result in consumers paying artificially high prices.

And even outside of this litigation, small businesses have complained that Amazon has stolen their business ideas and passed them off as Amazon's own. All of this can stunt innovation.

With this suit, we hope the Court will put a stop to Amazon's use of illegal price restraints. And we hope to recover damages and penalties to deter similar conduct by Amazon and other companies in the District as well as across the country.

We also hope that our lawsuit will encourage other Attorneys General in other States to find creative and impactful ways to rein in the abuses of big tech and stand up for consumers.

Thank you, and I look forward to your questions.

FOLLOW-UP WRITTEN STATEMENT BY HON. KARL A. RACINE,
ATTORNEY GENERAL, DISTRICT OF COLUMBIA

Chairwoman Warren, Ranking Member Cassidy, and distinguished members of the subcommittee, thank you for the opportunity to testify before you on December 7th to discuss how my office is enforcing antitrust laws and stopping anticompetitive behavior from tech giants.

My office was the first Attorney General office in the country to bring an antitrust lawsuit against Amazon, alleging that it is illegally controlling prices through restrictive agreements with third-party sellers that sell on Amazon's marketplace and wholesalers that feed Amazon's retail business.

Below is a quick recap of why my office brought an antitrust lawsuit and why it's important for consumers:

1. As a result of these agreements (the Price Parity Provision, the Fair Pricing Policy and the Minimum Margin Agreement), third-party sellers and wholesalers cannot offer their products for lower prices on a competing online platform—including their own—or else Amazon will impose sanctions on the seller. These agreements are artificially inflating prices, stifling innovation, and harming consumers.
2. Because Amazon controls between 50 to 70 percent of all online retail sales, third-party sellers and wholesalers have little choice but to offer their products on and to Amazon and accept their anticompetitive terms.
3. We are asking the court to put a stop to Amazon's use of illegal price restraints and recover damages and penalties to deter similar conduct in the future.

In addition, I respectfully raise one more issue for this subcommittee's awareness. According to an April 2020 article from *The Wall Street Journal* (see below), Amazon employees have used data about independent sellers on the company's platform to develop competing products—a practice that is at odds with Amazon's stated policies.

To be sure, our office has fielded complaints from small businesses about this insidious business practice. For example, a company called Snap + Style began as an app that allows people to snap a picture of an article of clothing and then get advice on additional clothes that would match the photographed wardrobe item. The company contracted with Amazon to sell its services on Amazon's ubiquitous Internet mall. After experiencing success on the Amazon cyber-mall, Snap + Style faced extraordinary competition from a company with a nearly identical technology, and eventually saw its early business success dry up. That competitor was the largest storefront on the Internet itself—Amazon. Yes, Amazon brazenly started competing against its client by effectively inverting the client's name from Snap + Style to its brand—StyleSnap.

Monopoly and economic principles 101 tell us that such power crushes creativity, entrepreneurship, and small business. More examples of this type of conduct are stated in the previously referenced *Wall Street Journal* article below.

From *The Wall Street Journal,* April 23, 2020

AMAZON SCOOPED UP DATA FROM ITS OWN SELLERS
TO LAUNCH COMPETING PRODUCTS

By Dana Mattioli

Amazon.com Inc. employees have used data about independent sellers on the company's platform to develop competing products, a practice at odds with the company's stated policies.

The online retailing giant has long asserted, including to Congress, that when it makes and sells its own products, it doesn't use information it collects from the site's individual third-party sellers—data those sellers view as proprietary.

Yet interviews with more than 20 former employees of Amazon's private-label business and documents reviewed by *The Wall Street Journal* reveal that employees did just that. Such information can help Amazon decide how to price an item, which features to copy or whether to enter a product segment based on its earning potential, according to people familiar with the practice, including a current employee and some former employees who participated in it.

In one instance, Amazon employees accessed documents and data about a best-selling car-trunk organizer sold by a third-party vendor. The information included total sales, how much the vendor paid Amazon for marketing and shipping, and how much Amazon made on each sale. Amazon's private-label arm later introduced its own car-trunk organizers.

"Like other retailers, we look at sales and store data to provide our customers with the best possible experience," Amazon said in a written statement. "However, we strictly prohibit our employees from using nonpublic, seller-specific data to determine which private label products to launch."

Amazon said employees using such data to inform private-label decisions in the way the *Journal* described would violate its policies, and that the company has launched an internal investigation.

Nate Sutton, an Amazon associate general counsel, told Congress in July:[1] "We don't use individual seller data directly to compete" with businesses on the company's platform.

It is a common business strategy for grocery chains, drugstores and other retailers to make and sell their own products to compete with brand names.[2] Such private-label items typically offer retailers higher profit margins than either well-known brands or wholesale items. While all retailers with their own brands use data to some extent to inform their product decisions, they have far less at their disposal than Amazon, according to executives of private-label businesses, given Amazon's enormous third-party marketplace.

The coronavirus pandemic has enabled Amazon to position itself as a national resource capable of delivering needed goods to Americans sheltering in place,[3] garnering it goodwill in Washington. The company continues, however, to face regulatory inquiries into its practices that predate the crisis.

Last year, the European Union's top antitrust enforcer said that it was investigating whether Amazon is abusing its dual role as a seller of its own products and a marketplace operator[4] and whether the company is gaining a competitive advantage from data it gathers on third-party sellers.

The Justice Department, Federal Trade Commission and Congress also are investigating large technology companies,[5] including Amazon, on antitrust matters. Amazon is facing scrutiny over whether it unfairly uses its size and platform against competitors and other sellers on its site. Amazon disputes that it abuses its power and size, noting that it accounts for a small proportion of overall U.S. retail sales, and that the use of private-label brands is common in retail.

Amazon has said it has restrictions in place to keep its private-label executives from accessing data on specific sellers in its marketplace, where millions of businesses from around the globe offer their goods. In interviews, former employees and a current one said those rules weren't uniformly enforced. Employees found ways around them, according to some former employees, who said using such data was a common practice that was discussed openly in meetings they attended.

---

[1] *https://www.wsj.com/articles/congress-puts-big-tech-in-crosshairs-11563311754?mod=article_inline.*

[2] *https://www.wsj.com/articles/how-kirkland-signature-became-one-of-costcos-biggest-success-stories-1505041202?mod=article_inline.*

[3] *https://www.wsj.com/articles/amazon-to-hire-100-000-warehouse-and-delivery-workers-amid-coronavirus-shutdowns-11584387833?mod=article_inline.*

[4] *https://www.wsj.com/articles/european-union-probing-amazon-s-treatment-of-merchants-using-its-platform-1537367673?mod=article_inline.*

[5] *https://www.wsj.com/articles/justice-department-to-open-broad-new-antitrust-review-of-big-tech-companies-11563914235?mod=article_inline.*

"We knew we shouldn't," said one former employee who accessed the data and described a pattern of using it to launch and benefit Amazon-products. "But at the same time, we are making Amazon-branded products, and we want them to sell."

Some executives had access to data containing proprietary information that they used to research best-selling items they might want to compete against, including on individual sellers on Amazon's website. If access was restricted, managers sometimes would ask an Amazon business analyst to create reports featuring the information, according to former workers, including one who called the practice "going over the fence." In other cases, supposedly aggregated data was derived exclusively or almost entirely from one seller, former employees said.

Amazon draws a distinction between the data of an individual third-party seller and what it calls aggregated data, which it defines as the data of products with two or more sellers. Because of the size of Amazon's marketplace, most products have many sellers. Viewing the data of aproduct with a number of sellers wouldn't give it insight into proprietary seller information because the figures would show lots of different seller behavior.

Amazon said that if there is only one seller of an item, and Amazon is selling returned or damaged versions of that item through its Amazon Warehouse Deals clearance account, Amazon considers that "aggregate" data—and hence is permissible for its employees to review.

Amazon's private-label business encompasses more than 45 brands with some 243,000 products, from AmazonBasics batteries to Stone & Beam furniture. Amazon says those brands account for 1% of its $158 billion in annual retail sales, not counting Amazon's devices such as its Echo speakers, Kindle e-readers and Ring doorbell cameras.

Former executives said they were told frequently by management that Amazon brands should make up more than 10% of retail sales by 2022. Managers of different private-label product categories have been told to create $1 billion businesses for their segments, they said.

Amazon has a history of difficult relationships with sellers, especially those that choose not to sell their products on its site.[6] While some of the issues have involved counterfeit goods or frustration about lack of pricing control on their products, another concern for some is that Amazon would use data they accumulate to copy the products and siphon sales.

Because 39% of U.S. online shopping occurs on Amazon, according to research firm eMarketer, many brands feel they can't afford *not* to sell on the platform. In a recent survey from e-commerce analytics firm Jungle Scout, more than half of over 1,000 Amazon Marketplace sellers said Amazon sells its own products that directly compete with the seller's products.

"We had a brand say they wanted to sell exclusively on Walmart,[7] and when we proposed Amazon, they said they don't want to risk private-label copying of their product," said Kunal Chopra, the CEO of etailz, which helps vendors sell across platforms.

Early last year, an Amazon private-label employee working on new products accessed a detailed sales report on a car-trunk organizer manufactured by a third-party seller called Fortem, a four-person, Brooklyn-based company run by two 29-year-olds. That employee showed the report to the *Journal.* More than 33,000 units of the organizer were sold during the 12 months covered in the report, according to a copy reviewed by the Journal. The report has 25 columns of detailed information about Fortem's sales and expenses.

Fortem accounted for 99.95% of the total sales on Amazon for the trunk organizer for the period the documents cover, the data indicate. Oleg Maslakou, one of Fortem's founders, said "no one is selling the Fortem organizer besides us and Amazon Warehouse Deals," a resale clearance account of returned or damaged goods from Fortem. "You hit us with a big surprise," he said after reviewing the data Amazon's private-label employee had on his brand.

Amazon said that there was one other seller of Fortem's trunk organizer during the period of the data the *Journal* reviewed. It wouldn't comment on how many days

---

[6] *https://www.wsj.com/articles/nike-to-stop-selling-directly-to-amazon-11573615633?mod=article_inline.*

[7] *https://www.wsj.com/market-data/quotes/WMT.*

that seller was active or how many sales it made. The *Journal* reached the other seller of the Fortem trunk organizer, who said for the period of time, he sold only 17 units of the item. Fortem's own sales and a slight number of its own damaged goods and returns sold through Amazon's Warehouse Deals account accounted for nearly 100% of the more than 33,000 sales of the unit during the period, the data show.

The data in the report reviewed by the *Journal* showed the product's average selling price during the preceding 12 months was about $25, that Fortem had sold more than $800,000 worth in the period specified, and that each item generated nearly $4 in profit for Amazon. The report also detailed how much Fortem spent on advertising per unit and the cost to ship each trunk organizer, according to the documents and former Amazon employees who explained their contents.

"We would work backwards in terms of the pricing," said one of the people who used to obtain third-party data. By knowing Amazon's profit-per-unit on the third-party item, they could ensure that prospective manufacturers could deliver a higher margin on an Amazon-branded competitor product before committing to it, said another person who accessed the data.

Fortem launched its trunk organizer on Amazon's Marketplace in March 2016, and it eventually became the number one seller in the category on Amazon. In October 2019, Amazon launched three trunk organizers similar to Fortem's under its AmazonBasics private-label brand.

The Fortem trunk organizer detailed in the documents is still a bestseller in the category, Amazon noted. Fortem spends as much as $60,000 a month on Amazon advertisements for its items to come up at the top of searches, said Mr. Maslakou.

Pulling data on competitors, even individual sellers, was "standard operating procedure" when making products such as electronics, suitcases, sporting goods or other lines, said the person who shared the Fortem documentation. Such reports were pulled before Amazon's private label decided to enter a product line, the person said.

"Customers' shopping behavior in our store is just one of many inputs to Amazon's private-label strategy," said Amazon. Other factors include fashion and shopping trends and suggestions from manufacturers, it said.

Amazon employees also accessed sales data from Austin-based Upper Echelon Products, according to the data reviewed by the *Journal.* Its office-chair seat cushion is a popular seller on Amazon. An Amazon private-label employee pulled a year's worth of Upper Echelon data when researching development of an Amazon-branded seat cushion, according to the person who shared the data.

An Amazon employee pulled the data early last year. Last September, AmazonBasics launched its own version.

After the *Journal* disclosed the contents of the sales report to Travis Killian, CEO of seven-person Upper Echelon, he said: "It's not a comfortable feeling knowing that they have people internally specifically looking at us to compete with us."

Amazon said there were more than two dozen sellers of the Upper Echelon seat cushion during the period, but declined to specify how many units those sellers sold. Mr. Killian said if that were the case, he isn't sure how the private-label data on his seller account provided to the Journal matched his internal sales data so perfectly.

In traditional retail, a company such as Target[8] Corp. or Kroger[9] Co. places a weekly purchase order with the brands on its shelves. It subsequently owns the inventory, setting the price and discounts.

Because of the limitations of shelf space, traditional retailers stock far fewer products than Amazon's hundreds millions of items. Typically, they create private-label products to compete in generic categories such as paper towels, rather than copycat versions of items created by smaller entrepreneurs, private-label executives said. Amazon said the vast majority of its private-label sales are staples such as batteries and baby wipes.

The majority of Amazon's sales—58%—come through third-party sellers, primarily small and medium-size firms that list their items for sale on Amazon's Marketplace

[8] *https://www.wsj.com/market-data/quotes/TGT.*
[9] *https://www.wsj.com/market-data/quotes/KR.*

platform. (Amazon also buys items directly from manufacturers and sells them directly in "first-party" sales.)

Amazon started making its own products in 2007 with its Kindle e-reader, and it has steadily added new categories and other private-label brand names. Some of its private-label products,[10] such as batteries, have been home runs. Investment firm SunTrust Robinson Humphrey estimates Amazon is on track to post $31 billion in private-label sales by 2022, or nearly double retailer Nordstrom[11] Inc.'s 2019 revenues.

PREPARED STATEMENT OF SAMM SACKS, SENIOR FELLOW, YALE LAW SCHOOL PAUL TSAI CHINA CENTER; AND CYBERSECURITY POLICY FELLOW, NEW AMERICA

Chair Warren, Ranking Member Cassidy, and members of the subcommittee, thank you for the opportunity to testify today.

I am a senior fellow at Yale Law School's Paul Tsai China Center and a cybersecurity policy fellow at New America. I have worked as an analyst of Chinese data and technology policies for the last decade, in the U.S. national security community, and in the private sector. I also advise corporate clients on China's technology policies.

Today I will focus my testimony on data security in the context of the U.S.-China relationship and global cross-border data flows.

While my expertise focuses on China—and I will first speak specifically about the Chinese Government's approach to acquiring and extracting value from data—my view is that the most effective solutions for the United States require a more comprehensive approach to regulating data security and privacy. Some of these challenges require tools that are specific to risks posed by China, but these issues are bigger than China. Setting basic standards on what data can be collected and retained by all companies will help protect U.S. personal and other sensitive data, regardless of whether the risk comes from a state-sponsored hacker, a data broker, or a private company transferring the data to China. U.S. lawmakers have an opportunity to address transnational security threats while also advancing a more secure, ethical, and democratic global Internet in its own right.

CHINA'S NATIONAL DATA STRATEGY

1. *The Chinese Government has embarked on an ambitious national data strategy with the goal of acquiring, controlling, and extracting value from large volumes of data.*

In addition to China's two landmark laws that took effect this fall (the Data Security Law and Personal Information Protection Law[1]), Beijing has elevated the concept of data as an economic and strategic asset,[2] centralizing state power over information flows within and outside of China's borders:

– An April 2020 directive issued by the State Council and Central Committee of the Chinese Communist Party (CCP) designates data as the fifth factor of production—after land, labor, capital, and technology.[3] At the National People's Congress in March 2021, the outline of the 14th Five-Year plan called for "improving the market of data factors," and stressing the need to unlock the value of data to fuel the digital economy.[4]

---

[10] *https://www.wsj.com/articles/amazon-tests-pop-up-feature-touting-its-lower-priced-products-11552655614?mod=article_inline.*

[11] *https://www.wsj.com/market-data/quotes/JWN.*

[1] For translation and analysis of the Data Security Law, Personal Information Protection Law, and related regulations and directives, *please see* the Stanford Cyber Policy Center's DigiChina Project, *https://digichina.stanford.edu/*.

[2] The concept of data as a strategic resource is not new in China. It appears in the Big Data White Papers (2014, 2016, 2018) published by an influential think tank under the Ministry of Industry Information Technology (MIIT), as well as in the Big Data Strategy (2017). The 13th Five Year Plan (2016–2020) calls for "fully implementing the promotion of the big data development initiatives and accelerating the sharing of data resources and development of applications, to assist in industrial transformation and upgrading. . . . "

[3] Ouyang Shijia, "New guideline to better allocate production factors," April 10, 2020, *China Daily, https://www.chinadaily.com.cn/a/202004/10/WS5e903fd7a3105d50a3d15620.html.*

[4] Sina Online, "What Is the Meaning of the '14th Five-Year Plan' Outline (Draft) to Improve the Market of Data Elements?", March 5, 2021, *https://finance.sina.com.cn/china/2021-03-05/doc-ikftssaq1688850.shtml.*

– On November 30th of this year, China's Ministry of Industry and Information Technology released the 14th Five Year Plan (2021–2025) for China's big data industry. The plan defines big data as a strategic emerging industry, slated for greater state support to unlock the value of data. State supporting measures focus on expanding "international cooperation" between Chinese and foreign "big data services" companies in standard setting and research and development (R&D), and encourage multinationals to set up R&D centers in China. By 2025, the plan calls for China to set up new mechanisms to facilitate China's role in data trading and cross-border transfers and "encourages Chinese firms to offer big data services in Belt and Road Initiative (BRI) countries and regions."

Beijing is also taking steps to centralize state control over data by breaking down silos or data islands across different government ministries and between the government and private companies, which have long plagued the government's ability to aggregate and coordinate data. Barriers to data sharing are due to a variety of reasons. Chinese companies are reluctant to share their data as valuable commercial intellectual property, while government agencies often push back against one another's access requests, guarding their data as a form of political power.[5]

An article by the Tencent Research Institute argues for facilitating more data flows to China's large tech platforms. Citing an International Data Corporation (IDC) estimate, the article states that "by 2025, the proportion of the world's data held by [China] will increase from 23.4 percent in 2018 to 27.8 percent, making China the first in the world. The open use of data resources will determine whether our country can seize the initiative in a new round of international competition and guarantee national data security through the development and growth of the digital industry."[6]

What are the implications for the United States of China's domestic and international efforts to acquire and make use of data as a strategic asset?

2. *Understanding China's motivations and different scenarios for how aggregated datasets could be used by the Chinese Government is vital for creating effective U.S. policy.*

There are concerning potential uses of U.S. personal data from a national security perspective. Beijing is already presumed to have sensitive national security information from the theft of personnel records of roughly 21 million individuals from the U.S. Office of Personnel Management; travel information from a cyberattack on Marriott hotels covering roughly 400 million records; and credit data from Equifax on roughly 145 million people.[7] If additional sources of personal data such as location, social media, or pattern of life data were to be acquired or bought openly through unregulated data brokers and combined with what Beijing has already acquired through cyber-theft, Chinese security services could use it to target individuals in sensitive government national security positions or military personnel for manipulation, blackmail, or other forms of coercion. This is particularly concerning from a counterintelligence perspective for individuals with security clearances or those with access to critical infrastructure.

As Chinese online services and network infrastructure gain in prominence around the world, it is also possible that the Chinese Government could filter or monitor data processes abroad, just as the United States had done, as shown by Snowden, in utilizing data transmissions across U.S. networks for intelligence gathering. We

---

[5] Yuan Yang and Nian Liu, "Alibaba and Tencent refuse to hand loans data to Beijing," *Financial Times,* September 18, 2019, *https://www.ft.com/content/93451b98-da12-11e9-8f9b-77216ebe1f17;* Martin Chorzempa, Paul Triolo, Samm Sacks, "China's Social Credit System: A Mark of Progress or a Threat to Privacy?", Peterson Institute for International Economics Policy Brief, June 2018, *https://www.piie.com/publications/policy-briefs/chinas-social-credit-system-mark-progress-or-threat-privacy;* Samm Sacks testimony before Senate Judiciary Committee hearing "Dangerous Partners: Big Tech and Beijing," March 4, 2020, *https://www.judiciary.senate.gov/imo/media/doc/Sacks%20Testimony.pdf;* Amba Kak and Samm Sacks, "Shifting Narratives and Emerging Trends in Global Data Governance Policy," AI Now and Yale Law School Paul Tsai China Center Policy Report, August 21, 2021, *https://law.yale.edu/sites/default/files/area/center/china/document/shifting—narratives.pdf.*

[6] Chen Weixuan et al., "Data Production Factors in the Framework of Macroeconomic Growth: History, Theory and Prospects," Tencent Research Institute, June 12, 2020, *https://tisi.org/14625.*

[7] "China's Collection of Genomic and Other Healthcare Data from America: Risks to Privacy and U.S. Economic and National Security," National Counterintelligence and Security Center Fact Sheet, February 2021.

also simply do not know what value and harm data created today will have in the future, regardless of who has access to it. As we move toward a world in which people have online profiles built on aggregated data, we must ask: what are the implications of the CCP gaining effective control of information flows beyond China's closed Internet system? What are the implications as the CCP takes even more drastic steps to close off the loopholes that to this day keep even the Great Firewall relatively porous and circumventable[8] (*e.g.,* stricter enforcement of restrictions on virtual private networks (VPNs) or shifting from a blacklist to a whitelist approach to permissible websites so technical controls can keep pace with online content deemed threatening)?

At the same time, the Chinese Government's use of data is not monolithic. Different actors are seeking data not just for security and surveillance, but also as fuel for the digital economy and other basic administrative functions. Outside observers of China often view Beijing's actions solely through the lens of security, neglecting the economic development drivers that play an important role. China's Data Security Law makes explicit that security and development must be balanced in China's data-governance system. These two competing priorities have shaped China's cyber bureaucracy for years. This longstanding internal source of friction and negotiation has contributed, at least in part, to the Chinese Government not necessarily enforcing to date the strictest or most conservative security-oriented readings of Chinese cybersecurity laws and regulations. An entire early chapter of the Data Security Law was dedicated to this balance, indicating a recognition by Chinese authorities that state power hinges not only on security of data, but also on its commercial use, and that China must therefore find an effective way to leverage both at once. This duality also is driving an ambitious national effort to classify all data resources held by government and industry by category and grade ("categorized and graded protection system for data"). The goal is to distinguish less sensitive data for circulation to fuel the economy from data that should be locked down with tighter security restrictions.

As China grows in prosperity, and its leadership seeks to assert state control over data for both strategic and economic gain, the United States must also develop a comprehensive vision and regulation to maintain leadership. Leading Chinese data scholar Dr. Hong Yanqing writes that "China should also consider how to enable Chinese enterprises to control and use more data globally. After all, the United States can extend its 'arm' because its enterprises are all over the world." Hong observes that Chinese tech companies need access to global data flows, and that if the United States and the European Union are able to align on digital policies, China will be at a disadvantage of creating split products for different markets (for example, Bytedance segmenting its global and Chinese versions of the apps TikTok and Douyin). He adds that this approach "prevents Chinese ICT companies from upgrading services by using a global data pool and limits the gains from the economies of scale. Once the United States and the European Union reach an agreement, at least their enterprises can avoid data localization and segregating storage, which puts Chinese ICT enterprises at a disadvantage."[9]

Inaction by the United States will result in failure to create the interoperable coalition on data that Chinese leaders fear. Stalled progress on Privacy Shield and a global vision for data flows like APEC Cross-Border Privacy Rules underscore the challenges ahead.

RECOMMENDATIONS

To be effective, U.S. policy should be based on an accurate understanding of why data matters. The analogy of data as the new oil is false, and leads to bad policy

---

[8] Magaret Roberts assesses China's Great Firewall relies on "friction-based censorship" that "works through distraction and diversion. It nudges—but does not force—most users away from unsavory material. This framing of censorship, Roberts says, helps explain why, even though China's Great Firewall is porous and can be circumvented, the number of people who 'jump the wall' using a virtual private network (VPN) remains relatively low. People are not necessarily afraid of legal or political consequences of using a VPN, but rather the process of doing so is deemed too bothersome or offers too little value for the effort in most people's day-to-day lives." Stanford Freeman Spogli Institute, March 6, 2020, *https://fsi.stanford.edu/news/china%E2%80%99s-great-firewall-built-friction-based-censorship-says-margaret-roberts.*

[9] Hong Yanqing, "Game of Laws: Cross-Border Data Access for Law Enforcement Purposes," trans. Yale Law School Paul Tsai China Center, originally published in *Global Law Review* in Chinese. This article is the result of a special 2018 project by the Ministry of Justice, "Big Data and Cybersecurity Legislation" (18SFB1005), in which the author participated, *https://law.yale.edu/sites/default/files/area/center/china/document/game_of_laws-7.pdf.*

that treats data as a finite and zero-sum resource that is only valuable in large volumes. Matt Sheehan writes that five dimensions are crucial for machine learning data today: quantity, depth, quality, diversity, and access.[10] This understanding of data's value matters because it means that policies by Beijing or Washington that seek to hoard or wall off data as a national resource from the other could have unintended consequences that lessen national power, rather than increase it.

Lack of regulation in the United States makes Americans' sensitive data vulnerable to privacy and security harms not only from sophisticated state-backed cyber intrusions, but also from the unregulated industry of data brokers around the world trading in consumer data without transparency or controls. Setting basic standards on what data can be collected and retained by all companies will help protect U.S. personal data, regardless of where the risk originates. Developing a comprehensive Federal privacy law that includes restrictions on data brokers is vital to this effort, along with the creation of strong enforcement mechanisms. Inaction by the United States means ceding leadership and influence in setting international standards to both Europe and China in setting international standards.

Without higher standards for data security and privacy, U.S. citizen data held by unregulated private companies are more vulnerable to breaches by hackers from China or from being sold to third-parties openly buying, aggregating, and selling consumer data. For example, Equifax's many security issues are well-documented, such as the company's failure to patch known vulnerabilities that ultimately left exposed the data of 145 million Americans. But the hack was also conducted by a foreign government entity with sophisticated hacking capabilities and access to considerable state resources. Companies should not have access to such a volume of personal data that it creates a target to be hacked or transmitted to China.

This reality is also why bans on Chinese software applications are not an effective way to secure Americans' data. Even if TikTok were American-owned, for example, it could still legally sell data to data brokers that could transmit it to China's security services.

Given this, American data is shockingly exposed and will remain that way so long as restrictions on data flows only focus on specific companies from countries deemed adversaries.

Debate over a range of issues will make progress on a federal privacy law slow. In the meantime, having baseline rules for the data broker industry would contribute to closing off vectors that make American's data vulnerable to exploitation by a range of actors.

We must also keep in mind that U.S. actions to respond to data security risks posed by the Chinese Government are not occurring in a vacuum. Our policy approach should be tailored to take into account the fact that technology competition with China will not only play out in the United States and China, but also in other parts of the world from India to Europe. How we respond to Chinese companies operating in the United States has ramifications on whether other countries are willing to accept our vision of data governance.

The ability of U.S. firms to maintain a high rate of innovation depends upon access to global markets, talent, and, perhaps most important, datasets. But rising data sovereignty policies around the world are an increasing obstacle to the ability of U.S. companies to operate internationally, beyond China. These policies are an effort by nation-states to ensure control over data by prohibiting transfers of data out of the country or seeking to limit foreign access to certain kinds of data. In this context, U.S. actions will be a reference and a roadmap for other governments that are concerned about U.S. companies and the U.S. government getting access to their citizens' data.

The United States should work with like-minded governments to develop a common set of standards that would allow data to flow—building off of the concept of "data free flows with trust" put forward by Japan.[11] A multilateral approach should be based on creating a system of incentives for compliance. The United States could lead the way in setting up a certification system that would extend benefits to countries whose data regimes and companies meet certain clear criteria for data protec-

---

[10] Matt Sheehan, "Much Ado About Data: How America and China Stack Up," Macro Polo, June 16, 2019, *https://macropolo.org/ai-data-us-china/?rp=e.*

[11] "Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows," World Economic Forum, *https://www.weforum.org/whitepapers/data-free-flow-with-trust-dfft-paths-towards-free-and-trusted-data-flows.*

tion. The OECD privacy guidelines, for example, could serve as a reference in creating a baseline for commercial data flows.[12]

We need to address national security risks where they exist, but that should be done as one part of a broader U.S. initiative for comprehensive data privacy and higher cybersecurity standards for all companies —whether domestic or foreign. Failure to offer a compelling vision for U.S. data governance will make the United States less secure, less prosperous, and less powerful, and allow more space around the world for companies controlled by the CCP to flourish.

PREPARED STATEMENT OF JUSTIN SHERMAN, FELLOW AND RESEARCH LEAD, DATA BROKERAGE PROJECT, SANFORD SCHOOL OF PUBLIC POLICY, DUKE UNIVERSITY

Chair Warren, Ranking Member Cassidy, and distinguished members of the subcommittee, I appreciate the opportunity to testify about privacy issues facing American citizens.

I am a fellow at Duke University's Sanford School of Public Policy, where I lead a research project focused on the data brokerage ecosystem. We study the virtually unregulated industry and practice of data brokerage—the collection, aggregation, analysis, buying, selling, and sharing of data—and its impacts on civil rights, national security, and democracy. I am also affiliated with the Atlantic Council and with American University Washington College of Law, where I work on cybersecurity, Internet policy, and geopolitical issues.

Data brokerage is a threat to civil rights, to U.S. national security, and to democracy. The entire data brokerage ecosystem—from companies whose entire business model is data brokerage, to the thousands of other advertisers, technology giants, and companies that also buy, sell, and share Americans' personal data—profits from unregulated surveillance of every American, particularly the most vulnerable. While I support a strong, comprehensive consumer privacy law, Congress must not wait to resolve the debate over such a law to regulate the data brokerage industry.

There are three steps Congress should take now:

- Strictly control the sale of data collected by data brokers to foreign companies, citizens, and governments;
- Strictly control the sale of data in sensitive categories, like genetic and health information and location data; and
- Stop data brokers from circumventing those controls by "inferring" data.

THE DATA BROKERAGE PROBLEM

Today, and for several decades, thousands of companies have surreptitiously collected data from public and private sources about each and every American. Often, these companies will use tools to "infer" additional data about each American. These companies then repackage and resell that data on the open market, with very few controls. This is the data brokerage ecosystem.

Data brokerage is a virtually unregulated practice in the United States (except for two, limited State laws and some narrowly targeted Federal regulations discussed below). Brokered data is used to target consumers, marginalized communities, veterans, military service members, government employees, first responders, students, and children. Too often, this targeting is exploitative.

- *Military personnel:* Data brokers advertise data about millions of U.S. military personnel. Criminals have acquired this data to run educational scams against veterans because of Federal military benefits.[1] Foreign governments could acquire this data to profile military personnel, track them and their families, and otherwise undermine U.S. national security. The Chinese Government's 2015 hack of the Office of Personnel Management was one of the most damaging data breaches the Federal Government has suffered—yet, in the future, there is no need for the Chinese Government or any other foreign intelligence agency to even hack many U.S. Government databases when the

[12] "The OECD Privacy Framework," Organisation for Economic Co-operation and Development, 2013, *https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.*

[1] Tariq Habash and Mike Saunders, "The Predatory Underworld of Companies that Target Veterans for a Buck," Student Borrower Protection Center, February 1, 2019, *https://protectborrowers.org/the-predatory-underworld-of-companies-that-target-veterans-for-a-buck/*.

data can be legally purchased from American data brokers, who problematically appear to do very little customer vetting.

- *Survivors of domestic violence:* Data brokers known as "people search websites" aggregate millions of Americans' public records and make them available for search and sale online. Abusive individuals have used this data—including highly sensitive information on individuals' addresses, whereabouts, property filings, contact details, and family members—to hunt down and stalk, harass, intimidate, and even murder other individuals, predominantly women and members of the LGBTQ+ community.[2] There is little in U.S. law stopping data brokers from collecting, publishing, and selling this data on victims and survivors of intimate partner violence.
- *Individuals with mental health conditions:* Data brokers advertise data on millions of Americans' mental health conditions. Companies can legally purchase this data from other firms, circumventing existing health privacy laws, and use it to exploit consumers. Criminals could acquire this data to run scams against senior citizens with Alzheimer's and dementia.[3] Foreign governments could even acquire this data for intelligence purposes. Once again, there is little evidence data brokers conduct robust customer screening.

Our research at Duke University has found data brokers widely and publicly advertising data regarding millions of Americans' sensitive demographic information, political preferences and beliefs, and whereabouts and real-time locations, as well as data on first responders, government employees, and current and former members of the U.S. military.[4] Data brokers gather your race, ethnicity, religion, gender, sexual orientation, and income level; major life events like pregnancy and divorce; medical information like drug prescriptions and mental illness; your real-time smartphone location; details on your family members and friends; where you like to travel; what you search online; what doctor's office you visit; and which political figures and organizations you support. All of this is aggregated, analyzed, and packaged into datasets for sale with such titles as "Rural and Barely Making It," "Ethnic Second-City Strugglers," "Retiring on Empty: Singles," "Tough Start: Young Single Parents," "Credit Crunched: City Families," "viewership-gay," "African American," "Jewish," "working class," "unlikely voters," and "seeking medical care."[5] All of this information is typically collected without any consumer notice or consumer consent.

Hundreds of data brokers make selling this data their entire business model, and thousands more companies, from small businesses to technology giants, buy, sell, and share data as part of this ecosystem. The entities using this data include banks, credit agencies, insurance firms, Internet service providers, predatory loan companies, online advertisers, U.S. law enforcement and security agencies, and perpetrators of domestic violence—not to mention the foreign governments, criminals, terrorist organizations, and violent individuals that could potentially acquire the data. There are single data brokers alone that advertise thousands of individual data points on billions of people around the world. Large brokers also spend millions of

---

[2] This goes back decades. *See, e.g.,* Supreme Court of New Hampshire. *Helen Remsburg, Administratrix of the Estate of Amy Lynn Boyer v. Docusearch, Inc., d/b/a Docusearch.Com and a* (2003). *Also see:* National Network to End Domestic Violence, "People Searches and Data Brokers," last accessed December 2, 2021, *https://nnedv.org/mdocs-posts/people-searches-data-brokers/*.

[3] Criminals have already used broker data to facilitate elder scams. *See, e.g.,* U.S. Department of Justice, "List Brokerage Firm Pleads Guilty To Facilitating Elder Fraud Schemes," *Justice.gov,* September 28, 2020, *https://www.justice.gov/opa/pr/list-brokerage-firm-pleads-guilty-facilitating-elder-fraud-schemes.*

[4] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals* (Durham: Duke University Sanford School of Public Policy, August 2021), *https://sites.sanford.duke.edu/techpolicy/report-data-brokers-and-sensitive-data-on-u-s-individuals/*.

[5] U.S. Senate Committee on Commerce, Science, and Transportation. *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes.* Washington, DC: Senate Committee on Commerce, Science, and Transportation, December 18, 2013. *https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577,* ii; U.S. Federal Trade Commission. *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers.* Washington, DC: Federal Trade Commission, October 21, 2021. *https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf,* 22.

dollars lobbying against strong U.S. Federal privacy legislation that would undercut their business models.[6]

The harms are well-documented. Scammers have acquired data to run educational scams against veterans, military service members, and their families.[7] Abusive individuals have used people search websites—where data brokers scrape public records and publish Americans' addresses and other information on the Internet—to hunt down and stalk, intimidate, harass, and even murder individuals trying to escape them.[8] Financial firms have used brokered data to market products to consumers that "limit or obscure their access to loans, credit, and financial services."[9] GPS location data companies have secretly tracked citizens attending protests and demonstrations and identified their ages, genders, ethnicities, and other sensitive demographic characteristics—all of which they can legally sell.[10] Health insurance companies have aggregated millions of Americans' medical diagnosis, test, prescription, and socioeconomic data—as well as sensitive demographic information like race, education level, net worth, and family structure—to market their products and, possibly, calculate how much they can charge consumers.[11] Law enforcement and security agencies have purchased data broker data on U.S. citizens, ranging from home utility data to real-time locations, without warrants, public disclosure, and robust oversight.[12] The data law enforcement and other customers use may not even be updated, complete, or accurate.[13] The list of known harms goes on. And with all this data, companies can easily identify individuals by name.

The potential harms are also numerous. Domestic extremists could acquire real-time GPS location data to target politicians at home. Foreign governments could acquire Americans' data to run disinformation campaigns, uncover spies, blackmail U.S. Government employees, and conduct other kinds of intelligence and military operations. Criminal organizations will continue purchasing this data to run scams and phishing campaigns.[14] Individuals will continue using address, whereabouts, and GPS data to stalk and commit violence against fellow citizens. Companies will continue buying data on consumers and then make decisions and target advertisements based on sensitive demographic characteristics like race, ethnicity, gender, sexual orientation, religion, income level, family structure, political affiliation, and immigration status. Not to mention, threat actors can simply hack into the data brokers, online advertising firms, and other entities housing this highly sensitive data.

Companies can collect this data on Americans directly, whether those individuals know it or not; indirectly, by purchasing or licensing the data or by plugging into data sources like online advertising networks or third-party software development kits (SDKs); and by running algorithms to predict (what they often call "infer") sensitive information about individuals, from income level to sexual orientation.

Based on our research at Duke University, the companies selling this data on the open market conduct varying degrees of know-your-customer due diligence: some ap-

---

[6] Alfred Ng and Maddy Varner, "The Little-Known Data Broker Industry Is Spending Big Bucks Lobbying Congress," *The Markup,* April 1, 2021, *https://themarkup.org/privacy/2021/04/01/the-little-known-data-broker-industry-is-spending-big-bucks-lobbying-congress.*

[7] Habash and Saunders, "The Predatory Underworld of Companies that Target Veterans for a Buck."

[8] Sherman, *Data Brokers and Sensitive Data on U.S. Individuals.*

[9] Testimony of Pam Dixon before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, "Data Brokers, Privacy, and the Fair Credit Reporting Act," June 11, 2019, *https://www.banking.senate.gov/imo/media/doc/Dixon%20Testimony%206-11-19.pdf,* 1.

[10] Zak Doffman, "Black Lives Matter: U.S. Protesters Tracked By Secretive Phone Location Technology," *Forbes,* June 26, 2020, *https://www.forbes.com/sites/zakdoffman/2020/06/26/secretive-phone-tracking-company-publishes-location-data-on-black-lives-matter-protesters/.*

[11] One such company has alleged it does not use this data for pricing. Marshall Allen, "Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates," ProPublica, July 17, 2018, *https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates.*

[12] Drew Harwell, "ICE investigators used a private utility database covering millions to pursue immigration violations," *The Washington Post,* February 26, 2021, *https://www.washingtonpost.com/technology/2021/02/26/ice-private-utility-data/;* Joseph Cox, "How an ICE Contractor Tracks Phones Around the World," *VICE,* December 3, 2020, *https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps.*

[13] *See, e.g.,* United States District Court, Central District of California, *Gerardo Gonzalez et al. vs. Immigration and Customs Enforcement et al.* (2019), *https://www.courthousenews.com/wp-content/uploads/2019/09/Gonzalez.v.ICE_.detainer.final_.order_.9.27.pdf.*

[14] *See, e.g.,* U.S. Federal Trade Commission, "FTC Charges Data Brokers with Helping Scammer Take More Than $7 Million from Consumers' Accounts," *FTC.gov,* August 12, 2015, *https://www.ftc.gov/news-events/press-releases/2015/08/ftc-charges-data-brokers-helping-scammer-take-more-7-million.*

pear to conduct some due diligence before initiating a data purchase agreement, some appear to conduct a little due diligence, and some appear to conduct none at all. For those that appear to conduct some due diligence, it is unclear how comprehensive that vetting is in practice. Further, based on the copious evidence of data brokerage-linked harms (from domestic violence to consumer exploitation), there is very little to suggest data brokers implement controls to prevent harmful uses of their data once sold. Data brokers may also require clients to sign nondisclosure agreements preventing them from identifying where they obtained U.S. citizens' data.

As part of talking about the power of Big Tech, the dangers of modern surveillance, and data threats to Americans' civil rights, U.S. national security, and democracy, we must focus on this entire data brokerage ecosystem.

THE REGULATORY GAP

Data brokerage is a virtually unregulated practice. While there are some narrow controls around the collection, aggregation, buying, selling, and sharing of certain types of data—such as with the Health Insurance Portability and Accountability Act (HIPAA) and covered health providers, or with the Family Educational Rights and Privacy Act (FERPA) and covered educational institutions—these regulations are very limited and easily circumventable. It is remarkably easy to collect, aggregate, analyze, buy, sell, and share data on Americans, even millions at a time, without running into any legal barriers, regulatory requirements, or mandatory disclosures.

Two State laws mention data brokers: one in California and one in Vermont.[15] However, these laws are limited and insufficient to prevent the harms identified for four main reasons—and, therefore, this committee should lead and enact legislation to regulate the data brokerage ecosystem.

First, both State laws focus merely on disclosure. They do not put meaningful restrictions on data collection, aggregation, or analysis or on the buying, selling, and sharing of data by companies classified as "data brokers." Instead, they focus on requiring those companies to register with the State, after which basic company information (*e.g.,* the company's name) is published in a registry on the respective State government's website.[16] The Vermont law also imposes a few basic technical requirements to protect the security of what it describes as individuals' "personally identifiable information," though this is aimed at preventing data breaches instead of putting controls on data sales.[17]

Second, these laws define data brokers (generally) as only those companies buying and selling data on people with whom they do not have a direct business relationship. This definition excludes every single company that buys, sells, and shares data on its own customers from coverage under a "data broker" law. In practice, if this definition were paired with substantive controls, much of the data brokerage ecosystem would escape regulation. This definition is also insufficient because some firms occupy gray areas vis-à-vis these laws: for example, Oracle has registered as a data broker in both States, but it appears to buy and sell data it did not directly collect from consumers—as well as data it may collect directly but through subsidiaries. The same could be argued with respect to online advertisers, which frequently have direct interactions with consumers but often in ways consumers do not recognize or understand.[18]

Third, even with the given definitions of data brokers, the two State laws do not target the underlying ecosystem—the collecting, aggregating, analyzing, buying, selling, and sharing of Americans' data. The practice of buying and selling data with virtually no restrictions enables consumer exploitation, civil rights abuses, and direct threats to U.S. national security, but it is not meaningfully controlled by these laws. And even with a legal focus on specific "data broker" entities, many firms that engage in data brokerage are not captured in the laws, due to last-minute defini-

---

[15] These are, respectively, California Civil Code § 1798.99.80 and Vermont Statute 9 V.S.A. § 2430.

[16] The California registry can be found at: *https://oag.ca.gov/data-brokers.* The Vermont registry can be found at: *https://bizfilings.vermont.gov/online/DatabrokerInquire/DataBrokerSearch.*

[17] Vermont Statute 9 V.S.A. § 2447. Data broker duty to protect information; standards; technical requirements.

[18] For more on how these laws provide lessons for writing a Federal privacy legislation, *see:* Justin Sherman, "Federal Privacy Rules Must Get 'Data Broker' Definitions Right," *Lawfare,* April 8, 2021, *https://www.lawfareblog.com/federal-privacy-rules-must-get-data-broker-definitions-right.*

tional changes obtained by industry lobbyists prior to State-level enactment: companies that buy and sell data on their direct customers; third-party code providers that plug into apps and websites to collect data on unwitting individuals; companies that run real-time bidding networks for online advertisements, where dozens of companies get access to data on consumers whom they could target with paid ad access.

Lastly, these laws rely on the notion that some data is clearly personally identifiable while other data is not. There is a difference between data with an individual's name attached and data which does not have a name attached, but that line is increasingly blurring. The sheer volume of data that exists on any given American—including for sale on the open market—means individuals, companies, and government agencies can easily combine datasets together to unmask or "reidentify" the person behind a piece of information. For instance, researchers unmasked supposedly anonymized ride data for New York City taxi drivers and could then calculate drivers' incomes.[19] Basing laws too much on this distinction does not recognize the complicated reality, where simply removing a name or Social Security number from a dataset does not meaningfully protect individuals' privacy. This distinction can also allow companies to circumvent the narrow legal restrictions that do protect individuals' data, because they can buy, sell, and share Americans' information without a name attached and simply acquire other identifying data or perform their own reidentification separately.

THE CONGRESSIONAL RESPONSE

Congress has an opportunity to regulate the data brokerage ecosystem, protecting Americans' civil rights, U.S. national security, and democracy in the process. While a strong, comprehensive consumer privacy law is important, Congress must not wait to resolve the debate on such a law to regulate the data brokerage industry.

There are three steps Congress can take now:

Strictly control the sale of data collected by data brokers to foreign companies, citizens, and governments. Currently, there is virtually nothing in U.S. law preventing American companies from selling citizens' personal data—from real-time GPS locations and health information to data on military personnel and government employees—to foreign entities, including those entities which pose a risk to U.S. national security. As a result, it is far too easy for a foreign government to set up a front company through which it can simply buy highly sensitive data on millions of Americans, including members of Congress, Federal Government employees, and military personnel. In response, Congress should develop a set of strict controls on data brokers' sales of data to foreign companies, citizens, and governments—weighing outright prohibitions in some cases (*e.g.,* on selling data on government employees and military personnel) and conditional restrictions in others (*e.g.,* banning sale to a particular end user determined, through a robust security review process, to have requisite links to a foreign military or intelligence organization). As more and more U.S. citizen data is available for sale on the open market, this set of restrictions would better protect national security and also protect against exploitation of American consumers by foreign corporations.

Strictly control the sale of data in sensitive categories, like genetic and health information and location data. Congress should also consider banning the sale of certain categories of data altogether. While many kinds of data can be used in harmful ways, some categories are arguably more sensitive than others. For instance, individuals' genetic information is highly sensitive. Location data is also a very dangerous kind of data. With GPS data, law enforcement agencies operating without adequate oversight as well as foreign intelligence organizations, terrorist groups, criminals, and violent individuals could acquire this data to follow people around as they visit bars, restaurants, medical centers, divorce attorneys, police stations, religious buildings, military bases, listed and unlisted government facilities, their relatives' homes, and their children's schools. Based on tracking U.S. citizens as they walk, travel, shop, sit, and sleep, organizations and individuals intent on doing harm can also derive other sensitive information about Americans' health, income, lifestyle, and more. Congress should develop a list of sensitive data categories that each correspond to bans on sale or other controls.

Stop data brokers from circumventing those controls by "inferring" data. If data brokers are prevented from collecting, aggregating, buying, selling, and sharing cer-

[19] Marie Douriez et al., "Anonymizing NYC Taxi Data: Does It Matter?", 2016 IEEE International Conference on Data Science and Advanced Analytics, October 2016, *https://ieeexplore.ieee.org/document/7796899.*

tain kinds of data and/or selling it to and sharing it with certain entities, they may still get data using their third vector—analyzing data and making "inferences" from it. For instance, if data brokers were prohibited specifically from buying and selling Americans' GPS location histories, a company could still, in line with current practice, mine individuals' spending histories, WiFi connection histories, phone call logs, and other information to derive the data that is supposed to be controlled in the first place, without *technically* "collecting" GPS location itself. Congress should stop data brokers from circumventing controls by implementing additional prohibitions around "inferring" categories of sensitive information about individuals. This will tackle the third main way data brokers currently get their data—and prevent companies from circumventing controls to keep exploiting Americans.

The data brokerage ecosystem perpetuates and enables civil rights abuses, consumer exploitation, and threats to U.S. national security and democracy. It operates with virtually no regulation. Rather than waiting to resolve the debate over a strong, comprehensive consumer privacy law—which is also sorely needed—Congress can and should act now to regulate data brokerage.

PREPARED STATEMENT OF HON. ELIZABETH WARREN,
A U.S. SENATOR FROM MASSACHUSETTS

Good morning, and welcome to today's hearing of the Subcommittee on Fiscal Responsibility and Economic Growth. I'm pleased to be working with Ranking Member Cassidy on this hearing on "Promoting Competition, Growth, and Privacy Protection in the Technology Sector." Senator Cassidy will be joining us remotely. We're going to do a mixed hearing with some people in person and some people remote.

Under President Biden's leadership, the American economy is rebounding. The unemployment rate has dropped from a pandemic height of 14.8 percent in April 2020 to 4.6 percent today.[1] Five point six million jobs[2] have been added since President Biden's inauguration—more than was added during the first 10 months of any administration since we've been keeping records. Child poverty is projected to plummet by more than 40 percent[3] thanks to the American Rescue Plan.

All of this has occurred despite an ongoing pandemic that has plagued us for nearly 2 years. Families have tried to adapt, and those changes have echoed throughout our economy. Demand has shifted[4] as people have consumed fewer services while buying more durable goods like exercise equipment and home appliances. The economy has recovered more quickly[5] than many businesses projected and all of this is contributing[6] to unexpected bottlenecks in our supply chains and sporadic shortages in warehouses.

And these factors contribute to price increases for many consumer goods. But they are not the only reasons prices have gone up.

Sure, giant companies will raise prices when they have to. But they will also raise prices when they can get away with it. And how do we know this? Because when companies are simply passing along increases in their costs, then profit margins should stay the same. But when companies see a chance to gouge consumers, particularly while everyone is talking about inflation, then those companies raise their prices beyond what's needed to cover their increased costs.

Right now prices are up at the pump,[7] at the supermarket,[8] and online. At the same time, energy companies,[9] grocery companies, and online retailers[10] are report-

---

[1] *https://www.bls.gov/news.release/pdf/empsit.pdf.*
[2] *https://www.dol.gov/newsroom/releases/osec/osec20211105.*
[3] *https://www.urban.org/sites/default/files/publication/104626/how-a-permanent-expansion-of-the-child-tax-credit-could-affect-poverty_1.pdf.*
[4] *https://www.bls.gov/opub/mlr/2021/beyond-bls/COVID–19-causes-a-spike-in-spending-on-durable-goods.htm.*
[5] *https://www.nytimes.com/2021/04/06/business/imf-outlook-global-economy.html.*
[6] *https://www.businessinsider.com/why-store-shelves-are-empty-supply-chain-crisis-shortages-2021-10.*
[7] *https://www.nytimes.com/2021/11/23/business/biden-oil-reserves-gas-prices.html.*
[8] *https://www.today.com/food/groceries/how-to-save-money-on-groceries-rcna36938.*
[9] *https://www.cnn.com/2021/10/29/energy/exxonmobil-chevron-profits/index.html.*
[10] *https://www.cnbc.com/2021/11/30/amazon-touts-record-sales-amid-weak-start-to-holiday-shopping-season.html.*

ing record profits. That's not simply a pandemic issue. It's not simply some inevitable economic force of nature. It's greed—and in some cases, it is flatly illegal.

One reason for this price gouging is that fewer and fewer markets in America are truly competitive. When several businesses are competing for customers, companies can't use a pandemic or a supply chain kink to pad their own profits. In a competitive market, the margin above costs stays steady, even in troubled times. But in a market dominated by one or two giants, price gouging is much easier.

For generations, policymakers and regulators under both Democrats and Republicans promoted free-market competition. But starting in the 1970s,[11] our government changed course. For decades now regulators and courts have looked the other way even as one sector after another has become dominated by one or two giants. They rubber-stamp merger after merger without regard to the consequences, and when small businesses got wiped out and startups were smothered or bought out, they just didn't care.

Today, as a result of increasing consolidation across industries, bigger and bigger corporations have more and more power to charge their customers any price they want. They also wield more and more power to under-invest in things like supply chain resiliency, and more and more power to hold down wages and benefits for workers.

And it's getting worse. Earlier this month, Federal Trade Commission Chair Lina Khan noted[12] that by September of this year, our antitrust agencies had already received more merger filings than any other year in the previous decade. In fact, they are on track in 2021 to receive a 70 percent increase above average filings in recent years.

Giant corporations[13] are taking advantage of this global crisis to gobble up struggling small businesses and to increase their power through predatory mergers. I introduced my Pandemic Anti-Monopoly Act[14] last year to slow down this trend and to protect workers and small businesses and families from being squeezed even more by harmful mergers during this crisis, and I will reintroduce it this year because the need is clear.

The effects of limited competition in our technology sector are particularly severe, and that is why I'm interested in exploring today's hearing. Limited competition in tech is having spillover effects across our entire economy. Anticompetitive practices[15] in the semiconductor industry have exacerbated[16] supply-chain issues. Big Tech firms have used their dominance to inflate prices[17] throughout the online retail market and to subject their workers to inhumane conditions[18] during the pandemic. And as Ranking Member Cassidy has rightly highlighted in his own work, tech firms collect and exploit[19] sensitive personal information—often threatening national security,[20] harming our emotional health,[21] and discriminating[22] against vulnerable groups.

It doesn't have to be like this. With stronger antitrust laws and robust enforcement, we can ensure that our economy works for American families, not just for the wealthiest corporations. Congress could provide better tools to the FTC and the Department of Justice to investigate anticompetitive mergers and break up the companies that have held our economy down. We could also make it easier for the agencies

---

[11] *https://hbr.org/2017/12/the-rise-fall-and-rebirth-of-the-u-s-antitrust-movement.*

[12] *https://www.ftc.gov/system/files/documents/public_statements/1598131/statement_of_chair_lina_m_khan_joined_by_rks_regarding_fy_2020_hsr_rep_p110014_-_20211101_final_0.pdf.*

[13] *https://publicknowledge.org/acquisitions-in-the-time-of-covid-big-tech-gets-bigger/.*

[14] *https://www.warren.senate.gov/newsroom/press-releases/warren-ocasio-cortez-to-introduce-pandemic-anti-monopoly-actread-one-pager-here.*

[15] *https://www.wsj.com/articles/ftc-charges-broadcom-with-illegal-monopolization-proposes-consent-order-11625248681.*

[16] *https://www.wsj.com/articles/the-world-relies-on-one-chip-maker-in-taiwan-leaving-every-one-vulnerable-11624075400.*

[17] *https://www.vox.com/recode/22810795/amazon-marketplace-prime-report.*

[18] *https://www.npr.org/2021/02/17/968568042/new-york-sues-amazon-for-COVID–19-workplace-safety-failures.*

[19] *https://theconversation.com/the-ugly-truth-tech-companies-are-tracking-and-misusing-our-data-and-theres-little-we-can-do-127444.*

[20] *https://www.forbes.com/sites/joetoscano1/2021/12/01/data-privacy-issues-are-the-root-of-our-big-tech-monopoly-dilemma/?sh=5d3aba083cfd.*

[21] *https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.*

[22] *https://algorithmwatch.org/en/automated-discrimination-facebook-google/.*

to reject such mergers in the first place. By promoting competitive markets for consumers and workers, we can foster a stronger American economy and a stronger American democracy.

So I look forward to discussing these issues today. I appreciate all of our witnesses who are joining us, and I look forward to hearing about your insights and experiences.

Statement of the International Brotherhood of Teamsters and the Strategic Organizing Center

The International Brotherhood of Teamsters is America's largest, most diverse union. We represent 1.4 million hardworking men and women throughout the United States, Canada and Puerto Rico. We started in 1903 as a merger of the two leading team driver associations. As we say, "these drivers were the backbone of America's robust economic growth, but they needed to organize" to get their fair share from too-powerful corporations. The Strategic Organizing Center is a democratic federation of labor unions representing millions of working people. We strive to ensure that every worker has a living wage, benefits to support their family and dignity in retirement, and we advocate not just for jobs, but for good jobs: safe, equitable workplaces where all employees meaningfully participate in the decisions affecting their employment. Our organizations are concerned with ensuring corporate power does not overshadow the authority, autonomy and well-being of workers—or anyone else—in our country, and we believe that antitrust law has a vital role to play in that effort. We thank you for holding today's hearing and hope you will use this time to examine the impact of anticompetitive behavior in the technology sector on labor market and workers.

We are not the first to observe troubling trends in our economy. These include a decline in real wages in spite of significant productivity growth, a huge and growing gap between the wealthy and the rest of us, an increasingly fissured workforce that allows employers to shift labor costs—and deny responsibility for the safety and economic security of the workers that create their wealth—onto others. They also include the disproportionate impact these trends have on workers who are people of color and on reinforcing racism in our economic structure. The concentration of power of large corporations across the economy is of significant concern because this concentration drives and exacerbates all of these trends. We are particularly concerned about the largest digital platform companies because they are able to exercise unprecedented power in our economy in ways that negatively impact workers, consumers and other economic players—and the very structure of the economy itself. Unions—and workers' authority as union members to negotiate employment terms with their employer—are a potent counterweight to concentrated corporate power in labor markets, but we also recognize the paramount importance of the overall structure of the economy and ways that corporate power is dispersed: the very subject that antitrust law was meant to address.

During this period of growing corporate consolidation, antitrust laws have weakened dramatically—not because Congress has changed the laws, but because the courts have. A defining feature of court-made, "modern" antitrust law is its singular focus on the consumer welfare standard, under which courts have deemed consumer price increases the primary cognizable competitive harm. This fundamental misinterpretation of both the purpose and the language of antitrust law ignores myriad other forms of harm including declining quality, diversity, innovation, choice, and anticompetitive concentration in supply markets, including labor markets—which in turn has allowed these additional competitive harms to manifest in our economy along with highly concentrated corporate power.

It is against this backdrop that we join the growing chorus that considers the hollowing-out of competition law over the past several decades at least partly responsible for the increase in corporate might and the corresponding decline in virtually every other source of power in our economy—workers over their jobs, consumers over choice and privacy, and small businesses over where and at what price they sell their goods. We strongly advocate vigorous antitrust reform to both restore needed protections for competition among diverse participants in the economy, and address the challenges that new, uniquely dominant digital platform companies present. We also believe that our Nation's antitrust laws must be updated to address the current economic realities—including that consumer welfare, or price, should not be the sole touchstone of competitive harm, and further, to foreclose judicial distortion of the law. We urge this reform to ensure that antitrust law plays

the role that Congress intended by leveling the playing field for workers, consumers, small businesses and other market participants in our economy.

As explained further below, our concerns are driven by evidence of increased corporate concentration across the economy and the effects of this concentration on all market participants, and workers in particular, as well as the rise of extraordinarily powerful digital platform companies with unique characteristics that current antitrust law is ill-suited to address. This statement outlines our specific concerns regarding the current state of antitrust law, and details specific aspects of antitrust law and jurisprudence that we believe are the most in need of reform to protect and promote a robust, competitive economy, including fair and competitive labor markets where workers have a fair shot at family-supporting wages, safe working conditions and a job they can be proud of.

CONCENTRATION ON THE RISE IN BOTH PRODUCT AND LABOR MARKETS

The U.S. has a market concentration problem. In terms of product markets, over the last 2 decades approximately 75 percent of U.S. industries have become more concentrated.[1] Since 1980, in a variety of sectors across the economy, the four largest firms have significantly increased their share of sales.[2] With respect to efficiency and innovation, this is a cause for concern. The entry rate of new firms into the U.S. market has fallen sharply, particularly since 2007,[3] while firm exit rates have remained relatively flat.[4] In other words, the number of firms in various industries is declining, and existing producers are gaining share while new entrants find it increasingly difficult to challenge the established dominant players. This implies a lack of economic dynamism and increased market concentration.

Over the past decade, empirical evidence has demonstrated that the majority of local labor markets in the U.S. are also overly concentrated. Research indicates that 20 percent of all U.S. workers work in highly-concentrated labor markets,[5] and that, across all U.S. labor markets, the average measurement of labor market concentration well exceeds the Federal Trade Commission and Department of Justice's own guidelines.[6] Labor market concentration—or labor monopsony, the corollary of monopoly in the supplier or labor market—may significantly impact the wages and working conditions of workers. Labor monopsony power, alongside persistent trends including declining labor mobility,[7] can lead to negative outcomes for U.S. workers. A range of studies have shown that workers in highly concentrated labor markets receive suppressed wages,[8] less non-wage compensation in the form of health benefits,[9] and are more likely to be subject to labor rights violations.[10] Further, such negative impacts fall much more heavily on workers who are people of color, so

---

[1] *See* Gustavo Grullon, Yelena Larkin, and Roni Michaely, *Are U.S. Industries Becoming More Concentrated?,* Review of Finance, Swiss Finance Institute Research Paper No. 19–41 (October 25, 2018) at 1, *available at https://ssrn.com/abstract=2612047.*

[2] *See* Ufuk Akcigit and Sina Ates, *Slowing Business Dynamism and Productivity Growth in the United States,* Federal Reserve Bank of Kansas City publication (October 8, 2020) at 4, 31 note 31, 45, *available at https://www.kansascityfed.org/documents/4952/aa_jh_201008.pdf.* The sectors are manufacturing, retail trade, wholesale trade, services, utilities and transportation, and finance. *Id. See also* David Dayen, *Monopolized: Life in the Age of Corporate Power* at 3 (2020) (noting that in the markets for airlines, commercial banking, and phone, wireless, cable, and Internet services, four companies control the market).

[3] *See* John Haltiwanger, *Entry, Innovation and Productivity Growth in the U.S. Economy,* Federal Reserve Bank of Dallas publication (May 31, 2018) at 9, *available at https://www.dallasfed.org/-/media/Documents/research/events/2018/18ted-haltiwanger.pdf.*

[4] *Id.*

[5] *See* José Azar, Ioana Elena Marinescu, Marshall Steinbaum, and Bledi Taska, *Concentration in US Labor Markets: Evidence from Online Vacancy Data,* NBER at 2 (August 10, 2018), *available at https://www.nber.org/system/files/working_papers/w24395/w24395.pdf.*

[6] *See* José Azar, Ioana Elena Marinescu, and Marshall Steinbaum, *Labor Market Concentration,* NBER at 2 (December 10, 2018), *available at https://www.nber.org/system/files/working_papers/w24147/w24147.pdf.*

[7] *See* Damien Azzopardi, Fozan Fareed, Mikkel Hermansen, Patrick Lenain, and Douglas Sutherland, *The decline in labor mobility in the United States: Insights from new administrative data,* OECD (December 14, 2020), *available at https://www.oecd-ilibrary.org/docserver/9af7f956-en.pdf?expires=1615398612&id=id&accname=guest&checksum=19D81A08C345C32998FCE5FBCBBBE60B.*

[8] Azar, Marinescu, and Steinbaum, *supra* note 6.

[9] *See* Yue Qiu and Aaron J. Sojourner, *Labor-Market Concentration and Labor Compensation,* IZA Institute of Labor Economics (January 8, 2019), *available at https://ssrn.com/abstract=3312197.*

[10] *See* Ioana Elena Marinescu, Yue Qiu, and Aaron J. Sojourner, *Wage Inequality and Labor Rights Violations,* IZA Institute of Labor Economics (August 13, 2020), *available at https://ssrn.com/abstract=3673495.*

labor market concentration also exacerbates the existing problems of inequality and ongoing racism affecting our economy.

Further, research suggests that monopolizing employers do not pass on cost savings they receive from reduced wages to consumers.[11] Instead, dominant employers tend to retain savings from lower wages.[12] At the same time, lower wages can increase consumer prices because employers purchase less of the input (labor), which results in higher marginal costs per product, and thus higher prices.[13]

In spite of the problems caused by labor market concentration, labor market antitrust litigation against employers is extremely rare. Since 1960, there have been fewer than 100 labor market cases compared to over 2,300 product market antitrust cases.[14] Fully half the labor market cases that have been brought under section 1 of the Sherman Act have addressed only the niche employment setting of sports leagues.[15] At the same time, not a single labor market case brought under section 2 of the Sherman Act has survived summary judgment.[16] This "litigation gap" is exacerbated by the lack of attention to labor market effects in the Department of Justice and Federal Trade Commission's current Horizontal Merger Guidelines.[17] Indeed, no merger has ever been blocked based on increased labor market concentration.

The lack of antitrust enforcement and successful cases regarding labor markets is another illustration—an even more extreme one—indicating that current antitrust jurisprudence is the product of judicial interpretation rather than congressional intent. There is broad agreement that the Clayton Act provides for review of the effects of mergers on labor markets as well as on product markets. Indeed, Congress's intention to protect labor markets from the harms of monopsony power has been clear since the inception of U.S. antitrust policy: One of the reasons Senator John Sherman gave for legislating against monopoly was that "[i]t commands the price of labor without fear of strikes, for in its field it allows no competitors."[18]

Contrary to Sherman's intent, courts have generally failed to properly adjudicate or even recognize labor claims under antitrust law. With limited exceptions, including piecemeal victories against certain "no poaching" agreements,[19] the courts have proven largely unreceptive to labor monopsony claims, and instead over the years have eroded important antitrust precedents beneficial to labor.[20] This contradicts not only the original intention of key laws meant to protect fairness in the economy, but also severely limits the ability of workers to vindicate important rights through antitrust law.

This history explains why, to be meaningful, any antitrust reform must not only be written clearly and with enough specificity to prevent courts from subverting its meaning and intent, but must also be emphatically clear that competition in labor markets as well as product markets is protected.

RISE OF DIGITAL ECONOMY REQUIRES NEW LAW AND ENFORCEMENT

In addition to concerns related to the broader U.S. economy, the rise of dominant digital companies present unique issues and threats to competition and people's welfare. Companies including Amazon, Apple, Facebook and Google are increasingly dominant across a number of markets including e-commerce, online search, online advertising and cloud computing. It has been projected, for example, that Amazon's

---

[11] *See* Alan James Devlin, "Questioning the Per Se Standard in Cases of Concerted Monopsony," *Hastings Business Law Journal,* Vol. 3, No. 223, 2007 at 224 (July 6, 2009) (citing statements by DOJ antitrust division officials regarding the consumer price impact of monopolies), *available at https://repository.uchastings.edu/cgi/viewcontent.cgi?article=1106&context=hastings_business_law_journal.*

[12] *Id.* at 231.

[13] *Id.*

[14] *See* Eric A. Posner, *Why the FTC Should Focus on Labor Monopsony, Pro Market* (November 5, 2018), *available at https://promarket.org/2018/11/05/ftc-should-focus-labor-monopsony/*.

[15] *See* Ioana Elena Marinescu and Eric A.Posner, *Why Has Antitrust Law Failed Workers?,* 105 *Cornell L. Rev.* 1343, 1365 (2020), *available at https://ssrn.com/abstract=3335174.*

[16] *Id.* at 1371.

[17] *Horizontal Merger Guidelines* (revised April 8, 1997). Department of Justice/Federal Trade Commission, *available at https://www.justice.gov/atr/horizontal-merger-guidelines-0.*

[18] *See* Congressional Record 2457 (1890), *available at https://appliedantitrust.com/02_early_foundations/3_sherman_act/cong_rec/21_cong_rec_2455_2474.pdf.*

[19] *See* Marinescu and Posner, *supra* note 16.

[20] *See* Marshall Steinbaum, "Antitrust, the Gig Economy, and Labor Market Power," *Law and Contemporary Problems* at 49 (June 12, 2019), *available at https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=4918&context=lcp.*

market share will account for 50 percent of the entire e-commerce market in 2021.[21] Many sources have documented how these companies have utilized their dominance in ways that harm consumers, small businesses, and workers as these platforms seek to expand, including self-preferencing over businesses competing on their platforms, data collection and use practices that may harm consumers, and the decline in diversity in such industries as publishing because of consolidated control.[22] Meanwhile, the Amazon Web Services (AWS) segment of Amazon's business controls 32 percent of the cloud computing market, greater than the share held by AWS's three largest competitors combined.[23] While many industries are dominated by only four corporate players, in the Big Tech arena a single company often dominates the market: for example in social media (Facebook), Internet search (and search advertising) (Google), or e-commerce (Amazon).[24]

Such consolidation of control over product markets begets control over corresponding labor markets. The example of Amazon is again illustrative of this phenomenon. Following unrelenting expansion of its business, Amazon now employs approximately 1.3 million workers worldwide,[25] the majority in the U.S. The company's growth within labor markets is both record breaking[26] as well as diverse in terms of the categories of workers affected. Indeed, from white collar technology workers to blue collar warehousing workers, Amazon is an increasingly powerful employer. For example, it is now estimated that Amazon employs fully one-third of all warehousing workers in the U.S.[27] As a consequence of Amazon's power in warehousing labor markets, there are reports that in areas where the company has established warehouses, wages for warehouse workers have declined.[28]

The power of dominant tech companies in labor markets has also contributed to—and accelerated—the fissuring of the American workplace. Fissuring has allowed corporations to treat large portions of their workforces as non-employees, and to shift responsibility for their workforce's work conditions, safety and well-being out of their sphere of corporate liability.[29] We find this trend highly problematic as it not only shifts responsibility away from corporations but also reduces worker power to secure decent wages and working conditions and address workplace abuses. We believe that this increasing labor market dominance and fissuring by large digital companies should not go unchecked.

The need for updated tools to regulate dominant digital companies has been written about elsewhere at length,[30] but we note that dominant digital companies have several unique features for which current antitrust law—particularly in its current anemic, price-focused form—is ill-suited. Features of these companies include platform or other utility-like structures that generate network effects: the platform becomes more and more valuable as more people use it. These network effects accumu-

---

[21] *Projected retail e-commerce GMV share of Amazon in the United States from 2016 to 2021,* Statista (December 1, 2020), *available at https://www.statista.com/statistics/788109/amazon-retail-market-share-usa/.*

[22] *See* Investigation of Competition in Digital Markets, Subcommittee on Antitrust, Commercial, and Administrative Law of the House Committee on the Judiciary (2020); Petition for Investigation of Amazon.com, Inc., submitted to Federal Trade Commission (2020), *available at http://www.changetowin.org/wp-content/uploads/2020/02/Petition-for-Investigation-of-Amazon.pdf.* Regarding the impact of Amazon's 65-percent market share in e-books over diversity in publishing, *see* Lina M. Khan, "Amazon's Antitrust Paradox," 126 *Yale L.J.* 710, 766 (2017), *available at https://www.yalelawjournal.org/note/amazons-antitrust-paradox.*

[23] *Cloud Infrastructure Spend Grows 46 percent in Q4 2018 to Exceed U.S.$80 Billion for Full Year,* CANALYS (February 4, 2019), *available at https://www.canalys.com/newsroom/cloud-market-share-q4-2018-and-full-year-2018.*

[24] Dayen, *supra* note 2.

[25] *See* Form 10–K for Amazon, Inc. filed with the U.S. Securities and Exchange Commission, February 3, 2021, at 4, *available at https://www.sec.gov/ix?doc=/Archives/edgar/data/1018724/000101872421000004/amzn-20201231.htm.*

[26] Michael Mandel, *A Historical Perspective on Tech Job Growth,* Progressive Policy Institute, (January 13, 2017), *available at https://www.progressivepolicy.org/wp-content/uploads/2017/08/PPI_TechJobGrowth_V3.pdf.*

[27] According to Bureau of Labor Statistics estimates, the warehousing and storage sector counted a total of 1,194,400 employees in June 2020. The total number of Amazon warehousing and storage workers was approximately 425,000 as of June 2020, or 36 percent of the sectoral total.

[28] *See, e.g.,* "Amazon Has Turned a Middle-Class Warehouse Career Into a McJob," *Bloomberg,* December 17, 2020, *available at https://www.bloomberg.com/news/features/2020-12-17/amazon-amzn-job-pay-rate-leaves-some-warehouse-employees-homeless;* "Unfulfillment Centre: What Amazon does to wages," *The Economist,* January 20, 2018, *available at https://www.economist.com/united-states/2018/01/20/what-amazon-does-to-wages.*

[29] *See* David Weil, *The Fissured Workplace* (Harvard University Press 2014).

[30] *See, e.g.,* Khan, "Amazon's Antitrust Paradox," 126 *Yale L.J.* 710.

late and multiply until a tipping point is reached, beyond which entry by new competitor platforms is difficult. As a result, these markets become essentially winner-take-all. Second, in part because of the potential network effects, these companies' corporate strategies turn on growth—acquisition of market share—and not profit. Similarly, companies also focus on expanding their business lines, including through acquisitions whose aim is to eliminate nascent competition. Finally, for digital platform companies, the acquisition and use of data play a key role in both the value of the company and how it can exercise dominance and exclude others from markets. Relatedly—because companies invariably have been able to acquire data for free—digital companies' services are often "free" to consumers, which makes traditional consumer welfare-price analysis inapplicable.

Because of the unique features of these platform companies, antitrust reform must develop new tools suited to these types of firms. These tools must include: recognizing harms beyond consumer welfare/price and traditional profit-driven strategies for growth; recognizing the value of consumer data acquisition and use in exchange for supposedly "free" services; and grappling with the ability of such companies to exercise dominance and squelch new entry and competition at lower-than-monopoly levels of market share, because of the network effect features of such platforms.

With the dominance of large digital platform companies comes equally problematic power in labor markets: In the high tech industry, tech companies dominated by colluding to prevent competition among high tech employees for jobs.[31] Google workers have complained en mass regarding sexual harassment and anti-union as well as race-related dismissals.[32]

In addition, the extraordinary growth of Amazon's direct and indirect employment, as discussed above, has impacted labor markets. Amazon's dominance in employment has brought reports that Amazon's warehouses result in declining warehouse wages in areas where they locate.[33] The New York Attorney General believes Amazon has so blatantly ignored State COVID safety protocols in New York that she has sued Amazon under general public safety laws, seeking injunctive relief including disgorgement of profits.[34] Amazon continues to exercise its power to substantially increase fissuring of the workplace, including by pushing employment responsibility onto hundreds of small delivery businesses that it effectively controls, and by using thousands of delivery/logistics drivers who not only are without traditional employment protections as independent contractors, but are also subject to unrelenting delivery load and speed demands that may compromise safety.[35] Similarly, it has created a whole new army of Prime Now shoppers who pick and delivery groceries, again as "gig workers" with none of the traditional protections of employment.

In addition, such corporations are able to mount vigorous corporate backlash against workers who attempt to exercise their right to organize. At Amazon, the company tried to recruit "labor spies and anti-union analysts with background in Federal intelligence work,"[36] to surveille its direct employees for union activity. The

---

[31] "Judge Koh OKs $415M Google, Apple Anti-Poaching Deal," *Law360,* Sept. 3, 2015, *available at https://www.law360.com/articles/677683/judge-koh-oks-415m-google-apple-anti-poaching-deal.*

[32] "Hundreds of Google Employees Unionize, Culminating Years of Activism," *New York Times* (January 4, 2021), *available at https://www.nytimes.com/2021/01/04/technology/google-employees-union.html#:~:text=OAKLAND%2C%20Calif.,staunchly%20anti%2Dunion%20Silicon%20Valley.*

[33] *See supra* note 29 and accompanying text.

[34] *James v. Amazon.com, Inc.* (NY Sup. Ct., Feb. 16, 2021). *See also Palmer v. Amazon,* 20–cv–02468–BMC (E.D.N.Y. June 20, 2020) (public nuisance suit brought against Amazon alleging that Amazon's failure to protect workers adequately from COVID created a public nuisance, a common law tort that endangered public safety). The suit was dismissed on the grounds that OSHA preempts State claims regarding workplace safety. *Palmer,* Slip Op. (November 2, 2020). *See also Smalls v. Amazon,* 20–05492 (E.D.N.Y., November 12, 2020) (class action Federal civil rights case alleging that Amazon violated civil rights statutes by failing to protect a workforce that has a majority of people of color from the dangers of COVID.) *Smalls* is still pending in Federal court in the Eastern District of New York.

[35] "Amazon's Next-Day Delivery Has Brought Chaos and Carnage to America's Streets," *BuzzFeed,* August 31, 2019, *available at https://www.buzzfeednews.com/article/carolineodonovan/amazon-next-day-delivery-deaths.*

[36] "12 Facts About Morgan Lewis, Amazon's Powerful Anti-Union Law Firm," LaborOnline, Feb. 18, 2021 (citing report that Amazon posted-and then deleted-a job listing for an 'intelligence analyst' to monitor workers' efforts to unionize, Business Insider, September 1, 2020), *available*

Continued

company even allegedly conducted anti-union surveillance of its independent contractor Flex drivers, manifesting an "Orwellian" program that allegedly monitored as many as 43 driver Facebook accounts for hints of union sympathies.[37] The company is also pursuing a highly-funded, vicious union-busting campaign at Amazon's 6,000-worker warehouse facility in Bessemer, AL where workers are voting on union representation this month.[38]

RECOMMENDATIONS FOR ANTITRUST REFORM

For reasons discussed above, we urge vigorous antitrust reform. Meaningful reform should include the following:

(a) *Eliminate rule of reason:* Eliminate the highly open-ended and problematic "rule of reason" decision-making, in favor of a clear, simple rules against abuse of market power, to prevent courts misinterpreting the law or imposing additional barriers to antitrust protections in the future.[39] As this implies, parties should be permitted to prove an antitrust violation by showing anti-competitive harm from a dominant firms' conduct in a labor or product market. Firms should not be able to defend, or rebut, evidence of abusive conduct by offering a pro-competitive justification. Piecemeal or partial rules that permit certain pro-competitive justifications, or that allow other "rule of reason" defenses provide too great an opening for continued judicial lawmaking and subversion of antitrust protections.

(b) *Include labor markets in merger reviews:* For merger review, establish labor market-related filing triggers, and require consideration of the effects on labor market concentration of all mergers reviewed.

(c) *Prohibit anti-competitive worker restraints:* Prohibit outright anticompetitive worker restraints such as noncompetes and no poach restrictions. Such restrictions directly interfere with workers' mobility and limit their ability to compete for different jobs with better wages or other terms of employment. These restraints exacerbate inequality and the imbalance between corporate and worker power, distorting competition in labor markets. Similarly, unfair and anti-competitive mandatory arbitration clauses should be made illegal and unenforceable.

(d) *Provide for labor monopsony claims clearly and expressly:* Expressly provide for labor monopsony claims under antitrust laws by including abuse of labor market power and exclusionary conduct in labor markets in antitrust laws and legal standards. These changes should be done using clear and express language so that courts may not refuse to apply antitrust laws to labor monopsony behavior.

(e) *Establish an appropriate threshold for labor market power:* Establish a lower market share threshold at which a firm is presumed to have market power. Evidence suggests that a special feature of labor markets is that they become significantly less competitive at lower levels of concentration than product markets; we thus urge a 20 percent threshold for labor markets.[40]

---

at http://www.lawcha.org/2021/02/02/12-facts-about-morgan-lewis-amazons-powerful-anti-union-law-firm/.

[37] "Amazon Flex Driver Fights Attempt to Arbitrate Privacy Claims," *Law360,* March 1, 2021 (detailing Amazon Flex driver's class allegations that Amazon "purportedly hired intelligence experts to use automated tools and monitoring software to track and intercept drivers' social media activity."), *available at https://www.law360.com/articles/1359635/amazon-flex-driver-fights-attempt-to-arbitrate-privacy-claims.*

[38] "Amazon Is Paying Nearly 10K a Day to Anti-Union Consultants," *The Sludge* opinion, March 8, 2021, *available at https://readsludge.com/2021/03/08/amazon-is-paying-nearly-10k-a-day-to-anti-union-consultants/;* "Amazon fights aggressively to defeat union drive in Alabama, fearing a coming wave," *Washington Post,* March 9, 2021, *available at https://www.washingtonpost.com/technology/2021/03/09/amazon-union-bessemer-history/.*

[39] The last 40 years of courts weakening antitrust laws in response to Robert Bork's *The Antitrust Paradox* is the most commonly cited example of judicial activism in antitrust (Khan, *supra* note 30 at 717–721), but judicial attempts to subvert the purpose—as well as specific provisions—of antitrust law have been endemic since antitrust laws were first enacted. Khan relates how Congress outlawed predatory pricing starting in 1914, only to pass several new statutes outlawing the same practice as courts repeatedly held those statutes allowed predatory pricing conduct, until finally "by the mid-twentieth century, the Supreme Court recognized and gave effect" to the statutory prohibition on predatory pricing. *Id.* at 723–24.

[40] *See* Investigation of Competition in Digital Markets, Subcommittee on Antitrust, Commercial, and Administrative Law of the House Committee on the Judiciary (2020) at 393 ("It is the view of Subcommittee staff that the 30 percent threshold established by the Supreme Court in

(f) *Expand antitrust exemption to include gig/fissured worker organizing:* Organizing activity by workers classified as independent contractors should be exempt from antitrust laws just as employee organizing is exempt. Independently classified workers must be permitted to engage in collective activity to improve their working conditions.

(g) *Address special problems posed by Big Tech for a healthy, competitive economy:* Revise antitrust laws to address the unique characteristics of digital platform companies in ways that recognize the value to such companies of growth in market share over profits in the areas of predatory pricing, mergers and recognition of cognizable competitive harms; the threat posed by vertical integration and cross-business-line self-preferencing and exclusionary conduct; and the outsized power such firms can exercise over workers and over the fissuring of the workplace when they become dominant economic actors.

We believe that the structure of our economy matters. In order to have a fair chance at a good job, good wages, and chance to have a choice and negotiate these conditions—as well as a choice about what we buy, where we live, who has our information—it matters who has power in our economy and in our system. In all of these areas, as discussed above, we believe the power of individuals has been declining, and the power of the large corporation has increased. And it is increasingly clear that corporate concentrations of power harm consumers, workers and other market participant as well as the economy itself in a multitude of ways—from wage inequality to corporate influence on politics to innovation.

International Brotherhood of Teamsters
25 Louisiana Avenue, NW
Washington, DC 20001

Iain Gold
202–437–0963
IGold@teamster.org

The Strategic Organizing Center
1900 L Street, NW #900
Washington, DC 20036

Joan Moriarty
(917) 208–5978
JMoriarty@thesoc.org

Marka Peterson
(202) 215–6115
MPeterson@thesoc.org

Philadelphia National Bank is appropriate, although a lower standard for monopsony or buyer power claims may deserve consideration by the Subcommittee."), *available at https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519.*

COMMUNICATIONS

CENTER FOR FISCAL EQUITY
14448 Parkvale Road, Suite 6
Rockville, MD 20853
fiscalequitycenter@yahoo.com

Statement of Michael G. Bindner

Chair Warren and Ranking Member Cassidy, thank you for the opportunity to submit these comments for the record to the subcommittee on this topic.

The technology sector has certainly been an attractive target for those who seek to create a wealth tax, which is why we believe the subcommittee is addressing this topic. Whether this sector produces long-term wealth for its owners is questionable, however. Founders are often leveraged and cash flow comes, not from revenue, but from continued capitalization. When making comments on wealth and social media, I always ask the following question:

"How often do you buy a product that is advertised on the platform?"

Me neither. When I buy things, I go to Amazon and similar sites and browse. When I buy airline tickets, I go to the carrier's webpage or a page where I can compare prices. On some media sites, I may follow an ad from one influencer to another, but commercial ads are simply an annoyance, not an opportunity to buy something outside of my budget.

The jury on commercial advertising success in this sector is still out. Any regulation of such advertising is, or should be, the job of the Federal Trade Commission. Advertising in such an environment is no different than advertising in other broadcast or print media. If there are gaps in the law, they can be easily filled by the appropriate committee, which this is not.

Social media is by nature monopolistic. Our generation finds old classmates, paramours and even disconnected relatives in one place, rather than across multiple platforms. Should the inability to stay afloat without capital infusions be realized, many of us will search for different platforms as a group, using old fashioned technologies like the telephone to decide where to land. True social groups are not really a productive market for most advertising. Indeed, in order to remain friends, political debates often run out of steam.

Of late, it is the political advertisements that are attracting the most attention. There is very real concern about online sedition—although seditionists who use public sites are not the sharpest of tacks in the desk drawer.

If it were not for the lives lost and the potential for real mayhem, the Insurrection would have been comical. It was based on Mr. Eastman's rather wishful reading of the 12th Amendment. Once alternative slates became an impossibility, the winner had to be the current President. Even with all of the contested state delegations omitted, Biden still had more electoral votes. A clear reading of the Amendment states that the House counts only a majority of valid electors. Invalidating electors reduces the total.

Even if a Kangaroo Kongress had found a way to kill or detain members to get a majority to their liking, the rule of law is too strong in this nation and its military for the traitors to have succeeded. The organizers would have simply been elected immediately rather than after the current FBI and congressional investigations (including the Ethics Committee) finish their work. Our democracy was never in real danger—although members of Congress certainly were.

Most social media politics is not that blatantly stupid or dangerous. The real "muscle" of the militia movement is currently rotting in the District of Columbia jail. Most will realistically face long prison terms, as will certain members of the legislature who were in any way part of the master conspiracy. Existing law will punish the guilty, as will the Ethics Committees.

Having eliminated commerce, capital finance and sedition as concerns in the technology sector, it is time to address what is left and why there is little that can be done by this, or any other committee.

Issues of competition, growth and privacy must be considered around the issues of political speech and advertising. Platforms have, of late, been policing themselves (Twitter) or are shut down (Parler) when extremists become dangerous. Any discussions along these lines are probably best discussed by the Intelligence Committees and their staff. A new minority leader, with new staff, on the minority side of the other chamber can be trusted to get down to business.

The avenues for Congress to regulate political advertising have been foreclosed by the Constitution and the Courts. The content of political speech on social media cannot be touched. The same applies to issues and independent campaigns. That social media leaves a trail that could prove that some independent campaigns are more linked to the main campaign than is allowable is a positive.

The FEC needs adequate staffing to follow such leads—and a more robust membership model. The current structure would be comical if it did not endanger our democracy. The FEC must also build stronger relationships to the intelligence community to avoid a repeat of 2016. I suspect more shoes will drop soon.

The questions of the privacy of data in this context consist of voter identification, get out the vote and fundraising data. When funds are raised for a candidate's political committee, information must be public. For dark money committees, more sunshine is desperately needed.

President Obama's campaign perfected the tools for using technology in 2008. The Trump campaign merely followed the existing playbook. Any campaign that does not target using the same methods should not bother filing papers to get on the ballot.

Regulations on soliciting contributions and volunteers are problematic. The real gold in electoral politics are good donor and volunteer lists. The kind of donors and activists who are most in demand already know that their information is as valuable to future campaigns as it is for the ones they are currently working on.

Adding "fine print" to donations—or possibly a video to be watched before making a contribution or volunteering would be worthwhile to let first time donors know what they are truly signing up for it. I wish you luck getting such measures passed. No one wants to be the first to warn potential donors, although in the long run, it may be a selling point for reform minded candidates.

As long as the Supreme Court takes a broad view of what constitutes political speech (and measures to regulate it constitutionally have as much chance to pass as those on flag burning—and neither should pass), there is little that Congress can do to regulate political speech on the Internet.

As long as there are monied interests in politics, these issues will arise. The problem is capitalism itself. The truth is, even if capitalism is entirely replaced by a more cooperative economy, the governance of political speech should still be off the table—especially as authoritarian capitalism is in its eventual death throes. Eventually, workers will beat them at their own game.

I hope these comments have raised issues not previously discussed in this debate—which if taken to heart should end it.

Thank you for the opportunity to address the committee. We are, of course, available for direct testimony or to answer questions by members and staff. A YouTube video of these comments will be shared with the committee under separate cover.

SARA MONICA LLC
P.O. Box 168
Dunellen, NJ 08812
www.SaraMonica.com
sara@saramonica.com

Statement of Sara Maher

Amazon's Incentives for Employees' Inefficiencies

A secondary incentive for Amazon to force their employees to work unrealistic fast paces, beyond the benefit Amazon receives from the amount processed, is the additional profits Amazon illegally gains through the inefficiencies of the work that can't be done properly or correctly due to the restrictive time demands and unrealistic quotas. Most notably in 1) FBA guaranteed returns mail fraud, 2) FBA overcharges, non-reimbursements and phantom inventory, 3) vetting of counterfeits screening.

Amazon profits from what slips through the cracks when the employees are forced to work so fast that they *must* let things slip through the cracks to make their quotas. Amazon gives the impression that they're working efficiently to prevent errors, but the unrealistic working pace sets the system up for failures. Amazon's sweat shop pace actually hinders the process being done efficiently and carefully, allowing Amazon to illegally profit immensely from those failures. Amazon abuses and uses its employees as proxies for these illegal practices.

First, take another look at the insightful and truthful comments from Courtenay Brown about Amazon's "High tech sweat shops", and going forward you'll realize that Amazon is financially incentivized to be dysfunctional by design.

Courtenay Brown's quotes,

> Now Amazon doesn't care about how their workers are trained, it's all about speed and quantity . . .
>
> Workers cannot do their jobs well because Amazon wants to make more money . . . A lot of us want to do good work, but it's really frustrating because, you know, we're at a limit.
>
> Workers cannot do their jobs well because Amazon wants to make more money. That's the bottom line for them. As much product as they can get out and more money.
>
> And most importantly, And you attempt to try and do, you know, these things like give customers good quality, actually practice customer obsession, you get written up and terminated, so it's all about Amazon's profits.[1]

So, if they get punished for trying to do a good job for their customers, but rewarded for doing a bad one, and if Amazon financially benefits from the work poorly executed and from the mistakes, then that's basically the definition of dysfunctional by design, which means Amazon's executives are aware of the benefits from the dysfunctions, therefor it's fair to assume it's intentional. And if Amazon has always been aware of these mistakes, but by not fixing these mistakes Amazon benefits by immense profits, then again you have to ask, are they really mistakes anymore or are they dysfunctional by design, therefore *liable* for those mistakes. And as long as Amazon has these financial incentives and monopoly power they have no need or motivation to fix these mistakes or to do a better job for their employees and for their customers which includes their 3rd party sellers.

And remember, Amazon has 2 customer bases, 1st—The customers who purchase the products and services from the platform. And 2nd—The 3rd party sellers who pay fees to sell on the platform and use the FBA services.

The 3rd party sellers I'm referring to in this document are the American small businesses who are following the rules of Amazon's platform and the rules of the federal and state laws. I'm not referring to the 3rd party sellers, mostly in foreign countries, who are selling through FBA in America and are gaming the system by paying Amazon employees to rig the system for them, and are not accountable to federal or state laws.[2]

---

[1] Subcommittee Hearing, Promoting Competition, Growth, and Privacy Protection in the Technology Sector, Tuesday, December 7, 2021, 09:30 AM, *https://www.finance.senate.gov/hearings/promoting-competition-growth-and-privacy-protection-in-the-technology-sector.*

[2] Some Amazon Sellers Are Paying $10,000 A Month To Trick Their Way To The Top, By Leticia Miranda, BuzzFeed News Reporter, Posted on April 24, 2019, at 3:35 p.m. ET. Last up-

Continued

1—FBA Returns (Fulfillment by Amazon's returns processing warehouses).

The financial burdens and risks of FBA's returns are disproportionately put on the 3rd party sellers rather than Amazon. The extreme inefficiencies in the returns processing system frauds the 3rd party sellers out of additional and unnecessary consecutive returns processing fees on the same returned items that are often in an infinite loop going back and forth between FBA returns department and the buyers. Where stressed employees knowingly process used and damaged "non-sellable" returns, then mark them as "sellable" as a faster processing option due to unrealistic quotas, and then place the item back into inventory to be shipped to the next customer, only to get returned again due to its used condition. Employees are pushed to work so fast, that it's impossible for them to take enough time to properly inspect the condition of all the FBA returns, and a guaranteed second return of the same item gives Amazon's FBA additional fraudulent lucrative profits in FBA returns processing fees payable by the victimized unwitting 3rd party sellers. And it frauds the buyers who believed they were to receive products in new and unused condition, and potentially dangerous to the buyers depending on the condition of the compromised products. Considering this grand scale fraud is conducted through the mail, its millions of dollars in mail fraud.

An Amazon employee who worked at LEX2 processing returns made a post on Reddit where he answered questions about the LEX2 returns processing. The following quotes gives you an idea of the state of affairs.

A Reddit user named anning123 asked this question:

> I bought something in new condition, but the package I received was clearly opened and used. The item itself has a sticker with "LPN PM" number, do you know if it means anything?

The Amazon employee named AmazonAssociate09876 answered:

> The LPN PM sticker is a "License Plate Number." They are used by Amazon returns facilities to label returned items so that a new barcode with a track history can be applied. If you ever see that sticker it means the item has been returned via Amazon. This doesn't exactly mean it's been used though as plenty gets returned in brand new condition.
>
> What happened with you though could be multiple things. For example clothes are inspected to see if it is clean, undamaged, and the correct item. The packaging is not considered unless the item won't stay in it in which case it is repackaged in a new bag. We are not required to fold it nor make it look nice again.
>
> If it was basically anything else, then you are one of about 3 million customers every year who got a bad product due to "work place laziness." Amazon requires it's employees to process 44 returns an hour to maintain "acceptable" rate. At my FC they have been lax on this and the average is now 36 an hour. Not maintaining rate will lead to a warning. Do it again is a write up. Three write ups is a termination. Most new hires struggle to hit 44 an hour and at least half lose their jobs due to rate alone. So a lot of associates cheat and never even look inside the packaging (or new hires not answering their UI questions correctly because they don't read the thing) and end up processing items that are clearly damaged as new. Which leads to customers like you getting a bad product.
>
> It's a two sided issue that can be fixed if Amazon bloody stopped putting on the blame on the returns associates and acknowledged their own fault. Just one simple solution is to have the out bound employees call out bad product when they stow it. That said they also have a rate to maintain as well. Maybe having inflexible rates that only ever go up is a bad thing? Or maybe being inflexible to the point that a machine decides if someone loses their job not a human and no one can supersede said machine is problem as well?[3]

I've been selling on Amazon since 2009 as a low volume 3rd party seller. And for many years, sellers and myself, have been requesting Amazon create a button (option) in seller central where we can opt to have all our FBA returns automatically

---

dated on April 24, 2019, at 4:47 p.m. ET, *https://www.buzzfeednews.com/article/leticiamiranda/amazon-marketplace-sellers-black-hat-scams-search-rankings.*

[3] Reddit post: Hello! I am an Amazon Returns associate, AMA!, *https://www.reddit.com/r/IAmA/comments/nv1cg4/hello_i_am_an_amazon_returns_associate_ama/*.

removed from inventory regardless of the condition so we can evaluate them for ourselves to determine if they're in sellable condition. There are many examples of this request in the seller forums.[4, 5, 6] And it would be by far easier on Amazon's employees to not have to judge within 96 seconds (60m/44r = 96s) if a product had been tampered with, opened, used, swapped out with another product, etc. . . . But Amazon has denied us this simple option over and over again. And it would be much easier for Amazon to automatically remove the returns since they already have a process of "removal of returns" and "removal of inventory". And the returns would be easy to track and send back to the original seller because each stickered FBA product has internal bar codes printed on a sticker that's placed on the products which tracks the logistics of individual sellers' products.

Since Amazon was very aware of the problem for years, and after a lot of pressure, to appease us, Amazon finally tried a wonderful pilot program for a limited time called the "FBA Customer Returns Removal Pilot Program". Where sellers give Amazon the ASIN numbers of the products they want to be automatically removed from inventory if they're returned. Amazon would automatically mark them when they're returned as "unsellable" regardless of the condition, which would automatically have them pulled from inventory and returned to the original seller. A perfect super simple solution that worked within their existing system. But then Amazon stopped the pilot program for unknown reasons.[7] They had many opportunities of simple and fantastic solutions like this one to correct the situation, but chose not to. The only problem I see, if Amazon improved the returns processing system by reducing the quotas on their workers to allow them to do a better job, and allowing sellers to automatically pull out all of their returns out of inventory, then Amazon would lose potentially millions to billions of dollars in unnecessary and fraudulent additional fulfillment fees and returns processing fees payable by the victimized unwitting 3rd party sellers.

Here's the math:

This is a screenshot of one of my returns payment summaries from 2016.

Payments Learn more

Statement View | Transaction View | All Statements | Date Range Reports | Advertising Invoice History

Find a transaction: Enter order number GO

Order Id search: 106-8313552-9673842 GO
or Filter the list of all transactions

106-8313552-9673842 Download

Items 1 to 2

Date	Transaction type	Order ID	Product Details	Total product charges	Total promotional rebates	Amazon fees	Other	Total
Dec 30, 2016	Refund	106-8313552-9673842	Sara Monica Flower Hair Clip and Pin Ro...	-$19.95	$0.00	$2.39	$0.00	-$17.56
Dec 27, 2016	Order Payment	106-8313552-9673842	Sara Monica Flower Hair Clip and Pin Ro...	$19.95	$0.00	-$5.87	$0.00	$14.08

Items 1 to 2

Show 10 results per page GO

So basically, if the product is sold and the customer keeps it, then on this product that costs $19.95 Amazon would profit $5.87 in processing and referral fees, and the seller profits $14.08. Keep in mind these fees do not include the amount of money spent in FBA storage fees, shipping fees to the fulfillment centers, or Amazon's advertisement fees for the sale of that product on Amazon's platform.

But if that product is returned in damaged and used condition, Amazon still profits $3.48 in processing fees, but the seller loses the entire price of the product in addition to $3.48 in processing fees ($19.95 + $3.48 = $23.43). And if the product was marked correctly as non-sellable and shipped back to the seller, then the additional removal fee of .50 cents would have made the total a loss of $23.93 ($23.43 + .50¢ = $23.93).

---

[4] Amazon, please make a few FBA changes to help sellers avoid suspensions by ConcernedFbaSeller Posted on: 05 August 2015 5:16 PM, *https://sellercentral.amazon.com/forums/thread.jspa?threadID=264246&start=0&tstart=0&sortBy=date.*

[5] How do I stop returns from getting put back in to inventory? By Schiit Audio Posted on: 02 October 2014 10:38 AM, *https://sellercentral.amazon.com/forums/thread.jspa?threadID=223907&tstart=0.*

[6] How to Identify Returned Item for Purpose of Removal Order, by LucasP, May 9, '15 8:46 AM, *https://sellercentral.amazon.com/forums/t/how-to-identify-returned-item-for-purpose-of-removal-order/49183.*

[7] FBA Customer Returns Removal Pilot Posted byu/frankyford, *https://www.reddit.com/r/FulfillmentByAmazon/comments/ebo25y/fba_customer_returns_removal_pilot/.*

And now, if that same returned product that's used and damaged is put back into inventory to be fraudulently sold as new and unused condition to the 3rd party sellers next buyer, then it pretty much guarantees the buyer will return it based on its poor condition. So, the second time that same products gets processed as a return, Amazon profits a combined total of $6.96, and the seller now loses a combined total of $6.96 plus the entire cost of the product ($19.95 + $6.96 = $26.91).

And you can easily see how the math can quickly add up if the product goes unnoticed by the 3rd party seller, and is in an infinite loop between the returns department and the customers. I assume that eventually the customer would finally receive a new and unused product in good condition, but who knows after how many attempts, and it would be at the expense of the 3rd party seller.

So, if the process was honest and efficient, and the product was removed the first time, then Amazon would profit a total of $5.87. But when it's returned twice and processed twice, Amazon profits in returns processing fees a total of $6.96 ($3.48 + $3.48 = $6.96). The additional profit from the first return and the second return combined is a total of $1.09 ($6.96 − $5.87 = $1.09). So Amazon made an extra $1.09 in the fraudulent reprocessing of a used and damaged return, than if they simply pulled it out of inventory when it was returned the first time.

One dollar and 9 cents doesn't sound like much money, but Amazon has about 200 million PRIME members, and more than 200 million shipments a year. So, say for example, if Amazon only did this once a year with approximately only 10% of their PRIME members, a seemingly overlooked and honest "mistake" that gets refunded. And if Amazon makes an additional profit of $1.09 from the combination of the fees earned on the 1st and 2nd return of the same unit, in this scenario if the originally costs is $19.95, then $20 million x $1.09 = $21,800,000.00, in potential illegal profits per year.

Now imagine if it happened to all of their PRIME members, but only once a year. Imagine if it happened to all of their PRIME members, but several times a year. Keep doing the math, and the motivation to not fix this debilitating situation starts to become more obvious at the expense of the FBA employees who are used as proxies, the 3rd party sellers who Amazon is stealing from, and the customers who are put at risk of potentially receiving a dangerously tampered with product. And at the expense of the shareholders as well since these illegal profits also inflates the value of Amazon, because it's undetectable as to how this extra money was made since it's undetectable as how it should have never happened.

It's also very dangerous for the consumers because many of the non-sellable returns that are placed back into inventory and shipped out again typically have a variety of these issues: no packaging, no product instructions, no warning labels, no users manuals, no warranty papers, no tamper evident security seals, missing parts, used items, soiled items, damaged items, swapped items with different low quality products, originals swapped with counterfeit items, items covered in human hair or pet hair, items covered in body fluids, etc. . . . just simply repackaged in Amazon's plastic bags and barcodes and put back into inventory to be shipped to the next unwitting 3rd party FBA sellers' customers.[8, 9, 10, 11, 12]

This fraudulent activity also damages 3rd party sellers' accounts in "violation reports" which the 3rd party sellers' accounts can get suspended for, since Amazon passes the blame for "Item not as described" and "used items sold as new" complaints onto the unwitting 3rd party FBA sellers who have no idea that Amazon's

---

[8] "Online order of diapers arrives at Jersey City home—but they were already soiled," By Joshua Rosario | *The Jersey Journal,* Updated January 11, 2020; Posted January 10, 2020, *https://www.nj.com/hudson/2020/01/online-order-of-diapers-arrives-at-jersey-city-home-but-they-were-already-soiled.html.*

[9] "Why did Amazon send this man a pair of moldy shoes?", Inside Edition, Duration: 01:43 2/6/2020, *https://www.msn.com/en-us/video/viral/why-did-amazon-send-this-man-a-pair-of-moldy-shoes/vi-BBZJmc9.*

[10] "Amazon Customer Outraged To Find 'Baggie of Drugs' Inside Package Containing Gift For His 8-Year-Old Niece" *Newsweek,* by Khaleda Rahman On 11/24/19 AT 9:26 AM EST, *https://www.newsweek.com/amazon-customer-outraged-drugs-package-1473750.*

[11] "A "new" Amazon waffle maker came with an old crusty-looking waffle already in it"; "Buying from Amazon is still a crap shoot." Vox, By Jason Del Rey@DelRey January 3, 2020, 2:20pm EST, *https://www.vox.com/recode/2020/1/3/21047550/amazon-waffle-maker-babycakes-marketplace-seller.*

[12] "Police investigate after 65 pounds of weed included with Orlando couple's Amazon order," WFTV.com By: Jeff Deal, Updated: October 20, 2017–6:16 PM, *https://www.wftv.com/news/local/police-investigate-after-63-pounds-of-weed-included-with-orlando-couples-amazon-order/627653301/.*

FBA put used returns back into inventory. Typically when an FBA seller's account is suspended, they have to pay Amazon a disposal fee for their inventory if they can't afford to have it all shipped back to them and if they can't afford long term storage fees in FBA. The disposal fee is the cheapest removal option, but at the greatest loss. But "disposal" doesn't necessarily mean Amazon disposes of it, in many cases it's free inventory for Amazon to sell. So if Amazon wants the inventory of a 3rd party FBA seller, there are ways for Amazon to get it for free, and the returns fraud "account violations" could be a means amongst many to that scenario.

And since there is no way to leave company feedback directly for Amazon, then the 3rd party FBA sellers have to take the full blow of the customers' negative reviews and feedback from poor FBA experiences, which is extremely damaging to their businesses' reputation, brands and sales, even though they had no control over the FBA shipments and activities.[13] And the returns fraud also damages the product reviews of private label brands when a customer receives a used/damaged/swapped/counterfeit/knock-off/moldy/soiled returned item they thought was supposed to be the legitimate product in new condition.

"Feedback" reviews are about the companies' services, which is different than the "product reviews". And without visible feedback reviews about Amazon, then Amazon will always look better as it fraudulently deceives the buyers that Amazon is more trustworthy than any other 3rd party seller or any other business in general. This is an unfair business practice since Amazon allows others to judge 3rd party sellers, but no one is allowed to judge Amazon. It's also damaging to other honest businesses outside of Amazon because customers can't compare their reviews to Amazon since Amazon has no reviews about itself. Therefor there are no limitations on how poorly Amazon's services are and how badly they can abuse their entire ecosystem to squeeze, cheat and steal more cash out of its debilitated bodies. And too many 3rd party sellers are too scared to speak up, out of fear of retaliation and loss of their selling privileges.[14]

2—FBA overcharges, non-reimbursements, swapped inventory and phantom inventory.

Another way Amazon unjustly profits from FBA warehouse inefficiencies due to employee stress, and quotas, is that their employees are forced to works so fast that they make many costly mistakes, and then to compensate, out of fear of losing their jobs or pressure from management, they'll cover their tracks by manipulating the inventory data at the expense of the 3rd party sellers, or they won't process the information correctly for reimbursements, or they won't cooperate with sellers for their contractual reimbursements.

When FBA sellers catch mistakes where they didn't receive their due reimbursements for FBA lost and damaged inventory or FBA returns not returned within 45 days,[15] they have to report it within a claim period to get their money back. Sometimes after a great deal of work and documentation from the FBA sellers, Amazon will actually reimburse them, but typically below the fair market value.[16] Other times Amazon will simply refuse to reimburse the claim even if it's within the claim period, by making nonsensical excuses, or changing the facts, or hiding the discrep-

---

[13] Are we really this powerless with new feedback removal team? Kings Fan Goods Posted on: 21 September 2017 8:56 PM, *https://sellercentral.amazon.com/forums/thread.jspa?threadID=367788&tstart=0.* Kings Fan Goods Posted on: 21 September 2017 8:56 PM.

[14] Mas_Des_Bories comment August 14, 2017 6:07 AM post #23, *https://sellercentral.amazon.com/forums/t/what-s-do-i-do-next-amazon-will-not-pay-for-what-they-destroyed/321102/23.*

[15] How do you catch the refunds that need to be reimbursed?, *https://sellercentral.amazon.com/forums/thread.jspa?threadID=206387&tstart=0* Uplifting Deals 25 May, 2014 7:40 AM.

[16] OnlineSeller comment in What's happening with FBA system October 8, 2017 6:04 AM, *https://sellercentral.amazon.com/forums/t/whats-happening-with-fba-system/326179/10.*

ancies by changing the terminology, etc. . . .[17, 18, 19, 20, 21] Other time's Amazon won't reimburse in cash but with a totally different cheaper bogus product, as an exchange.[22, 23] Sometimes claims are denied for no practical reason.

And in many cases Amazon employees will manipulate the inventory status to deny reimbursements, like if its "warehouse damaged" where Amazon would owe a reimbursement, they'll change it to "customer damaged" so Amazon wouldn't be responsible for the reimbursement, even if it's never been shipped to a customer.[24] They'll also delete the entire claim records (Case ID #) and retract and delete e-mails.[25] They've also suspended FBA sellers' accounts for bogus reasons if they try to get Amazon to pay them their due reimbursements too often.[26]

And Amazon will often change the status of a "warehouse damaged" unit to a "sellable" unit to not have to reimburse the FBA seller by swapping dissimilar inventory between sellers and hide their actions by saying in the "Adjustment Reports" the inventory came from a "Holding Account". Typically the dissimilar inventory is of far less value and in inferior condition than the original, or an entirely different product or counterfeit, but Amazon will claim it's the same type of product when it's not. Another use of a "holding account" is to make it look as if it's a totally new product that they held from the seller's inventory, even when there were no other units in the inventory it could have come from, it's phantom inventory to hide the discrepancies so when the data is reconciled, everything looks accounted for.

FBA also regularly overcharges 3rd party sellers in "weight handling fees," "long term storage fees" errors, fulfillment fees, oversize fees, etc.[27, 28, 29, 30, 31, 32]

There have also been widespread issues for FBA inbound shipments, and 3rd party sellers at their wits end sending petitions to Jeff Bezos directly through the seller forums. In a forum titled "Petition to Jeff/Executive Team regarding FBA Issues" Rooster wrote, "1—In the last few months a change was made whereby the Seller

---

[17] Beware Reimbursement Requests Getting Difficult by HonestSeller, Posted on August 2, 2017 11:48 AM, *https://sellercentral.amazon.com/forums/thread.jspa?messageID=4093066#4093066.*

[18] What do I do next? Amazon will not pay for what they destroyed! By TheLeatherman Posted on: 26 July 2017 12:03 AM, *https://sellercentral.amazon.com/forums/t/what-s-do-i-do-next-amazon-will-not-pay-for-what-they-destroyed/321102.*

[19] Is anybody aware of a policy change in handling "stickered" inventory? Funky Monkey Posted on: 16 February 2014 8:10 PM, *https://sellercentral.amazon.com/forums/t/is-anybody-aware-of-a-policy-change-in-handling-stickered-inventory/304119.*

[20] THEY CHANGED THE TERMINOLOGY! Funky Monkey March 20, 2014 2:45 AM, *https://sellercentral.amazon.com/forums/t/is-anybody-aware-of-a-policy-change-in-handling-stickered-inventory/304119/33.*

[21] Results and observations from my experience digging for FBA Reimbursements TiffDMP Posted on: 05 March 2016 12:52 PM, *https://sellercentral.amazon.com/forums/thread.jspa?threadID=293756.*

[22] Amazon no longer reimbursing units not returned in cash! Funky Monkey, Posted on: 28 July 2017 12:31 PM, *https://sellercentral.amazon.com/forums/t/amazon-no-longer-reimbursing-units-not-returned-in-cash/321425.*

[23] Amazon lost entire pallet of inventory, magically found cheaper substitute, by Richard Roberson Posted on: 20 November 2017 10:34 AM, *https://sellercentral.amazon.com/forums/t/amazon-lost-entire-pallet-of-inventory-magically-found-cheaper-substitute/336057.*

[24] Customer Damage when No Inventory was Returned, *https://sellercentral.amazon.com/forums/t/customer-damage-when-no-inventory-was-returned/349577.*

[25] FunkyMonkey's reply to TheLeathrman, *https://sellercentral.amazon.com/forums/t/what-s-do-i-do-next-amazon-will-not-pay-for-what-they-destroyed/321102/7.* TheLeatherman Posted post #7 July 28, 2017 12:19 AM.

[26] *https://sellercentral.amazon.com/forums/t/what-s-do-i-do-next-amazon-will-not-pay-for-what-they-destroyed/321102/26.* TheLeatherman post #26, August 15, 2017, 1:45 PM.

[27] FBA fulfillment is 131.74 for a 11.95 item, Real chance Posted on: 18 November 2017 6:50 PM, *https://sellercentral.amazon.com/forums/thread.jspa?threadID=376081&tstart=30.*

[28] Yet another reimbursement type . . . FBA storage fees for non-existent ASINs by Water_Enthusiast (formerly iSnorkel) Posted on: 14 March 2017 7:46 AM, *https://sellercentral.amazon.com/forums/t/yet-another-reimbursement-type-fba-storage-fees-for-non-existent-asins/284554.*

[29] FBA LONG TERM STORAGE FEE ERRORS!?!?!? WATCH OUT! Bee_Blessed Posted on: August 18, 2016 4:54 PM, *https://sellercentral.amazon.com/forums/t/fba-long-term-storage-fee-errors-watch-out/182971.*

[30] Been overcharged FBA fees for thousands of orders and amazon won't reimburse by SnoRainier Posted on: 26 April 2017 10:58 PM, *https://sellercentral.amazon.com/forums/t/been-overcharged-fba-fees-for-thousands-of-orders-and-amazon-wont-reimburse/302279.*

[31] Why is Amazon stealing from the little guys? By just_a_li April 18, 2017, 1:01 PM, *https://sellercentral.amazon.com/forums/t/why-is-amazon-stealing-from-the-little-guys/298524.*

[32] Anyone else being overcharged for FBA fees? By Florida_Man, *https://sellercentral.amazon.com/forums/t/anyone-else-being-overcharged-for-fba-fees/278036.*

was blamed for issues caused by the FBA warehouses—without recourse." "2—There is an auto-reconcile feature that seems to be in place which is causing widespread issues by not allowing a shipment to be researched for items lost by the warehouses—or not being counted correctly in receiving." "3—Complete and correct shipments are being counted in as short and then designated with a "Problem" designation requiring Sellers to Acknowledge that we caused the problem and thus taking a hit to our Inbound Metrics as well as losing the value of the items lost." Other sellers in the forum joined in and added their own lists of grievances over other disservices.[33]

These fraudulent practices are damaging to the sellers' businesses, sales, finances, brands, product reviews, feedback, and reputation. And of course absolutely devastating to their mental health as they watch in horror and agony as all their investments, hard work and dreams get stolen from them, and the fear of how they'll financially survive and provide for their families is unimaginable; millions of 3rd party sellers have been living through this every day for years. And of course sellers getting blamed for FBA issues out of the sellers' control creating "account violations" which suspends the sellers' accounts are even worse, aside from destroying the sellers' entire businesses, the sellers are unable to access their sellers' accounts to recover their reimbursements, and they'll have very few chances of ever recovering their money. Sometimes the sellers' only chances of reimbursements are if they go public with their story in Amazon's Seller Forums, if they get lucky a forum monitor will chime in and resolve the problem to save face on a now public issue. It's difficult for sellers to get the attention of the media, because reporters simply can't grasp the intricate details of online retail and have a hard time understanding the issues. It's the same problem with government agencies.

These fraudulent practices also defraud the buyers who believed they were getting a product in new and unused condition and/or believed they were getting the product they ordered, and not a product that FBA swapped out with something else to avoid reimbursing their FBA 3rd party sellers.

Any contractual reimbursements that are denied and not paid back fully are boundless profits for Amazon. It's a win-win situation for Amazon's financial advantage into the millions to billions of dollars, but it's all stolen money from the 3rd party sellers.

For example, in Amazon's Seller Forums where the FBA sellers try to keep everyone aware of FBA's latest inventory manipulations, a FBA seller named Water Enthusiast (formerly known as iSnorkel) Posted a warning to FBA sellers on: 17 September 2016 1:34 PM in a thread titled, "New type of FBA reimbursement to request: Missing Unfulfillable Units",

"We open cases for reimbursements that should have been issued automatically, but aren't, to the tune of over $15,000 a year (plus some lost units replaced to our inventory). Most cases are eventually successful."

. . . "Recently I've stumbled on yet another category of units that require reimbursement requests—missing unfulfillable units. In my experience, NONE of these types of missing units have been "auto-reimbursed" so opening a case is the only way to get what is due when Amazon misplaces unfulfillable units."

"When a customer returns an item with opened packaging, whether the item is damaged or not, Amazon puts it back into our FBA inventory as an unfulfillable unit. So far so good, system works as expected (we have the "repackaging of returns" option off). We have the account setting enabled to automatically return to us all unfulfillable units every 2 weeks. So you would expect that these unfulfillable units would make it back to us within a few weeks so we can inspect and repackage or otherwise deal with it at our facility."

"However I have found 60+ instances in the last several months where the unfulfillable unit apparently DISAPPEARED—it never came back to us, it does not remain as an unfulfillable unit in our FBA inventory, it has not been reimbursed in $ or in units, and I see no evidence of it being converted to a fulfillable unit and being added to FBA inventory that way."

"Multiple cases opened so far (with 5 units per case), half of the cases have successfully earned reimbursement for the missing units so far, with the rest of the cases still open. Several cases required multiple contacts to resolve, especially when there

[33] Petition to Jeff/Executive Team regarding FBA Issues. By Rooster, Posted on: August 11, 2017 2:28 PM, *https://sellercentral.amazon.com/forums/thread.jspa?threadID=362363.*

were multiple orders/returns for units of the same SKU, some of which were actually returned to us and some of which were not."

. . . (Side note—we've found our cases have been resolved quicker and more favorably since we've taken to answering every emailed survey "Were you satisfied with the support provided?" to reward reps who resolve in our favor (5 star), and to give appropriate feedback (1 to 2 star) to reps who give the runaround or make errors. I believe that the reps can look at the feedback we give to other reps, much as eBay members can view the "feedback left for others" in a buyer's feedback, and that this may influence how they treat our cases. Especially the prospect of earning 5 stars. YMMV.)

. . . And then in a reply to her post another seller named Chief Robot posted on 29 December 2016 2:17 AM and said, "Yes, we find these from time to time. Just found a few "reserved" inventory that were lost or should have been reimbursed. Status changed from unfulfillable to reserved. Then stays in reserved forever. Best is when it belongs to an old listing that no longer has a catalogue page and is archived, you never see it when quickly scanning trough gui page. New SS excuse, reserved unit is a fantom [Phantom] unit that was created to solve an error in the past."[34]

In the case of this seller Water Enthusiast, she carefully monitors her FBA inventory so her losses are minimum, but at the expense of her labor which is costly. This is labor Amazon FBA is getting paid to do through sellers' FBA fees, but FBA does the job so poorly that it takes sellers valuable additional time to correct FBA's costly errors. In many cases it costs more to pay an additional employee to keep track of FBA to prevent the non-reimbursement loses, than they would recover from non-reimbursements. So it's simply cheaper to succumb to victimization of Amazon stealing from them. Most sellers don't have the time, resources or knowledge to stay on top of it, or they're not aware of the non-payments because they assume Amazon's FBA is doing the job they're paying them to do. So they lose everything to Amazon.

So let's do the hypothetical math on this, say there were 100,000 FBA sellers selling at her sales volume that assumed Amazon was honestly and efficiently reconciling the inventory and payments, and weren't aware of the losses or unable to be reimbursed, then 100,000 × $15,000.00 = $1,500,000,000.00 a year of potential profits which Amazon could keep without detection or consequence. And that doesn't include the sellers that have higher or lower sales volume than her.

These profit should look like a negative on Amazon's balance sheets, but shows up as a positive. And are undetectable as how they were gained because it's undetectable as how they should have been lost. Perhaps somewhere in Amazon's fluctuating policy something is written about claim periods. But nowhere in the policy does it say FBA sellers are responsible for keeping track of FBA payments and reimbursements to make sure FBA pays them according to policy otherwise FBA is not liable for reimbursements. FBA is supposed to keep track of the inventory as a part of the contractual agreement of their services and pay reimbursements accordingly without margins of error.

No new Amazon FBA warehouse should be allowed to be built in the USA until a thorough external audit and investigation is done of all FBA business practices since the first day Amazon started FBA, for both the employees and the 3rd party sellers. Investigations need to be done into the abuse and exploitation of their employees who are also being used as proxies for theft; against their will. The "Adjustment Reports," "Reserved Units," "Holding Accounts" and "Inbound Shipments" need to be thoroughly investigated and reconciled. Non-reimbursements, non-payments, overcharges that's owed to the 3rd party sellers need to be investigated, reconciled and reimbursed. A reconciliation of all inventory needs to be done to find all the discrepancies over the years, so the full value of the lost, damaged and non-returned items can be fully accounted for and reimbursed to the 3rd party sellers. Additional fraudulent fees from processing the same returns over and over again into an infinite loop must be reimbursed. Overcharges from weight handling fees and long term storage fees errors must be reimbursed. And considering that the 3rd party sellers are illegally forced and racketeered into FBA via PRIME, since FBA is illegally tied to PRIME and the ranking visibility on the platform, then 3rd party sellers should also be reimbursed all their fulfillment fees as restitutions from being

[34] "New type of FBA reimbursement to request: Missing Unfulfillable Units," by Water Enthusiast (formerly known as iSnorkel) Posted on: 17 September 2016 1:34 PM, *https://sellercentral.amazon.com/forums/t/new-type-of-fba-reimbursement-to-request-missing-unfulfillable-units/198156.*

illegally racketeered into FBA. (I can further elaborate about racketeering via protection racket upon request). And an SEC investigation needs to be done on the additional money FBA stole from its 3rd party sellers but then reported as profits, when in fact it was stolen money. FBA & SFP needs to be untied from PRIME as the sole qualifications, so other fulfillment service companies can qualify a product for PRIME, or any other perks made available on the platform. And going forward, Amazon's FBA should be closely monitored and audited by external agencies. These agencies should do reviews and audits of the monitoring of inventory status, and making sure the reimbursements and inventory are reconciled. And Jeff Bezos's influence, and the resulting employees' fears and pressures to abide to his selfish and unethical commands in this massive fraud needs to be investigated.

3—Fast paced counterfeits screening forces counterfeits to slip through the cracks; and Amazon financially benefits.

Amazon gives the impression that they've invested heavily in stopping counterfeits on their platforms and within FBA. But the working pace is set up for failure and inefficiencies, just like the previous examples. And Amazon profits bountifully from the counterfeits that are forced to slip through the cracks.

Wade Shepard, an investigative reporter did such a thorough job explaining how this happens, that there's not much more I need to add to his reporting to explain this. So here are some quotes from his article "How Chinese Counterfeiters Continue Beating Amazon" by Wade Shepard, January 12, 2017:[35]

> Amazon's counterfeit problem grew exponentially when the marketplace began to aggressively target Chinese sellers in 2015. To help cut out the import/export middlemen and allow Chinese manufacturers and merchants to sell directly to buyers in the USA, Canada, and Europe, Amazon streamlined the shipping process by doing things like registering with the Federal Maritime Commission to provide ocean freight, which allowed for Chinese merchants to ship entire containers directly to Amazon's fulfillment warehouses.
>
> "Amazon wanted all those Chinese sellers in the U.S. They actively invited them to sell," explained Chris McCabe, an Amazon Seller consultant from ecommerce Chris and a former Amazonian who once worked in the company's merchant account investigation division.
>
> Once these bulkheads were removed, China-based merchants began pouring into the marketplace, doubling their presence in 2015 alone, and making Amazon the cross-border ecommerce choice for Chinese sellers. That same year, Amazon moved past Walmart as the most valuable retailer in the USA, Jeff Bezos moved up to number five on Forbes's wealthiest person list, and profits soared by 20%.
>
> . . . over 60% of the world's knockoffs originate from China—a big chunk of an industry worth half a trillion dollars per year.
>
> "Did we see a rise in counterfeits being sold on Amazon after the marketplace became popular with Chinese merchants?" I asked Julie Zerbo.
>
> "We absolutely did," she replied. "Sure, counterfeits were present on the site prior to Amazon's push for a greater presence of Chinese sellers, but the influx of fakes since then has been enormous."
>
> It is unreasonable to assume that Amazon expected anything different, as China's prevalence for counterfeit production was well know prior to their big China push. According to China's state-run Xinhua news agency, 40% of the country's domestic online marketplaces were made up of counterfeit goods in 2015, the same year that Amazon bridged the ecommerce hemispheres.
>
> Amazon claims to be doing whatever they can to inhibit counterfeits in their marketplace . . .
>
> But when fake items on Amazon are about as easy to find as authentic ones, I have to wonder what these anti-counterfeit measures actually consist of—and why they don't seem to be working effectively.

[35] How Chinese Counterfeiters Continue Beating Amazon, by Wade Shepard, January 12, 2017, *https://www.forbes.com/sites/wadeshepard/2017/01/12/why-amazon-is-losing-its-battle-against-chinese-counterfeiters/#7a75e68c585c.*

> Michael Jakubek, who worked on Amazon's fraud and abuse prevention teams between 2004 and 2012 . . . [said] "The big problem with this is that the investigators get rewarded based on how quickly they go," Jakubek said. "There's no reason they can't identify that these sellers are bad, but they're compensated to go so quickly that they typically just do really cursory reviews."
>
> Chris McCabe, who investigated merchant violations for Amazon for 5 years, elaborated: "You need people, properly trained people with the right kind of SOPs in their hands or in their heads, and that's where a lot of the failures come in. I mean, they are being pressured to review work very quickly. They have this IPH (investigations per hour) which always slowly inches up . . . If you know you have a certain number of investigations to do during an hour and you've done two that were incredibly complex and you have to do ten more in the rest of the hour, but those two took you half an hour or 20 minutes, it means you have to blow through the rest of them to catch up."
>
> . . . Amazon employees are not only pressured to work extremely rapidly—often sacrificing quality for quantity—but many positions are perpetually filled by those who are new on the job.
>
> "The highly skilled, experienced, trained people that I used to work with are gone," McCabe explained. "They need better training. They need more auditing of investigations, because it's clear that all the wheels have come off the cart when it comes to the quality of the work that goes into an investigation of an appeal, a review of an account."
>
> To put it simply, Amazon's high-pressure, high-turnover, metrics-driven work environment seems to result in torrents of seemingly mindless mistakes, oversights, and copy and paste responses. While Amazonians are encouraged to tear apart each other's ideas, be available to respond to emails 24/7, and treat their job like a lifestyle, scammers and counterfeiters are running amok, selling knockoffs on their marketplace with near impunity—even when caught they just open up a new account under a new name and hope to fall through the cracks of Amazon's porous HR strategy once again."

It's a clear pattern of behavior. So, since 2019, Amazon had employed approximately ten thousand additional employees to fight frauds and counterfeits. But they let it get so out of control for so long, that now they can't even stop it. So now tax payers are responsible to pay for it through the additional work of law enforcement, like the DOJ and FBI. "Amazon's hiring of former federal law enforcement agents seems like a strategy to avoid liability without seriously addressing the fundamental problems with its marketplace," Schakowsky said in an interview for an article by Emily Birnbaum and Daniel Lippman, "How one of America's largest employers leans on federal law enforcement"[36]

Conclusion

There's only so much money to squeeze out honestly and fairly, eventually when the sources runs dry, the only way left to attain it is to steal it or cheat it out. Just like Amazon did with the 61.7 million of stolen Flex driver tips. And lawmakers should be very wary that all those shiny objects that Amazon dangles in front of them to coax favoritism and to change laws in their favor is riddled with that stolen money.

○

[36] How one of America's largest employers leans on federal law enforcement, by Emily Birnbaum and Daniel Lippman, Tuesday, December 21, 2021, 4:30 AM, *https://news.yahoo.com/amazon-cultivates-close-ties-federal-093010630.html.*