ECONOMIC DANGER ZONE: HOW AMERICA COMPETES TO WIN THE FUTURE VERSUS CHINA

HEARING

BEFORE THE

SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE

OF THE

COMMITTEE ON ENERGY AND COMMERCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

FEBRUARY 1, 2023

Serial No. 118–3

Published for the use of the Committee on Energy and Commerce

govinfo.gov/committee/house-energy
energycommerce.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

51–706 PDF WASHINGTON : 2023

COMMITTEE ON ENERGY AND COMMERCE

CATHY MCMORRIS RODGERS, Washington
Chair

MICHAEL C. BURGESS, Texas
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
H. MORGAN GRIFFITH, Virginia
GUS M. BILIRAKIS, Florida
BILL JOHNSON, Ohio
LARRY BUCSHON, Indiana
RICHARD HUDSON, North Carolina
TIM WALBERG, Michigan
EARL L. "BUDDY" CARTER, Georgia
JEFF DUNCAN, South Carolina
GARY J. PALMER, Alabama
NEAL P. DUNN, Florida
JOHN R. CURTIS, Utah
DEBBBIE LESKO, Arizona
GREG PENCE, Indiana
DAN CRENSHAW, Texas
JOHN JOYCE, Pennsylvania
KELLY ARMSTRONG, North Dakota, *Vice Chair*
RANDY K. WEBER, SR., TEXAS
RICK W. ALLEN, Georgia
TROY BALDERSON, Ohio
RUSS FULCHER, Idaho
AUGUST PFLUGER, Texas
DIANA HARSHBARGER, Tennessee
MARIANNETTE MILLER–MEEKS, Iowa
KAT CAMMACK, Florida
JAY OBERNOLTE, California

FRANK PALLONE, JR., New Jersey
Ranking Member
ANNA G. ESHOO, California
DIANA DEGETTE, Colorado
JAN SCHAKOWSKY, Illinois
DORIS O. MATSUI, California
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
PAUL TONKO, New York
YVETTE D. CLARKE, New York
TONY CÁRDENAS, California
RAUL RUIZ, California
SCOTT H. PETERS, California
DEBBIE DINGELL, Michigan
MARC A. VEASEY, Texas
ANN M. KUSTER, New Hampshire
ROBIN L. KELLY, Illinois
NANETTE DIAZ BARRAGÁN, California
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
ANGIE CRAIG, Minnesota
KIM SCHRIER, Washington
LORI TRAHAN, Massachusetts
LIZZIE FLETCHER, Texas

PROFESSIONAL STAFF

NATE HODSON, *Staff Director*
SARAH BURKE, *Deputy Staff Director*
TIFFANY GUARASCIO, *Minority Staff Director*

SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE

GUS M. BILIRAKIS, Florida
Chairman

LARRY BUCSHON, Indiana
TIM WALBERG, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
NEAL P. DUNN, Florida
DEBBIE LESKO, Arizona
GREG PENCE, Indiana
KELLY ARMSTRONG, North Dakota
RICK W. ALLEN, Georgia
RUSS FULCHER, Idaho
DIANA HARSHBARGER, Tennessee
KAT CAMMACK, Florida
CATHY MCMORRIS RODGERS, Washington
(ex officio)

JAN SCHAKOWSKY, Illinois
Ranking Member
KATHY CASTOR, Florida
DEBBIE DINGELL, Michigan
ROBIN L. KELLY, Illinois
LISA BLUNT ROCHESTER, Delaware
DARREN SOTO, Florida
LORI TRAHAN, Massachusetts
YVETTE D. CLARKE, New York
FRANK PALLONE, JR., New Jersey *(ex officio)*

C O N T E N T S

[1]The report has been retained in committee files and is available at https://docs.house.gov/meetings/IF/IF17/20230201/115346/HHRG-118-IF17-20230201-SD008.pdf.

---

[2] The report has been retained in committee files and is available at https://docs.house.gov/meetings/IF/IF17/20230201/115346/HHRG-118-IF17-20230201-SD024.pdf.

ECONOMIC DANGER ZONE: HOW AMERICA COMPETES TO WIN THE FUTURE VERSUS CHINA

WEDNESDAY, FEBRUARY 1, 2023

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The subcommittee met, pursuant to call, at 10:32 a.m. in 2322 of the Rayburn House Office Building, Hon. Gus M. Bilirakis (chairman of the subcommittee), presiding.

Members present: Representatives Bilirakis, Bucshon, Walberg, Duncan, Dunn, Lesko, Armstrong, Allen, Harshbarger, Cammack, Rodgers (ex officio), Schakowsky (subcommittee ranking member), Castor, Dingell, Kelly, Blunt Rochester, Soto, Trahan, Clarke, and Pallone (ex officio).

Staff present: Michael Cameron, Professional Staff Member, Innovation, Data, and Commerce; Jack Heretik, Press Secretary; Jessica Herron, Clerk, Innovation, Data, and Commerce; Peter Kielty, General Counsel; Emily King, Member Services Director; Tim Kurth, Chief Counsel, Innovation, Data, and Commerce; Brannon Rains, Professional Staff Member, Innovation, Data, and Commerce; Lacey Strahm, Fellow, Innovation, Data, and Commerce; Teddy Tanzer, Senior Counsel, Innovation, Data, and Commerce; Hannah Anton, Minority Staff Assistant; Ian Barlow, Minority FTC Detailee; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Daniel Greene, Minority Professional Staff Member; Tiffany Guarascio, Minority Staff Director; Lisa Hone, Minority Chief Counsel, Innovation, Data, and Commerce; Joe Orlando, Minority Senior Policy Analyst; and C.J. Young, Minority Deputy Communications Director.

MR. BILIRAKIS. The Subcommittee on Innovation, Data, and Commerce will come to order.

The Chair recognizes himself for 5 minutes for an opening statement.

OPENING STATEMENT OF HON. GUS M. BILIRAKIS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Good morning, everyone. It is great to be here. Welcome to the first hearing for the Innovation, Data, and Commerce Subcommittee for the 118th Congress. I would like to thank the chair of the full committee for selecting me to chair this important panel, and I would also like to congratulate, again, Cathy McMorris Rod-

gers for being the first woman to serve as the chair of the powerful Committee on Energy and Commerce, the best committee in Congress. It really is. There is no question.

OK. I also want to identify our new members, our new Republican members of the subcommittee: Mr. Allen from the State of Georgia; Mr. Fulcher from Idaho; Ms. Harshbarger from the State of Tennessee; and then, of course, Mr. Duncan.

And I am glad to see you are back on the subcommittee from the great State of South Carolina.

And then we also have, of course, the great friend of mine, Kat Cammack, from the great State of Florida, and she represents Gator Nation.

Finally, I want to thank my esteemed colleague, Tim Walberg from the great State of Michigan, for serving as vice chair of the committee. I am greatly looking forward to working with Mr. Walberg, and I appreciate his partnership. We are going to do great things in this committee.

So Ranking Member Schakowsky, who did an outstanding job as the chair in the previous Congress, I am glad to see you are leading the subcommittee again.

And for our friends across the aisle, we worked very hard together last Congress moving forward very good success, great initiatives that went to the President's desk. This included legislative wins like the INFORM Consumers Act, which will protect consumers from stolen and counterfeit goods online, including those coming from China, and my bill, the Ransomware Act, which requires the FTC to submit recommendations on how to make America more resilient from ransomware and cyber attacks, specifically from cross-border foreign threats like China and Russia.

Switching gears, today's hearing focuses on the great threat to our country right now: China. So it is fitting that to begin the 118th Congress we focus on this threat and discuss how to recapture and maintain our global leadership.

The CCP will stop at nothing to undermine our global leadership and weaken our economy. They bought up our farmlands, stole our intellectual property, and embedded themselves deep within many of our supply chains. Now they are turning their attention towards establishing the global standards for emerging technologies. We are not going to let it happen.

The CCP has invested heavily in artificial intelligence and other emerging technologies. Paired with this investment, China is creating favorable environments for their private-sector companies and entrepreneurs to deploy and test these technologies. This has forced many American companies with global footprint and American innovators with cutting-edge ideas to consider a hard decision: whether to move their operations from American to Chinese shores.

It is also allowing Chinese companies to invest and expand further, potentially endangering our own infrastructure and data security. Waiting any further on a national framework is weakening our stance by the day, and time is of the essence. I can't emphasize that enough: Time is of the essence.

It is imperative that this committee establishes foundational frameworks for developing emerging technologies. We came close last Congress when we passed the bipartisan, bicameral American

Data Privacy and Protection Act. But this Congress we need to ensure it gets across the finish line, because China is not waiting on us to influence international norms and standards.

And I want to commend the previous chairman, Mr. Pallone, and the previous ranking member, Mrs. Rodgers, for getting it through committee, which was really incredible, historic. Now we have got to get it across the finish line as soon as possible.

I look forward to working again with Chair Rodgers, Ranking Members Schakowsky and Pallone, and the members of this committee to finish what we started. We need to get this done, and it is a priority. It is a priority for the American people. We must ensure our Nation remains a leader in global technology standards.

The American people are the most innovative in the world. I know you know this. It is our job in Congress to ensure that we eliminate bureaucratic red tape that has too often hampered innovation in the marketplace. For something like autonomous vehicles that will help senior citizens and Americans living with disabilities, it means reducing barriers to testing and setting the standards for how they will be adopted across the world and provide certainty for businesses and consumers.

America's global leadership depends on its people to be the best in class, and we must give them the regulatory certainty—remember, that is the key—on emerging technologies they need in order to live up to their legacy. If we fail, America will be left behind and our competitors, like China, will leave us in the dust.

Again, we are not going to let that happen.

I am eager to hear from our panel of experts today on such a critical topic. Thank you again to the witnesses for being here today.

[The prepared statement of Mr. Bilirakis follows:]

Opening Statement for Chairman Gus Bilirakis

Subcommittee on Innovation, Data, and Commerce

Hearing entitled, "Economic Danger Zone: How America Competes to Win the Future Versus China"

February 1st, 2023

Good morning, everyone, and welcome to the first hearing for the Innovation, Data, and Commerce subcommittee for the 118th Congress.

I'd like to thank the Chair of the Full Committee for selecting me to Chair this important panel and I would also like to congratulate Cathy McMorris Rodgers for being the first woman to serve as the Chair of the powerful Committee on Energy and Commerce the oldest standing legislative committee in the House – and the best too I'll add.

I also want to identify our new Republican Members of the Subcommittee. Mr. Allen from Georgia, Mr. Fulcher from Idaho, Miss Harshbarger from Tennessee, Miss Cammack from the greatest state of all, Florida, and Mr. Duncan from South Carolina. I'm glad to see you have made your way back to this Subcommittee.

Finally I want to thank my esteemed colleague, Tim Walberg from the great state of Michigan, for serving as Vice Chair of this Committee. I'm greatly looking forward to working with Mr. Walberg and appreciate his partnership.

Ranking Member Schakowsky, I'm glad to see you leading this Subcommittee for our friends across the aisle. We worked very well together last Congress, moving important initiatives to the President's desk. This included legislative wins like the INFORM Consumers Act, which will protect consumers from stolen and counterfeit goods online – including those coming from China, and my bill the RANSOMWARE Act, which requires the FTC to submit recommendations on how to make America more resilient from ransomware and cyber-attacks specifically from cross-border foreign threats like China and Russia.

Switching gears, today's hearing focuses on the greatest threat to our country right now – China. So, it is fitting that to begin the 118th Congress we focus on this threat and discuss how to recapture and maintain our global leadership.

The CCP will stop at nothing to undermine our global leadership and weaken our economy. They have bought up our farmlands, stolen our intellectual property, and embedded themselves deep within many of our supply chains. Now they are turning their attention towards establishing the global standards for emerging technologies.

The CCP has invested heavily in Artificial Intelligence and other emerging technologies. Paired with this investment, China is creating favorable environments for their private sector companies and entrepreneurs to deploy and test these technologies.

This has forced many American companies with a global footprint and American entrepreneurs with cutting-edge ideas to consider a hard decision: whether to move their operations from American to Chinese shores. It's also allowing Chinese companies to invest and expand further, potentially endangering our own infrastructure and data security. Waiting any further on a national framework is weakening our stance by the day – time is of the essence.

It is imperative that this committee establishes foundational frameworks for deploying emerging technologies. We came close last Congress when we passed the bipartisan and bicameral American Data Privacy and Protection Act, but this Congress we need to ensure it gets across the finish line because China is not waiting on us to influence international norms and standards.

I look forward to working with Chair Rodgers, Ranking Members Schakowsky and Pallone, and the members of this Committee to finish what we started. We need to get this done for the American people and ensure our nation remains a leader in global technology standards.

The American people are the most innovative in the world. It is our job in Congress to ensure that we eliminate bureaucratic red tape that has too often hampered innovation in the marketplace.

For something like Autonomous Vehicles, that will help Senior Citizens and Americans living with disabilities, it means reducing barriers to testing, and setting the standards for how they will be adopted across the world, and provide certainty for businesses and consumers.

America's global leadership depends on its people to be best in class, and we must give them the regulatory certainty on emerging technologies they need in order to live up to their legacy. If we fail, America will be left behind and our competitors like China will leave us in the dust.

I am eager to hear from our panel of experts today on such a critical topic. Thank you to our witnesses for being here and I yield back.

Mr. BILIRAKIS. And I yield back. The Chair recognizes subcommittee Ranking Member Schakowsky for 5 minutes for an opening statement.

OPENING STATEMENT OF HON. JAN SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. Thank you so much, Chairman Bilirakis. I am so excited to be back here on this—in the subcommittee, working with you and working with our new members and working with our returning members on both sides of the aisle.

You know, we were so successful passing bipartisan legislation in the last Congress. There was hardly any difference between us. And so I really look forward to continuing to do this.

And I did want to mention—you talked a bit about the challenge of competitiveness with China. And I want to congratulate you on maintaining our jurisdiction. There is a new special committee dealing with China. So thank you for making sure that this idea of our competitiveness and our ability to compete in a positive way with all of our competitors and certainly adversaries—so good work in making that happen.

But I did also want to mention some of the things that we did. You mentioned a couple of these bills, but I want to say that we were able to pass out of the full committee the consumer protection and the—our legislation on—the privacy legislation that we were able to get out of the House, the American Data Privacy and Protection Act. And I am hoping and looking forward to as a priority to try and move that. Americans want to do that.

We passed the Consumer Protection and the Recovery Act. We also passed out of the—into law Reese's Law, protecting children; the INFORM Consumer Act, which is not only good for consumers but for businesses that have been losing money; the STURDY Act, protecting children from furniture that falls over on them; the Ransomware Act; and the Restoring Brand USA. These were two of your bills that I was happy to cosponsor. The Manufacturing.gov Act, Safety Sleep for Babies, the FTC Collaboration—is that right—Act of 2022; the Carbon Monoxide Poisoning Prevention Act. I mean, so many things for consumers, for ordinary people that we were able to pass into law.

But I definitely do want to say that let's make a priority of passing our privacy bill. I think this will really put us on the right track.

And let me also say there is—we know that there is a lot of work to be done to make our supply chain resilient, and we need to work on that. Also—and we face these new challenges with the growth of our artificial intelligence that we need to address.

And let me just say in closing now is the time for us to come together. We can do this. We have done this. And I really look forward to the advances that we are going to make for consumers, for business, and for the economy of our country.

[The prepared statement of Ms. Schakowsky follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Subcommittee on Innovation, Data, and Commerce Ranking Member Jan Schakowsky

Hearing on "Economic Danger Zone: How America Competes to Win the Future Versus China"

February 1, 2023

Thank you, Chair Bilirakis, I'm glad you are holding this hearing today. Commerce, investment in America, and putting consumers first are how we compete with China and countries around the world. Last Congress, we delivered transformative investments in American competitiveness:

- Our "INFORM Consumers Act" with Chair Bilirakis stops foreign-based bad actors from harming consumers and undercutting legitimate U.S. businesses by selling counterfeit or stolen products.
- The "CHIPS and Science Act" invests $53 billion in American semiconductor manufacturing and research.
- The bipartisan "Infrastructure Investment and Jobs Act" invests in our bridges, roads, transit, broadband access, clean drinking water, and more.
- The "Inflation Reduction Act" reduces healthcare costs, promotes renewable and low-cost energy, and decreases the deficit.

All of this puts the U.S. on the path to sustained economic growth, secure supply chains, and the ability to compete globally. But our work is not done. We must build on these successes to ensure American competitiveness in emerging technologies:

- First and foremost, I look forward to continuing to work with my colleagues across the aisle to protect Americans' data privacy.
- Last Congress we passed the "American Data Privacy and Protection Act" out of the full committee by an overwhelming 53-2 vote.
- There is work left to do to make our supply chains resilient to shocks like the pandemic.
- And we face new challenges with the growth of artificial intelligence and its more transformative applications like autonomous vehicles.

Now is the time to come together to continue investing in America. Our nation's competitive edge is at risk if we pull back on our investments with draconian spending cuts. I look forward to continuing our important work together this Congress.

Ms. SCHAKOWSKY. I yield back.

Mr. BILIRAKIS. I thank the ranking member. The Chair recognizes the chair of the full committee, Mrs. Rodgers, for 5 minutes for her opening statement.

OPENING STATEMENT OF HON. CATHY MCMORRIS RODGERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WASHINGTON

Mrs. RODGERS. Thank you, Mr. Chairman. Welcome, everyone, to the first hearing of the Innovation, Data, and Commerce Subcommittee of the 118th Congress. It is great to have everyone here, and I would like to congratulate my good friend Congressman Gus Bilirakis on becoming the chairman of this subcommittee, as well as my friend Mr. Walberg for being the vice chair of the committee.

This committee plays a vital role in advancing American competitiveness and global technological leadership, and it is critical that we use this panel to ensure that America, not China, is setting the rules of the road for technologies of tomorrow.

It is no secret that the Chinese Communist Party wants to replace the United States as a global economic and technological power. Whether it is artificial intelligence, self-driving cars, or smart devices, China wants to dominate these new and emerging technologies.

But China's vision of the future is not one that welcomes American values, values like freedom of speech, privacy, entrepreneurial enterprise, individual rights, or the rule of law. The Chinese Communist Party, on the other hand, spies on its citizens and asserts strict government control over businesses and the economy. We need to make sure that these technologies of the future are developed in an ecosystem that promotes American values, not China's. And this is a race that we cannot afford to let them win.

We must work together to cement America's global technological leadership. We should start by passing comprehensive privacy and data security protections with one national standard. We made history last year when we passed the bipartisan, bicameral American Data Privacy and Protection Act 53 to 2 out of this committee, full committee. But our work isn't over yet, and we have already fallen behind other countries in establishing a national privacy standard.

I want to thank Mr. Pallone and Ms. Schakowsky and, of course, Mr. Bilirakis for his leadership on this. And I am eager to continue that work. It is a top priority for Americans, and it needs to be achieved this Congress. And we can't stop there.

It is also important that we take action to ensure the development and the deployment of self-driving cars. The regulatory framework for self-driving cars must be led in the United States.

And again, this comes down to our values versus the Chinese Communist Party. America values, the importance of safety for our citizens. China does not. We value our workforce and free market economies. China does not. We value civil society groups and their right to speak freely. China does not.

To win the future, the United States must lead on self-driving cars. We must chart a path so the road is one we design. And this can be the year we finally push past the barriers which have de-

railed the SELF DRIVE Act and other legislation from becoming law.

And we can also build on the America COMPETES Act legislation, which I had sponsored in the 116th Congress and worked with then-Chair Ms. Schakowsky to get passed, and it was on promoting emerging technologies, which is—was enacted with many provisions of—led by members of this committee.

The best way to beat China is to spur innovation and remove unnecessary, burdensome regulatory barriers. We cannot and we should not even try to beat China at their game of massive government handouts and centralized industrial policy. We won't outspend them, and authorizing billions of taxpayer dollars without removing burdensome red tape will only lead to waste.

Instead, we need to encourage innovation, ingenuity, and entrepreneurship. That is the backbone of our economy, and that can only be achieved with a government that encourages low barriers to entry for innovative technologies and startups, and the adoption of emerging technologies that will improve people's lives.

Ensuring Federal agencies don't put undue burden on businesses and innovators will be a top priority for this Congress. Whether it is ensuring people's online information is secure, charting an achievable path towards the development and the deployment of self-driving cars in the United States, or setting the global standards for AI and other emerging technologies, this subcommittee is at the center of it.

You know, the American ingenuity built its first car. America built its first car in 1893. And then we went on to dominate manufacturing the car for over 100 years. And we must secure and win the future in the auto and the tech sector. You know, I look forward to working with every Member on this panel to preserve our global leadership, strengthen our economic and national security, and beat China. My door is always open.

I want to thank the witnesses for all being here. Your testimony is critical in educating all of us.

[The prepared statement of Mrs. Rodgers follows:]

Opening Statement for Chair Cathy McMorris Rodgers
Committee on Energy and Commerce
Subcommittee on Innovation, Data, and Commerce
Hearing entitled, "Economic Danger Zone: How America Competes to Win the Future Versus China"
February 1st, 2023

INTRO

Welcome to the inaugural first hearing of the Innovation, Data, and Commerce Subcommittee for the 118th Congress.

I'd like to congratulate my good friend, Gus Bilirakis, the new Chair of this Subcommittee and would also congratulate my good friend Tim Walberg, the new Vice Chair of the Subcommittee.

FIGHTING TO WIN THE FUTURE

This committee plays a vital role in advancing American competitiveness and global technological leadership.

It's critical that we use this panel to ensure that America -- not China -- is setting rules of the road for technologies of tomorrow.

It's no secret the CCP wants to replace the U.S. as a global economic and technological power.

Whether it's artificial intelligence, autonomous vehicles, or smart devices, China wants to dominate these new and emerging technologies.

But China's vision of the future is not one that welcomes American values...

...values like freedom of speech, privacy, entrepreneurial enterprise, individual rights, or the rule of law.

The CCP, on the other hand, spies on its citizens and asserts strict government control over businesses and the economy.

We need to make sure these technologies of the future are developed in an ecosystem that promotes America's values, not China's.

This is not a race we can afford to let them win.

PRIVACY

We must work together to cement America's global technological leadership.

We should start by passing comprehensive privacy and data security protections with one national standard.

We made history last year when we passed the bipartisan, bicameral American Data Privacy and Protection Act 53-2.

But our work isn't over yet.... as we have already fallen behind other countries in establishing a national privacy law.

I want to thank Mr. Pallone, Ms. Schakowsky, and of course Mr. Bilirakis for their leadership on this.

I'm eager to continue that work.

This is a top priority for Americans, and needs to be achieved through Congress.

EMERGING TECHNOLOGIES

And we can't stop there.

It's important that we also take action to ensure the development and deployment of autonomous vehicles.

The regulatory framework for AVs must be led by the U.S.

Again, this comes down to our values vs. The CCP's.

America values the importance of the safety of our citizens – China does not.

We value our workforce and free market economics – China does not.

We value civil society groups, and their right to speak freely – China does not.

To win the future, the U.S. must lead on AVs... we must chart the path so the road is one we design.

This can be the year we finally push past the barriers which have derailed the SELF DRIVE Act and other legislation from becoming law.

We can also build on the American COMPETE Act, legislation I sponsored in the 116th Congress, on promoting emerging technologies, which was enacted with provisions from many members of this committee.

BAD BIDEN POLICIES

The best way to beat China is to spur innovation and remove unnecessary, burdensome regulatory barriers...

...We cannot, and shouldn't even try, to beat China at their own game of massive government handouts and centralized industrial policy...

We won't outspend them... and authorizing billions of taxpayer dollars without removing burdensome red tape will only lead to waste.

Instead, we need to encourage innovation, ingenuity, and entrepreneurship, the backbones of our economy...

...and that can only be achieved with a government that encourages low barriers to entry for innovative technologies and startups...

... and the adoption of emerging technologies that will improve people's lives.

Ensuring federal agencies' actions don't put undue burden on businesses and innovators will be a top priority this Congress.

CONCLUSION

Whether it's ensuring people's online information is secure, charting an achievable path towards AV development and deployment in the U.S., or setting the global standards for AI and other emerging technologies...

...this subcommittee is at the center of it.

I look forward to working with every member on this panel to preserve our global leadership, strengthen our economic and national security, and beat China... my door is always open.

I want to thank all the witnesses for your being here today.

Your testimony will be crucial in educating our work moving forward this Congress.

I yield back.

Mrs. RODGERS. And I yield back.

Mr. BILIRAKIS. Thank you, Madam Chair, for your testimony. I appreciate it.

Now I will recognize the ranking member of the full committee, Mr. Pallone, for 5 minutes.

OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Chairman, and congratulations again on your being made the chairman of the subcommittee.

America's economic competitiveness has helped cement America's technological, political, and national security dominance, but our Nation's competitiveness is facing unprecedented challenges. For three decades the Institute for Management Development designated our Nation's economy as one of the five most competitive in the world. Three years ago, during the Trump administration, that ranking plummeted to 10th.

Globalization, protectionist policies, and extraordinary market interventions by our economic rivals are key reasons for this drop. The Chinese Government, a frequent purveyor of predatory economic practices, has adopted policies to give Chinese companies an unfair competitive advantage. This includes massive tax breaks and subsidies for Chinese companies, stifling restrictions on access to the Chinese market, currency manipulation, foreign mergers and acquisitions, forced technology transfers, and intellectual property theft.

Their goal is to dominate high-tech industries like 5G, supercomputers, artificial intelligence, and advanced manufacturing that are essential to economic prosperity and military superiority in the 21st century. And as a result, American manufacturers, innovators, and workers are operating at a competitive disadvantage. Chinese manufacturers' output rose by 170 percent between 2008 and 2021. Over that same period, the U.S. production only grew by 12 percent.

Chinese companies now dominate the market for vital telecommunications network equipment, smartphones, commercial drones, and photovoltaic cells for solar panel production. China is also the largest producer of lithium battery cells and is making strides in the production of electric vehicles.

Now, fortunately, these unprecedented challenges to our economic prosperity and competitiveness are not going unchallenged. Last Congress, congressional Democrats delivered by taking bold action to strengthen our manufacturing base, help create good-paying jobs for American workers, unleash more innovation, and lower costs for consumers.

The CHIPS and Science Act was one of the major laws that we passed last Congress, and it invests $52.7 billion to spur American semiconductor production. It will ensure more superconductors are produced right here in the United States, end our reliance on other countries like China, and lower costs for consumers for automobiles, consumer electronics, home appliances, and other goods. It also invests 1.5 billion to support the deployment of innovative, American-made telecommunications equipment to help counter the

spread of harmful network equipment like China-backed Huawei. The CHIPS and Science Act was a major win for our global competitiveness, for our economy, for our consumers.

Based on the title of today's hearing, you would have thought congressional Republicans would have been running to the floor to vote yes on this bill, but only two Republicans on this committee supported it. The other 27 opposed it. While the overwhelming majority of Republicans opposed the CHIPS and Science Act, we have an opportunity to double down on these monumental victories and enact more vital competitiveness legislation into law this Congress.

And I know my—I know that both Chairman Bilirakis and our Ranking Member Schakowsky mentioned the American Data Privacy and Protection Act, which is the comprehensive privacy legislation that myself and Chairwoman Rodgers sponsored last Congress, and this bill ensures that consumers, wherever they reside in this country, will have meaningful control over their personal information, while providing clear and consistent rules of the road on privacy and data security to innovators, entrepreneurs, and small tech companies.

And I would also like to see us move the supply chain resilience subtitle in the America COMPETES Act, which passed out of the House last Congress. This would create a new office within the Department of Commerce responsible for leading a governmentwide effort to support manufacturing and strengthen supply chains critical to the Nation's economic vitality and national security.

We can continue to blaze a path to a more competitive, stronger economy by building on the work of the last Congress. But one thing we cannot do is dangerously play chicken with the debt limit, as House Republicans are threatening to do. House Republicans have pledged the Nation's full faith and credit to force devastating cuts to Social Security, Medicare, and Medicaid. And that is not the way to ensure our Nation leads the pack economically.

So I hope congressional Republicans realize the severe economic consequences of this action might have, and I also hope we can begin to work on bipartisan solutions to bolster our economy and to outcompete the world. And I urge a strategy that is bipartisan and that will return to responsible governance, working in the interests of all Americans.

I think all of us have America and our constituents at heart, and we can work together as we have in the past to achieve bipartisan solutions that deal with this challenge from China and other competitors.

[The prepared statement of Mr. Pallone follows:]

Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Ranking Member Frank Pallone, Jr.

Innovation, Data, and Commerce Subcommittee Hearing on "Economic Danger Zone: How America Competes to Win the Future Versus China."

February 1, 2023

America's economic competitiveness has helped cement America's technological, political, and national security dominance. But our nation's competitiveness is facing unprecedented challenges. For three decades, the Institute for Management Development designated our nation's economy as one of the five most competitive in the world. Three years ago, during the Trump Administration, that ranking plummeted to tenth.

Globalization, protectionist policies, and extraordinary market interventions by our economic rivals are key reasons for this drop. The Chinese Government – a frequent purveyor of predatory economic practices – has adopted policies to give Chinese companies an unfair competitive advantage. This includes massive tax breaks and subsidies for Chinese companies, stifling restrictions on access to the Chinese market, currency manipulation, foreign mergers and acquisitions, forced technology transfers, and intellectual property theft. Their goal is to dominate high-tech industries like 5G, super computers, artificial intelligence, and advanced manufacturing that are essential to economic prosperity and military superiority in the 21st century.

As a result, American manufacturers, innovators, and workers are operating at a competitive disadvantage. Chinese manufacturing output rose by 170 percent between 2008 and 2021. Over that same period, the United States' production only grew by 12 percent. Chinese companies now dominate the market for vital telecommunications network equipment, smartphones, commercial drones, and photovoltaic cells for solar panel production. China is also the largest producer of lithium-ion battery cells and is making strides in the production of electric vehicles.

Fortunately, these unprecedented challenges to our economic prosperity and competitiveness are not going unchallenged. Last Congress, Congressional Democrats delivered by taking bold action to strengthen our manufacturing base, help create good-paying jobs for American workers, unleash more innovation, and lower costs for consumers.

The CHIPS and Science Act was one of the major laws that we passed last Congress, and it invests $52.7 billion to spur American semiconductor production. It will ensure more superconductors are produced right here in the United States, end our reliance on other countries, like China, and lower costs for consumers for automobiles, consumer electronics, home appliances, and other goods.

It also invests $1.5 billion to support the deployment of innovative, American-made telecommunications equipment to help counter the spread of harmful network equipment, like China-backed Huawei.

The CHIPS and Science Act was a major win for our global competitiveness, our economy, and for consumers. Based on the title of today's hearing – you would have thought Congressional Republicans would have been running to the floor to vote "yes" on this bill. But only two Republicans on this Committee supported the bill. The other 27 Republicans opposed it.

While the overwhelming majority of Republicans opposed the CHIPS and Science Act, we have an opportunity to double down on these monumental victories and enact more vital competitiveness legislation into law this Congress.

We should act on the American Data Privacy and Protection Act, comprehensive privacy legislation I authored with Chair Rodgers. This crucial legislation ensures that consumers—wherever they reside in this country—will have meaningful control over their personal information, while providing clear and consistent rules of the road on privacy and data security to innovators, entrepreneurs, and small tech companies.

I'd also like to see us move the supply chain resilience subtitle in the America COMPETES Act, which passed out of the House last Congress. This would create a new office within the Department of Commerce responsible for leading a government-wide effort to support manufacturing and strengthen supply chains critical to the nation's economic vitality and national security.

We can continue to blaze a path to a more competitive, stronger economy by building on the work of the last Congress, but one thing we cannot do, is dangerously play chicken with the debt limit as House Republicans are threatening to do. House Republicans have pledged the nation's full faith and credit to force devastating cuts to Social Security, Medicare, and Medicaid. That is not the way to ensure our nation leads the pack economically.

I hope Congressional Republicans realize the severe economic consequences this action would have. I also hope we can begin to work on bipartisan solutions to bolster our economy and to out-compete the world.

I urge a strategy that is bipartisan and a return to responsible governance working in the interest of all Americans.

Mr. PALLONE. So I yield back. Thank you, Mr. Chairman.

Mr. BILIRAKIS. I thank the ranking member. We have now concluded with Members' opening statements.

The Chair would like to remind Members that, pursuant to the committee rules, all Members' opening statements will be part of the record.

We would like to thank all of our witnesses for being here today and taking the time to travel to Washington, DC, to testify before the subcommittee. Today's witnesses will have 5 minutes to provide oral testimony, which will be followed by a round of questions from Members.

Our witness panel for today's hearing will include Mr. Jeff Farrah, the executive director of the Autonomous Vehicle Industry Association—welcome, sir; Mr. Marc Jarsulic, who is a senior fellow and chief economist at the Center for American Progress—welcome; Ms. Samm Sacks, cyber policy fellow, International Security Program for New America—welcome; Mr. Brandon Pugh, policy director and resident senior fellow at R Street Institute. We appreciate you being here, as well.

So, Mr. Farrah, we will begin with you, and you have 5 minutes. Thank you.

Mr. FARRAH. Thank you.

Mr. BILIRAKIS. My pleasure.

STATEMENT OF JEFF FARRAH, EXECUTIVE DIRECTOR, AUTONOMOUS VEHICLE INDUSTRY ASSOCIATION; MARC JARSULIC, SENIOR FELLOW AND CHIEF ECONOMIST, CENTER FOR AMERICAN PROGRESS; SAMM SACKS, CYBER POLICY FELLOW, INTERNATIONAL SECURITY PROGRAM, NEW AMERICA; AND BRANDON J. PUGH, POLICY DIRECTOR AND RESIDENT SENIOR FELLOW, CYBERSECURITY AND EMERGING THREATS, R STREET INSTITUTE

STATEMENT OF JEFF FARRAH

Mr. FARRAH. Chair Rodgers, Ranking Member Pallone, Chairman Bilirakis, Ranking Member Schakowsky, distinguished members of the committee, it is my honor to be here before you today.

I am privileged to lead the Autonomous Vehicle Industry Association, which is the unified voice of the AV industry and represents leading automotive, technology, trucking, and transportation companies. Our mission is to advocate for the safe and timely deployment of autonomous technology that will increase safety, expand mobility, and boost supply chains.

We appreciate the strong leadership that has come from this committee in past Congresses and look forward to working with you this year.

It is important to recognize that autonomous vehicles are not science fiction. They are here today. Across the United States, autonomous driving technology is being applied to passenger vehicles, trucks, delivery vehicles, and shuttles. AVs are operating in Arizona, Arkansas, California, Florida, Michigan, Texas, Washington State, and more.

It is key to understand why developers are focused on bringing AV technology to market. It is not an exaggeration to say that safe-

ty motivates everything that the AV industry does, and AVs will make Americans safer. After all, AVs don't speed, they don't drive drunk, and they don't drive distracted. Sadly, human drivers do all of those things, and the Department of Transportation has affirmed that human behavior is the overwhelming contributor to the 43,000 deaths on American roads that we suffered in 2021, which is an 11 percent increase over the year before.

Our industry offers a solution to this tragic problem. Autonomous vehicles are safer than human drivers because they use advanced technology to develop a real-time three-dimensional view that informs the automated driving system, which is the brain that drives the vehicle without the need for human input. AVs are capable of making quicker decisions with many more inputs than a human driver.

Beyond improving safety, AVs have the potential to radically improve mobility for the elderly and disability communities. AVs are also starting to show how they can ease the supply chain crisis and deliver environmental benefits.

Let's turn to the issue of AV adoption worldwide. American AV companies have the most advanced autonomous vehicles, and billions of dollars have been invested in innovative companies. But unfortunately, the United States is at severe risk of falling behind the rest of the world on AV public policy, which could deny Americans the technology's lifesaving and mobility benefits.

One competitor is the Chinese Government, which has made AV development a top priority and highlighted AVs in its Made in China 2025 Strategic Initiative. These measures are producing autonomous companies with global aims. China's focus on advancement in this space should be alarming, as no American policymaker should want to see a world where China dominates the AV market. This scenario presents national security challenges and would also mean that the U.S. would not see much of the job creation from a prosperous AV industry.

The United States cannot assume it will win the global AV race, thereby securing a leadership position in what many estimate will be a multitrillion-dollar market opportunity. For the United States to win the AV race, we must put in place a national policy framework focused on deployment and commercialization.

The time is long past due, as efforts to enact a national AV framework have stalled in recent years. Twenty-two States have taken action to authorize deployment of autonomous vehicles on their roads. State-by-State action is not ideal, but it has become important for AV advancement in the absence of a Federal framework.

I detail what a Federal policy framework should look like in my written testimony, which includes reforming the vehicle exemption process that is harming commercialization and completing agency rulemakings that remove barriers to deployment. This action would send a strong message that our country is determined to be the global leader on the next great technological change for our world.

We are at a crossroads for the American AV industry, and frankly, we need your help. Make no mistake: The United States can lead the way on autonomous vehicles. But policymakers must prioritize AV policy, and do so with urgency.

Thank you for the opportunity to testify today, and I look forward to any questions you may have.

[The prepared statement of Mr. Farrah follows:]

U.S. House of Representatives

Committee on Energy & Commerce

Subcommittee on Innovation, Data, and Commerce

Hearing on "Economic Danger Zone: How America Competes to Win the Future Versus China"

Wednesday, February 1, 2023

Testimony of Jeff Farrah, Executive Director of the Autonomous Vehicle Industry Association

Summary of Testimony

Today, the United States is leading the world in the development and deployment of autonomous vehicles ("AVs"). By removing opportunities for human error, AVs are positioned to help significantly reduce roadway crashes and deaths at a time when both are at near record highs. The adoption of AVs will also expand transportation access to those who are unable to drive—like elderly individuals or individuals experiencing physical challenges—and will increase job access for millions of mobility- or transportation-challenged individuals, letting them participate in the economy in ways they could not before.

Autonomous vehicles are an American invention, with American AV developers pioneering the technology and American entrepreneurs investing in and building innovative AV companies across the country. However, American leadership in the AV industry is not guaranteed. Across the globe, other nations are seeking to take the lead in AV development by building out regulatory frameworks for widespread AV deployments and providing government support for AV developers as they put their vehicles on the road. The Chinese government, in particular, has prioritized and supported AV development through legislative and regulatory actions for years, and this support is helping to produce autonomous vehicle companies.

Losing ground on the deployment of this technology risks cutting the United States out of the safety, accessibility, economic, and job-creating benefits of a prosperous AV industry. The United States can maintain its lead in AV technology by creating a national policy framework that prioritizes American leadership and has Congress, the U.S. Department of Transportation, and the private sector acting in partnership to support the deployment of AVs and ensure that the safety, economic, mobility, and efficiency benefits of AVs can be felt not only in the states where AVs are already on the road, but nationwide.

Testimony of Jeff Farrah, Executive Director of the Autonomous Vehicle Industry Association

I. Introduction

Chairman Bilirakis, Ranking Member Schakowsky, distinguished members of the Subcommittee, it is my honor to testify before you today. My name is Jeff Farrah, and I am privileged to lead the Autonomous Vehicle Industry Association as its Executive Director. Our industry appreciates the strong engagement of members of this committee on autonomous vehicle policy.

The Autonomous Vehicle Industry Association ("AVIA") is the unified voice of the autonomous vehicle ("AV") industry[1] and we represent the world's leading technology, trucking, ridesharing, automotive, and transportation companies. The cross-section of companies demonstrates the widespread interest in developing AV technology across industries. Our mission is to bring the tremendous safety and mobility benefits of AVs—otherwise known as SAE Levels 4- and 5-capable vehicles—to consumers in a safe, responsible, and expeditious manner.[2]

The automation of driving has been an aspiration for decades, and for years many questioned *when* autonomous vehicles would be on America's roads. Today, we can proudly answer *they are here now*, with applications ranging from autonomous ride-hailing and trucking to delivery vehicles and shuttles, operating in states as diverse as Arizona, Arkansas, California,

[1] Our members include: Apple, Aurora, Cavnue, Cruise, Embark, Ford, Gatik, Kodiak, Lyft, May Mobility, Motional, Navya, Nuro, TuSimple, Uber, Volkswagen Group of America, Volvo, Waabi, Waymo, and Zoox. *See Our Mission and Members*, AVIA, https://theavindustry.org/about/mission.

[2] SAE's J3016 standards have been adopted industry wide. Level 2 systems (often called advanced driver assistance systems or "ADAS") are available on vehicles today and are capable of "partial driving automation," requiring human supervision at all times. Level 3 vehicles have "conditional driving automation," where the vehicle requires human interaction only in specific situations. Only Level 3, 4, and 5 vehicles are equipped with automated driving systems ("ADS"). *See Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles – J3016_202104*, SAE International, https://www.sae.org/standards/content/j3016_202104/ (last visited Jan. 30, 2023).

Florida, Michigan, Texas, and others. In these states, vehicles equipped with an "automated driving system," or "ADS," are making driving decisions, navigating roads, carrying passengers, and hauling freight all without the need for ongoing human input.

It is critical to distinguish autonomous vehicles from vehicles equipped with technology that helps licensed humans drive better. This "driver-assistance technology"—which we see in tens of millions of cars and trucks all around us—is important and helpful, but it is not *autonomous* driving. Rather, the term "autonomous vehicle," or "AV," indicates that the vehicle is capable of driving on its own, without relying on or having any expectation that a human will take back control. With an AV, the vehicle performs *all* aspects of the driving task on a sustained basis. This is the technology that is being developed by AVIA's members, and it will transform the way people and goods move in the world.

The ongoing deployment of AVs is beginning to show us how the adoption of autonomous vehicles will benefit the public in many ways. Of paramount importance is the ability of AVs to make us safer. AVs do not speed, they do not text, and they do not drive drunk or fatigued. Sadly, human drivers do all those things, contributing to a 16-year high in road deaths in 2021, when over 42,000 Americans died on our roads, an 11% increase over the year before.[3] The National Highway Traffic Safety Administration's ("NHTSA") early estimates for the first three quarters of 2022 fortunately signal a slight decline in road deaths—a .2% decrease as compared to the same time in 2021—for the first time since 2020, but those same numbers indicate increases in deaths among

[3] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., DOT HS 813 298, EARLY ESTIMATES OF MOTOR VEHICLE TRAFFIC FATALITIES AND FATALITY RATE BY SUB-CATEGORIES IN 2021, 1 (2022), https://www.nhtsa.gov/press-releases/early-estimate-2021-traffic-fatalities.

cyclists, motorcyclists, and pedestrians.[4] The 2022 numbers also show a 12% increase in deaths on rural roads and a 10% increase in fatalities from crashes involving at least one large truck.[5]

One fact has been confirmed and re-confirmed several times over: human behavior is overwhelmingly the most common factor in fatal accidents on our roads. A recent study by NHTSA found that over 55% of all people injured or killed in a roadway incident tested positive for drugs or alcohol.[6] Drivers are also frequently distracted by electronics; at any given time, almost 3% of all drivers are looking at or using their handheld device.[7] Though it is intuitive to begin with, studies have also found that drivers manipulating cell phones are two to six times more at risk of a crash.[8] Several categories of behavior-related fatalities have increased in the past few years, including police-reported alcohol-involved crashes and deaths of unrestrained passengers.[9]

AVs are positioned to combat the trend of unsafe driving that has persisted for years on U.S. roads. AVs have unprecedented visibility of the world and lanes around them as a result of the multiple technologies they employ—like LiDAR, radar, and cameras—that all work together to inform the ADS, which is the brain that drives the vehicle. The combination of these systems leads to quicker decisions with many more inputs compared to a human driver's capabilities. By combining multiple sensors, AVs also have a 360-degree field of vision which can detect, track, and react to objects and people even when they are hidden from human perception due to vehicles,

---

[4] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., DOT HS 813 406, EARLY ESTIMATE OF MOTOR VEHICLE TRAFFIC FATALITIES FOR THE FIRST 9 MONTHS (JANUARY-SEPTEMBER) OF 2022, 1 (2022), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813406.
[5] *Id.*
[6] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., DOT HS 813 399, ALCOHOL AND DRUG PREVALENCE AMONG SERIOUSLY OR FATALLY INJURED ROAD USERS, 2 (2022), https://rosap.ntl.bts.gov/view/dot/65623/dot_65623_DS1.pdf.
[7] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., DOT HS 813 184, DRIVER ELECTRONIC DEVICE USE IN 2020, 1 (2021), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813184.pdf.
[8] *Distracted driving*, IIHS, https://www.iihs.org/topics/distracted-driving (last visited Jan. 30, 2023).
[9] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., U.S. DEP'T OF TRANSP., DOT HS 813 298, EARLY ESTIMATES OF MOTOR VEHICLE TRAFFIC FATALITIES AND FATALITY RATE BY SUB-CATEGORIES IN 2021, 1 (2022), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813298.

buildings, and other obstructions. I was recently outside Dallas, Texas riding in autonomous trucks, and it is amazing to witness these vehicles navigate oncoming freeway traffic that a human could never see.

The adoption of AVs will also bring new mobility benefits to those who are unable to drive—like elderly individuals and individuals experiencing physical challenges—by providing greater access to transportation. By expanding transportation access, AVs can also increase job access for millions of mobility or transportation-challenged individuals, allowing them to participate in the economy in ways they could not before. Additionally, AVs can create new job opportunities for individuals with a wide range of educational backgrounds and experiences. Further, by bringing goods directly to consumers and optimizing the transportation of freight, AVs can ease the ongoing supply chain crisis. They can also deliver environmental benefits, as smoother driving reduces emissions and fuel consumption.

II. American Leadership on Autonomous Vehicles is Needed

Today, the United States is the global leader in the AV industry, with a robust ecosystem of American companies working on all aspects and applications of the technology. However, the United States must not assume it will win the global AV race and sustain its leadership position in a market potentially worth multiple trillions of dollars.[10] Rather, to ensure we will continue to lead on AV development and deployment in the future, we must get three things right: technology development; capital investment; and public policy.

---

[10] SONIA ABHAY, ALLIED MARKET RESEARCH, AUTONOMOUS VEHICLE MARKET BY LEVEL OF AUTOMATION (LEVEL 1, LEVEL 2, LEVEL 3, LEVEL 4, AND LEVEL 5), APPLICATION (CIVIL, DEFENSE, TRANSPORTATION & LOGISTICS, AND CONSTRUCTION), DRIVE TYPE (SEMI-AUTONOMOUS AND FULLY AUTONOMOUS), AND VEHICLE TYPE (PASSENGER CAR AND COMMERCIAL VEHICLE): GLOBAL OPPORTUNITY ANALYSIS AND INDUSTRY FORECAST, 2021-2030 (2022), https://www.alliedmarketresearch.com/autonomous-vehicle-market; TECONOMY PARTNERS, FOREFRONT: SECURING PITTSBURGH'S BREAK-OUT POSITION IN AUTONOMOUS MOBILE SYSTEMS ES-1-2 (2021), https://ridc.org/wp-content/uploads/2021/10/PGH-Autonomy-Report-Executive-Summary.pdf.

The United States is leading in the first two categories. AVs are an American invention. Many of the leading voices in AV development today participated in Defense Advanced Research Projects Agency ("DARPA")-sponsored challenges in the early 2000s. These pioneers used their technical prowess to become entrepreneurs, building dynamic companies across the United States—leading to an explosion in AV development over the last decade. American AV companies have developed the most advanced ADS to date, and billions have been invested in innovative AV companies, ranging from dogged startups to more established players with experience scaling in the transportation sector.

But the unfortunate truth is that the United States is at severe risk of falling behind the rest of the world on AV public policy, which could deny Americans the technology's lifesaving, mobility, and efficiency benefits, while also harming the United States' global economic competitiveness.

China looms as a major potential competitor to the United States for leadership in the AV industry. As discussed in detail below, the Chinese government has prioritized and supported AV development through legislative and regulatory actions since at least 2015, when the Made in China 2025 strategic initiative identified AVs as a key area of focus.[11] As China looks to the mass commercialization of AVs, a growing number of local governments are authorizing AV operation and driverless ride-hailing services. All of this government-backed support is helping to produce autonomous vehicle companies. Let me be clear: our industry is not asking that the United States approach AVs in the same way as the Chinese government. But we must recognize that the Chinese

[11] Anjani Trivedi, *China Sets the Rules of the Road*, WASH. POST (Oct. 12, 2022, 6:31 PM), https://www.washingtonpost.com/business/china-sets-the-rules-of-the-road/2022/10/11/db25bdda-49b0-11ed-8153-96ee97b218d2_story.html.

government takes AV development seriously and is determined to be a world leader in this transformational technology, as China is in several other technologies.

China's focus on advancement in this space should be alarming, as no American policymaker should want to see a world where China dominates the AV market. This scenario presents immense national security challenges and would also mean the United States would not see much of the job creation from a prosperous AV industry.

This international competition is happening at an inflection point for the American AV industry, as the technology is now being commercialized and the benefits of AVs are beginning to accrue. Now is the time for policymakers to establish a national policy framework that prioritizes American leadership and has Congress, the U.S. Department of Transportation, and the private sector acting in partnership. While federal efforts to establish such a framework have stalled in the last several years, twenty-two (22) states have recognized the benefits of AVs by expressly approving AV deployment on their roads. A state-by-state approach is certainly suboptimal, but it has become a necessary path forward for the AV industry to deploy our life-saving technology in the absence of federal action. Below I lay out in detail policy recommendations that would form such a federal framework. Our industry has greatly appreciated the leadership of members of this Committee on bipartisan AV legislation in the past and looks forward to working with you again this Congress as legislation moves and agencies take action. Such actions would send a strong message that our country is determined to be the global leader on the next great technological change in the world.

Make no mistake: the United States can lead the way on autonomous vehicles. But we must clear the path to safe commercialization and do so with urgency. Our country has been the global innovation leader for decades, but we cannot assume that we will continue to lead on AVs in the

absence of federal action. The United States must commit itself to AV leadership to ensure that the safety, economic, mobility, and efficiency benefits of AVs can be felt not only in the states where AVs are already on the road, but nationwide.

III. Competition on AV Leadership from Abroad

America's leadership role is integral to securing the economic growth, job creation, and many safety and societal benefits offered by AVs. It is important that policymakers understand the considerable foreign competition, including from China, Europe, and Japan, that is faced by the United States.

China. China's government has invested heavily in the development of autonomous vehicles in recent years as part of its strategy to overtake and replace foreign market leaders, leading to projections that China's share of the autonomous vehicle market will be worth approximately 50% of the market's overall estimated value by 2025.[12] Reflecting China's investment in AVs, the Chinese government issued a joint strategy in 2020 prioritizing AV development and establishing goals for the large-scale production of AVs by 2025, calling for at least 20% of all new vehicles sales to have SAE Level 4 capabilities by 2030.[13] In 2022, China's Ministry of Transportation released rules in an effort to commercialize driverless mobility.[14] Meanwhile, eight major cities in China currently allow testing of driverless ride-hailing services, and multiple AV companies have obtained permits in these cities to operate autonomous taxis.[15] One company, AutoX, backed by e-commerce giant Alibaba, announced the launch of autonomous

---

[12] *See* Anjani Trivedi, *China Sets the Rules of the Road*, WASH. POST (Oct. 12, 2022, 6:31 PM), https://www.washingtonpost.com/business/china-sets-the-rules-of-the-road/2022/10/11/db25bdda-49b0-11ed-8153-96ee97b218d2_story.html.
[13] Takashi Kawakami & Naoshige Shimizu, *China's self-driving car push hits legal and cost roadblocks*, NIKKEI ASIA (Jan. 19, 2023), https://asia.nikkei.com/Business/Automobiles/China-s-self-driving-car-push-hits-legal-and-cost-roadblocks.
[14] *Id.*
[15] *Id.*

taxis on public roads across an area three times the size of Manhattan within Shenzhen in January 2021.[16] Apollo Go, backed by China's leading search engine, Baidu, began publicly testing its robotaxis in Shanghai in September 2021.[17] According to Baidu, one million rides have already been completed since it rolled out the service, and it plans to expand into dozens of other Chinese cities by 2030.[18] Most recently, Baidu expanded its driverless ride-hailing services to public roads in Beijing in April 2022, where another China-based AV company, Pony.ai, also deploys driverless robotaxis.[19] Many other Chinese companies are investing in AV technology and testing, including Huawei, WeRide.ai, Didi Chuxing, and Momenta. Further, these companies are attracting investment from other countries around the world. The Chinese AV industry has seen some fluctuation as well, with total investments in 2022 at around $3 billion, a figure that was significantly smaller compared to 2021 investments.[20]

European Union ("EU"). In August 2022, the European Commission issued the first EU-wide safety regulations for the automated driving systems of "fully automated" vehicles, enabling EU-wide approvals for commercial deployment of vehicles with these systems.[21] This marked the first multinational safety regulation for fully automated vehicles and provided added certainty to the AV industry but also a significant competitive advantage for the region.

---

[16] Rita Liao, *China's Robotaxis Charged Ahead in 2021*, TECHCRUNCH (Jan. 14, 2022, 8:20 AM), https://techcrunch.com/2022/01/14/2021-robotaxi-china/.
[17] Rebecca Bellan, *Chinese Tech Giant Baidu Begins Publicly Testing Apollo Go Robotaxis in Shanghai*, TECHCRUNCH (Sept. 14, 2021, 1:24 AM), https://techcrunch.com/2021/09/13/chinese-tech-giant-baidu-begins-publicly-testing-apollo-go-robotaxis-in-shanghai/.
[18] *Robotaxis are taking over China's roads. Here's how they stack up to the old-fashioned version*, CBS NEWS (Aug. 18, 2022), https://www.cbsnews.com/news/china-robotaxis-self-driving-cabs-taking-over-cbs-test-ride/.
[19] Rebecca Bella, *Baidu, Pony.AI Win First Driverless Robotaxi Permits in China*, TECHCRUNCH (Apr. 27, 2022, 11:21 PM), https://techcrunch.com/2022/04/27/baidu-pony-ai-win-first-driverless-robotaxi-permits-in-china/.
[20] *Id.*
[21] Commission Implementing Regulation 2022/1426 of Aug. 5 2022, Laying Down Rules for the Application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as Regards Uniform Procedures and Technical Specifications for the Type-Approval of the Automated Driving System (ADS) of Fully Automated Vehicles, 2022 O.J. (L 221).

Germany. In February 2022, the German federal government adopted a domestic regulation for the operation of motor vehicles with automated and autonomous driving functions, which completes the national legal framework for autonomous driving.[22] Reflective of the German government's support for AVs, companies like Mobileye are already testing vehicles in German cities such as Munich.[23]

France. In September 2022, the French government enacted its regulatory framework for the approval, testing, and commercial operation of "fully automated" systems on public roadways across the country.[24]

United Kingdom ("UK"). In August 2022, the UK government announced its intention to establish a full legislative and regulatory framework by 2025 to enable the safe, commercial operation of AVs on UK roads.[25] The country has invested £200 million into British AV startups, and AV testing is already underway across the country with backing from the UK government, universities, technology companies, and research institutions.

Japan. Japan plans to incorporate SAE Level 4 autonomous driving into its traffic law in April of this year.[26] This is the latest step in Japan's demonstrated support for AVs, following

---

[22] German Fed. Ministry for Digital Affairs and Transport, *Federal Cabinet Passes Regulation on Autonomous Driving* (February 23, 2022), https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2022/008-wissing-verordnung-zum-autonomen-fahren.html.

[23] Kyle Hyatt, *Intel's Mobileye Goes for an Autonomous Spin Around Munich*, CNET: ROADSHOW (Dec. 15, 2020, 5:00 AM), https://www.cnet.com/roadshow/news/mobileye-self-driving-munich-demonstration/.

[24] Décret 2021-873 du 29, 2021 portant application de l'ordonnance n° 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation [decree 2021-873 of June 29, 2021 implementing Ordinance No. 2021-443 of 14, April 2021 on the responsibility regime applicable in case of circulation of a vehicle equipped with an automated driving system and its conditions of use], https://www.ecologie.gouv.fr/sites/default/files/DGITM-communication-decret-arretes_septembre_2022-EN.pdf.

[25] Ryan Morrison, *UK Government 2025 Driverless Cars Target "Ambitious and Achievable,"* TECH MONITOR (August 19, 2022), https://techmonitor.ai/leadership/governance/driverless-cars-uk-government-autonomous-vehicles.

[26] Graham Hope, *Japan to Greenlight Self-Driving Vehicles in 2023,* IOT WORLD TODAY (November 3, 2022), https://www.iotworldtoday.com/transportation-logistics/japan-to-greenlight-self-driving-vehicles-in-2023.

Japan's enactment of a Road Transport Vehicle law in 2020 recognizing AVs and establishing a related inspection regime and permit system.[27]

IV. The United States Risks Losing Out on the Economic Benefits of AVs

The United States risks ceding vast economic benefits if it falls behind countries like China in the race to AV deployment. In the United States, the AV industry has created new jobs and brought new investment, tax revenue, resources, and human capital to states across the country, including California, Alabama, Arizona, Arkansas, Kansas, Nevada, New Mexico, Oklahoma, Pennsylvania, Michigan, Florida, Washington, Colorado, and Texas. These benefits are already being felt at local levels, with a study performed for the Pittsburgh-based Regional Industrial Development Corporation finding that in the Pittsburgh region alone, the AV industry has created 6,300 new jobs.[28] In California, the introduction of AV trucking is anticipated to create 2,400 jobs and increase the state's real GDP and welfare by at least $6 billion a year.[29] By 2050, the value of public and consumer benefits of AV deployment, including reduced congestion, avoided accidents, and saved time, could add up to $796 billion annually.[30] The further development of the AV industry can help grow the U.S. economy and support the economic competitiveness of American businesses, allowing them to capitalize on the strength and breadth of American innovation in the

---

[27] Kazuhiro Ogawa, *Japan Revamps Laws to put Self-driving Cars on Roads*, NIKKEI ASIA (Mar. 9, 2019), https://asia.nikkei.com/Politics/Japan-revamps-laws-to-put-self-driving-cars-on-roads.

[28] TECONOMY PARTNERS, FOREFRONT: SECURING PITTSBURGH'S BREAK-OUT POSITION IN AUTONOMOUS MOBILE SYSTEMS ES-1-2 (2021), https://ridc.org/wp-content/uploads/2021/10/PGH-Autonomy-Report-Executive-Summary.pdf.

[29] *Autonomous long-haul trucking stands to grow the Golden State's economy while creating jobs and raising wages without mass driver layoffs*, SILICON VALLEY LEADERSHIP GROUP (Apr. 13, 2022), https://www.svlg.org/study-shows-autonomous-trucking-will-grow-californias-economy/.

[30] SECURING AMERICA'S FUTURE ENERGY, AMERICA'S WORKFORCE AND THE SELF-DRIVING FUTURE, SECURING AMERICA'S FUTURE ENERGY 9 (June 2018), https://avworkforce.secureenergy.org/wp-content/uploads/2018/06/SAFE_AV_Policy_Brief.pdf.

industry. Simply put, policies that support the deployment of AVs are policies that support the growth of the U.S. economy.[31]

A. Job Expansion in the AV Industry

Across the United States, the AV industry is creating jobs and providing opportunities for workers with a wide array of expertise and educational backgrounds, including many jobs that do not require a college degree. AV developers and manufacturers are hiring auto technicians, fleet managers, safety operations specialists, sensor calibrators, transportation planners, engineers, and many others to serve the growing needs of their vehicle fleets. As the industry continues to expand, delivery workers, and grocery store employees will be involved in selecting, packing, and delivering goods to consumers, among other jobs and roles that will emerge. The deployment of AVs can expand access to affordable delivery while also creating over three million new jobs by 2035, as retailers and delivery providers expand their services, according to a study conducted by Steer.[32]

Today, the AV industry is investing in partnerships to create the jobs of tomorrow. These investments not only move AV technology forward, but also prepare the American workforce to compete globally with our adversaries. For example, AVIA member Nuro has developed a program with De Anza Community College that will offer a new career pathway to prepare the next generation of autonomous fleet technicians.[33] The initiative, which will include more locations in the near future, includes a free tuition option, access to paid internships and part time

---

[31] Jack Caporal, William O'Neil, and Sean Arrieta-Kenna, *Bridging the Divide: Autonomous Vehicles and the Automobile Industry*, CSIS (Apr. 14, 2021), https://www.csis.org/analysis/bridging-divide-autonomous-vehicles-and-automobile-industry.

[32] STEER, ECONOMIC IMPACTS OF AUTONOMOUS DELIVERY SERVICES IN THE U.S. xi (2020), https://www.steergroup.com/sites/default/files/2020-09/200910_%20Nuro_Final_Report_Public.pdf.

[33] *Autonomous and Electric Vehicle Technician Pathway*, DE ANZA COLLEGE, https://www.deanza.edu/autotech/av#:~:text=A%20New%20Career%20Pathway%20With,nation%20%E2%80%94%20for%20De%20Anza%20students (last visited Jan. 30, 2023).

work, and preference for full time jobs with and benefits upon graduation. Similarly, AVIA member Aurora has partnered with Pittsburgh Technical College to create and launch a new associate degree program that trains autonomous service engineer technicians.[34]

B. Consumer Savings

AVs are positioned to reduce both the general costs of transportation and the costs of consumer goods. With respect to transportation costs—which amount to the second-largest expense for most households—AVs could reduce average household costs by as much as $5,600 per year when consumers rely on shared fleets of AVs.[35] When used for consumer deliveries, for example, AVs have the potential to dramatically reduce costs to consumers, with some pilots costing only $5.95 per grocery delivery, compared to added costs of between $10 and $20 charged by existing delivery services.[36] The wider deployment of AVs for consumer deliveries and personal transportation would be particularly impactful in food deserts, rural communities, and other areas that do not have significant, accessible public transit options.

AV trucking is also positioned to substantially decrease the cost of goods while fundamentally improving interstate commerce by changing the manner and speed in which goods move in our country, all while making roads safer for everyone. Our country faces a shortage of nearly 78,000 truck drivers, and that figure is projected to almost double by 2031.[37] Given the

---

[34] *Pittsburgh Technical College Launches Robotics and Autonomous Engineering Technology Program*, PITTSBURGH TECHNICAL COLLEGE, https://www.pghtech.org/news-and-publications/PTC_Robotics (last visited Jan. 30, 2023).
[35] SAFE, *FOSTERING ECONOMIC OPPORTUNITY THROUGH AUTONOMOUS VEHICLE TECHNOLOGY* (July 2020) https://safe2020.wpenginepowered.com/wp-content/uploads/2020/07/Fostering-Economic-Opportunity-through-Autonomous-Vehicle-Technology.pdf.
[36] STEER, ECONOMIC IMPACTS OF AUTONOMOUS DELIVERY SERVICES IN THE U.S., xi (2020), https://www.steergroup.com/sites/default/files/2020-09/200910_%20Nuro_Final_Report_Public.pdf.
[37] *Driver Shortage Update 2022*, AMERICAN TRUCKING ASSOCIATION (Oct. 25, 2022), https://ata.msgfocus.com/files/amf_highroad_solution/project_2358/ATA_Driver_Shortage_Report_2022_Executive_Summary.October22.pdf.

timeline for AV truck deployment, autonomous trucking is not likely to cause significant displacement of jobs in the trucking industry,[38] but it can serve as one tool to reduce strains on the supply chain caused, in part, by the longstanding truck driver shortage. Trucking is essential to the movement of goods in the United States; 65% percent of U.S. consumable goods are brought to market by trucks. Implementation of full autonomy in the trucking sector stands to decrease operating costs by about 45%—resulting in savings between $85 billion and $125 billion.[39] Additionally, a study funded by the U.S. Department of Transportation and the Federal Highway Administration indicated that adoption of AV trucking will increase total U.S. employment by 26,400 to 35,100 jobs per year on average and raise annual earnings for all U.S. workers by between $203 and $267 per worker per year.[40] The benefits to our nation's economy, workers, and supply chains make AV trucking well positioned to complement the broader array of economic benefits that AV deployment will bring.

Preserving American leadership in the AV industry is key to ensuring the economic benefits of AV deployment reach American companies, workers, and consumers. A supportive national AV policy framework that promotes widespread AV deployment and commercialization will help secure that leadership against foreign competitors and unlock greater opportunities for American companies to test and deploy AVs safely.

---

[38] *See* SECURING AMERICA'S FUTURE ENERGY, AMERICA'S WORKFORCE AND THE SELF-DRIVING FUTURE REALIZING PRODUCTIVITY GAINS AND SPURRING ECONOMIC GROWTH (June 2018), https://avworkforce.secureenergy.org/wp-content/uploads/2018/06/Americas-Workforce-and-the-Self-Driving-Future_Realizing-Productivity-Gains-and-Spurring-Economic-Growth.pdf.

[39] Aisha Chottani, Greg Hastings, John Murnane, and Florian Neuhaus, *Distraction or disruption? Autonomous trucks gain ground in US logistics*, MCKINSEY & CO. (Dec. 10, 2018), https://www.mckinsey.com/industries/travel-logistics-and-infrastructure/our-insights/distraction-or-disruption-autonomous-trucks-gain-ground-in-us-logistics.

[40] ROBERT WASCHIK ET AL., JOHN A. VOLPE NAT'L TRANSP. SYS. CTR., FHWA-JPO-21-847, MACROECONOMIC IMPACTS OF AUTOMATED DRIVING SYSTEMS IN LONG-HAUL TRUCKING, 1 (2021), https://rosap.ntl.bts.gov/view/dot/54596.

V. Creating a National Framework for AVs

To protect American leadership in the AV industry and maximize the benefits of AV technology, the AV industry and policymakers need to work together to establish a national framework for the safe and swift deployment of AVs in all forms. This should include actions by both Congress and the U.S. Department of Transportation to create legal and regulatory conditions that can help the AV industry thrive and bring the benefits of AVs to all Americans.

A. Federal AV Legislation

To maintain and strengthen American leadership in the AV industry, Congress should enact federal legislation that outlines the necessary statutory and regulatory elements that are critical to the industry's success. To best support the further development of the AV industry, federal AV legislation should:

- **Preserve Existing Federal Roles with Respect to Vehicle Regulation**. The wide deployment of AVs should not change the existing federal role in regulating the design, construction, and performance of motor vehicles, as administered by NHTSA, nor the traditional federal role in the operation, licensing, inspection, repair, and maintenance of commercial vehicles ("CMV") transporting property or passengers in interstate commerce, as administered by the Federal Motor Carrier Safety Administration ("FMCSA"). A comprehensive regulatory approach would also provide states with sufficient guidance to ensure AV regulations are uniform across the country for both commercial and passenger vehicles.
- **Reform the Exemption Process.** Companies granted exemptions from Federal Motor Vehicle Safety Standards ("FMVSS") for novel design vehicles currently face a statutory cap of 2,500 vehicles per company per year. This restrictive model prevents industry from

scaling. Federal legislation should reform, streamline, and expand the vehicle exemption process to increase the number vehicles that can be produced under an exemption and lengthen the window in which the vehicles can be produced.[41] When reforming exemptions, Congress should also expand eligibility for the FAST Act's testing and evaluation exemption to level the playing field among all stakeholders in the AV and ADS development ecosystem.[42]

- **Direct NHTSA to Complete Rulemakings.** Federal legislation should direct NHTSA to complete rulemakings to modernize the FMVSS to support the deployment of AV technology.
- **Codify Existing Interpretations.** To continue to provide certainty to the AV industry, federal legislation should codify existing NHTSA and FMCSA interpretations that support the deployment of AVs, including:
    - NHTSA's interpretation that the disabling of a vehicle's manual controls during autonomous operation does not run afoul of the "make inoperative provision" of the Motor Vehicle Safety Act (49 U.S.C. § 30122); and
    - FMCSA's interpretation that the Federal Motor Carrier Safety Regulations ("FMCSRs") do not require a human driver to operate or be present in a commercial motor vehicle operated by a SAE Level 4 or Level 5 ADS.

[41] Expanding the cap on vehicle production under exemptions was proposed in past drafts of AV legislation. *See* BILL CANIS CONG. RSCH. SERV., R45985, ISSUES IN AUTONOMOUS VEHICLE TESTING AND DEPLOYMENT 17-18 (2021), https://sgp.fas.org/crs/misc/R45985.pdf.

[42] The FAST Act exemption, codified at 49 U.S.C. § 30112(b)(10), allows the deployment of non-FMVSS-compliant vehicles for testing purposes, but only by manufacturers who were producing FMVSS-compliant vehicles prior to the date the FAST Act was enacted in 2015. Due to this, AV developers founded after 2015 or who have not previously produced FMVSS-compliant vehicles are unable to utilize the exemption.

- **Expand Access to Mobility.** First, federal legislation should ensure that no government policy, legislation, or regulation would require individuals to obtain a license to be a passenger in an autonomous vehicle. Second, to better understand the promise of AV technology, legislation could direct studies on the economic, access, and equity impacts of AVs to better understand the technology's promise.

B. AV Regulation and Policy

As federal AV legislation progresses, the Administration and the U.S. Department of Transportation can take a number of steps to help preserve American leadership in the AV industry. This includes:

- **Swiftly Update Regulations.** The U.S. Department of Transportation should swiftly update regulations to support AV deployment, starting with the implementation of existing proposed rules (*e.g.*, the rule on telltales, indicators, and warnings in ADS-equipped vehicles or the rule on crash avoidance testing for new ADS vehicle designs, both of which are currently in the prerule stage) and expanding to new enabling rules that support the deployment of ADS-equipped vehicles, including those with novel designs.
- **Establish a National Demonstration and Deployment Program**. To accelerate the path for novel design vehicles, the Administration should support, and the U.S. Department of Transportation should establish a national demonstration and deployment program for AV developers, a concept that has been proposed by NHTSA in recent years. This program would help evaluate the commercialization of AVs, including those that do not conform to all FMVSS. This program should be a streamlined, flexible supplement to traditional routes to deployment, such as the existing exemption processes and self-certification.

- **Complete the Final Rule on Safe Integration of ADS in Commercial Motor Vehicles.** FMCSA should swiftly complete a rule or series of rules that encourages AV truck developers to safely expand operations and commercialization and codifies the existing interpretation that the FMCSRs do not require a human driver to operate or be present in a commercial motor vehicle being operated by a SAE Level 4 or Level 5 ADS.
- **Pursue International Engagement**. The Administration and the U.S. Department of Transportation should preserve foreign market access and U.S. leadership in the AV industry by remaining actively engaged with other governments and international bodies about AV policymaking.

V. Conclusion

Congress is well positioned to help preserve America's AV leadership through legislation that creates a national framework for the deployment and commercialization of AVs. Such a framework will help bring the safety and economic benefits of AVs to all Americans. I thank the Subcommittee for its leadership on these important issues. The Autonomous Vehicle Industry Association looks forward to serving as a resource concerning both technical and policy questions and working with you to make safe autonomous vehicles a reality for Americans nationwide.

Mr. BILIRAKIS. Thank you, Mr. Farrah. Now we will recognize Mr. Jarsulic.

You are recognized, sir, for 5 minutes.

STATEMENT OF MARC JARSULIC

Mr. JARSULIC. Thank you, Chairman Bilirakis and Ranking Member Schakowsky, for the opportunity to testify at this important hearing.

Today I will focus briefly on three points: the importance of a strong manufacturing sector for economic competitiveness and national security; the requirements for success in advanced manufacturing; and the need for effective industrial policy to support that success.

First on manufacturing—the importance of manufacturing competitiveness. Manufacturing has historically been a source of productivity growth and high-wage employment. Much of manufacturing productivity growth is derived from innovation. It is the adoption of new technologies. The ability of many U.S. manufacturers to operate at the technical frontier has made U.S. manufactured goods competitive internationally. And until recently, the U.S. was the largest manufacturing exporter.

While in the aggregate much of U.S. manufacturing productivity remains at the frontier, the competitive lead has been eroded. For example, in recent decades German manufacturing total factory productivity growth, which is commonly used as a measure of innovation, has exceeded that of the U.S.

U.S. manufacturing has also been challenged by the rise of China as a competitor. China has overtaken the U.S. as the world's leading manufacturer—or leader in manufacturing value added, and leads the U.S. in manufacturing exports. In addition, the Chinese Government is devoting considerable resources to move ahead in crucial areas such as artificial intelligence, advanced robotics, energy-saving vehicles, biopharma.

These challenges to U.S. leadership in advanced manufacturing create both economic and security risks. The reduction in domestic auto production over the past 2 years caused by semiconductor chip shortages illustrates the economic risk posed by disruptions to semiconductor supply chains. Security risks are illustrated by the Department of Defense's ongoing reliance on Asian producers of microprinted circuit boards, which are essential to many national defense electronic systems.

Let me now talk briefly about the requirements for advanced manufacturing. Advanced manufacturing success has four basic elements: scientific discovery; the ability to translate new science into prototypes and new processes; standards and tests to control quality; and a well-trained workforce.

Because private actors can't capture all the benefits of investing in these requirements—it is hard, for example, to keep scientific ideas secret, or to prevent well-trained workers from going elsewhere—the level of investment in each of these can be insufficient. When there are public goods obstacles of this kind, policy can help to overcome them.

In the 1990s, for example, SEMATECH, an industry-government consortium, helped to develop semiconductor manufacturing proc-

esses and novel measuring techniques. These collaborations helped maintain industry competitiveness.

Let me now say something about the need for effective industrial policy. With the major exceptions of support for basic scientific research and defense-related investments by DARPA and other agencies, domestic policy has not systematically focused on manufacturing in recent decades. Given the challenges facing U.S. industry, this neglect has not been benign.

It is, therefore, encouraging that several pieces of legislation passed in the last Congress include important industrial policy measures. The bipartisan investment—the Bipartisan Infrastructure Act is a major step in restoring and upgrading basic public infrastructure. The CHIPS Act provides substantial new support for basic scientific research in strategic areas, public and private partnerships with industry, STEM education and workforce training, and standard-setting by NIST. The Inflation Reduction Act provides important incentives for private investment in clean energy and climate-related production over the next decade.

Taken together, these three bills provide support for public goods and create private-sector incentives that will strengthen our manufacturing competitiveness and national security.

In conclusion, it is reasonable to say that a competitive advanced manufacturing sector delivers important economic and security benefits. It is also reasonable to say that U.S. manufacturing is more likely to stay on a competitive frontier and to minimize economic and security risks if it is supported by effective industrial policy. These facts make industrial policy a crucial area for future action.

Thank you for your attention. I would be happy to answer any questions you may have.

[The prepared statement of Mr. Jarsulic follows:]

Building U.S. Manufacturing Competitiveness

Testimony before the U.S. House of Representatives
Subcommittee on Innovation, Data and Commerce

Marc Jarsulic
Senior Fellow and Chief Economist
Center for American Progress

Wednesday, February 1, 2023

Thank you, Chairman Bilrakis and Ranking Member Schakowsky, for the opportunity to testify on this important topic. I am a Senior Fellow and Chief Economist at the Center for American Progress. Today, I will attempt to outline the importance of a strong manufacturing sector for both economic competitiveness and national security, and the need for effective industrial policy in reaching both those goals.

The importance of manufacturing for competitiveness and security

Manufacturing has historically been a source of productivity growth and high wage employment. Much of manufacturing productivity growth has derived from innovation – adoption of new technologies rather than merely adding more capital equipment per unit of labor. The ability of many U.S. manufacturers to operate at the technological frontier has made U.S. manufactured goods competitive internationally, and until recently the U.S. was the world's largest manufacturing exporter.

While in the aggregate much of U.S. manufacturing productivity remains at frontier levels, the competitive lead has been eroded. For example, between 1995-2004 U.S. manufacturing productivity growth was higher than that of Germany, a major advanced economy manufacturing competitor. But during recent decades labor productivity growth rates in the

German economy have converged with ours.[1] In addition, German manufacturing total factor productivity (TFP) growth – the fraction of output growth which is not attributable to increased inputs to production, and which is commonly used as a measure of innovation [2] -- exceeded that of the U.S. and was more or less evenly distributed across all manufacturing sectors. [3]

U.S. manufacturing has also been challenged by the rise of China as a competitor. China has overtaken the U.S. as the world's leader in manufacturing value added, and leads the U.S. in manufacturing exports.[4] Millions of domestic manufacturing jobs were lost to the "China shock" beginning in 2000, as domestic Chinese firms entered the U.S. market as competitors, and as an increasing share of U.S. manufacturing employment was off-shored to China and elsewhere by U.S. multinationals.[5]

In addition, in 2015 the Chinese government announced a program called "China 2025", which has the goal of rapidly developing capacity in ten high-tech industries. They include artificial intelligence, advanced robotics, energy saving vehicles, and biopharma. The stated goal of the plan is to significantly improve manufacturing quality, productivity and innovation, and by

---

[1] Martin Neil Baily, Barry Bosworth, and Siddhi Doshi, "Productivity comparisons: Lessons from Japan, the United States and Germany", Brookings Institution, January 2020, p. 11, available at https://www.brookings.edu/wp-content/uploads/2020/01/ES-1.30.20-BailyBosworthDoshi.pdf.

[2] See Robert Shackleton, Total Factor Productivity Growth in Historical Perspective, Congressional Budget Office working paper, available at https://www.semanticscholar.org/paper/Total-Factor-Productivity-Growth-in-Historical-Shackleton/b436d848641fd396e13094d3327255cb777348cd.

[3] Baily et al., op. cit, pp. 35-36.

[4] Marc Levinson, "U.S. Manufacturing in International Perspective," Congressional Research Service, February 21, 2018, p.2, available at https://fas.org/sgp/crs/misc/R42135.pdf; World Trade Organization, World Trade Statistical Review 2022, Table A17, available at https://www.wto.org/english/res_e/booksp_e/wtsr_2022_c5_e.pdf.

[5] David Autor, David Dorn, and Gordon H. Hanson, "The China Shock: Learning from Labor-Market Adjustment to Large Changes in Trade," *Annual Review of Economics* 8 (2016): 223, available at http://www.ddorn.net/papers/Autor-Dorn-Hanson-ChinaShock.pdf; Daron Acemoglu and others, "Import Competition and the Great US Employment Sag of the 2000s," *Journal of Labor Economics* 34 (S1, Part 2) (2016): S141–S198, available at https://economics.mit.edu/files/11560; Christoph E. Boehm, Aaron Flaaen, and Nitya Pandalai-Nayar, "Multinationals, Offshoring and the Decline of U.S. Manufacturing", (Cambridge, MA: National Bureau of Economic Research, 2019), available at https://www.nber.org/papers/w25824.

2049 have the leading global position in advanced manufacturing.[6] The tools used to achieve these goals include subsidies, investments in foreign companies to obtain technology, and technology acquisition via joint venture requirements for foreign firms operating in China. The success of this effort is yet to be determined, but the government commitment and scale of resources available for the effort appear formidable.

These challenges to U.S. leadership in advanced manufacturing create both economic and security risks. Under the existing global division of labor in semiconductor production, both kinds of risk are substantial. The U.S. is dominant in semiconductor design, but has a relatively small and declining share of chip fabrication. Taiwan holds the dominant position in fabrication, operating leading-edge chip "foundries" that produce to customer specifications. Assembly, testing and packaging of semiconductors into finished components is done predominantly by contract manufacturers in Taiwan and China. This means that important elements of the semiconductor supply chain are subject to events in other countries, and, in the case of firms located in Taiwan and China, to Chinese government interference.

The reduction in domestic auto production, caused by chip shortages, over the past two years illustrates the economic risks posed by disruptions to semiconductor supply chains. Security risks are illustrated by DoD's ongoing reliance on Asian producers of micro-printed circuit boards (micro-PrCB's), which are essential to many national defense electronic systems. The economics of commercial micro-PrCB production have located it mostly outside the U.S.,

[6] China 2025 is described in James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade," Council on Foreign Relations, May 13, 2019, available at https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade; and in Karen M. Sutter, " 'Made in China 2025' Industrial Policies: Issues for Congress, Congressional Research Service, August 11, 2020, available at https://fas.org/sgp/crs/row/IF10964.pdf.

and foreign producers are developing technical and cost advantages that force DoD to depend on them.[7]

The geography of semiconductor production has been heavily influenced by foreign government interventions. Taiwan, for example, provides subsidies for land, construction, and manufacturing equipment that lowers fabrication costs by 25-30 percent. China has provided a single firm, Yangtze Memory Technology, with $24B in subsidies, has allocated $100B in support for 60 new manufacturing facilities, and its Integrated Circuit Investment Fund has provided $21B in capital to firms producing semiconductor manufacturing equipment, with an additional $29B on the way.[8]

Requirements for frontier-level advanced manufacturing

Advanced manufacturing is based on scientific discovery, the translation of discoveries into prototype products and production processes, adequate standards and tests to control quality, and a well-trained workforce. Because private actors cannot capture all the benefits of investing in these prerequisites – it is hard, for example to keep scientific ideas secret, or prevent well-trained workers from leaving for other employment – the level of investment in each of them is insufficient. In addition, uncertain demand sometimes acts as a barrier to needed manufacturing innovation.

- **Basic science, proof of concept, and standards**

It is widely recognized that public support for basic scientific research contributes significantly to U.S. economic success, in advanced manufacturing and other sectors. However,

[7] Department of Defense, *FY2019 Industrial Capabilities Report to Congress*, pp. 105-106, available at https://www.businessdefense.gov/Portals/51/Documents/Resources/USA000954-20%20RPT%20Subj%20FY19%20ICR%2007092020.pdf?ver=2020-07-10-124452-180.
[8] https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf.

the recognition of the public good benefits of basic science is often linked to a simplified picture, in which the discoveries of basic science are handed off to manufacturers, who do applied research and development to produce commercial products. This schematic misses two intervening steps which have public good characteristics:

> "One is "proof-of-concept research" to establish broad "technology platforms" that can then be used as a basis for developing actual products. The second is a technical infrastructure of "infratechnologies" that include the analytical tools and standards needed for measuring and classifying the components of the new technology; metrics and methods for determining the adequacy of the multiple performance attributes of the technology; and the interfaces among hardware and software components that must work together for a complex product to perform as specified. If the public–private dynamics are not properly aligned to encourage proof-of-concept research and needed infratechnologies, then promising advances in basic science can easily fall into a "valley of death" and fail to evolve into modern advanced manufacturing technologies that are ready for the marketplace. Each major technology has a degree of uniqueness that demands government support sufficiently sophisticated to allow efficient adaptation to the needs of its particular industry, whether semiconductors, pharmaceuticals, computers, communications equipment, medical equipment, or some other technology-based industry." [9]

The relatively slow development of biopharmaceuticals, after significant NIH investment in life-science research, has been attributed to the absence of a well-developed proof of concept technology platform.[10]

- **Workforce development**

In addition to scientists and engineers, advanced manufacturing requires a well-trained, flexible industrial workforce. The National Research Council has recognized this. They have pointed out that the success of German manufacturing relies on the country's "dual system" of vocational training, in which students engage in academic training for practical work, while

[9] Gregory Tassey, "Competing in Advanced Manufacturing: The Need for Improved Growth Models and Policies," *Journal of Economic Perspectives,* Volume 28, Number 1, Winter 2014, pp. 27-48, available at https://www.aeaweb.org/articles?id=10.1257/jep.28.1.27; *see also*, William B. Bonvillian and Peter L. Singer, *Advanced Manufacturing*, (Cambridge: MIT Press, 2017).
[10] Tassey, op. cit., p. 38.

simultaneously receiving training in apprenticeship programs run by firms or public institutes.[11] This commitment to workforce training provides industry with highly skilled workers who can adapt to changing production processes. It also provides workers with recognized credentials, which give them mobility and bargaining power with their employers. These credentials, together with extensive union representation, and mandatory works councils and worker representation on corporate boards, help to deliver the high real wages paid to German manufacturing workers.[12]

- **Demand certainty**

Uncertain demand also can inhibit manufacturing innovation. It is, for example, recognized that the scale of demand is a key limitation on manufacturing innovation in the U.S. defense sector. Although great amounts of money are spent on defense overall, manufacturers outside the defense sector have limited incentive to innovate products that might have defense applications. Relative to commercial products, the defense market can be small.

To address the demand problem, the DoD at times works to find ways to introduce defense-important technology into commercial applications. For example, in the 1990's DARPA successfully funded research and development in optoelectronics. However, in order to stimulate continued private sector development of the technology, DARPA funded two private-public partnerships that had the goal of establishing commercial fiber-optic networks. These efforts contributed to subsequent broad commercial adoption of fiber optics.[13]

---

[11] National Research Council. *21st Century Manufacturing: The Role of the Manufacturing Extension Partnership Program*. (Washington, DC: The National Academies Press, 2013), p. 230, available at https://doi.org/10.17226/18448.

[12] See David Madland, "The Future of Worker Voice and Power", Center for American Progress, October. 2016, available at https://cdn.americanprogress.org/wp-content/uploads/2016/10/06051753/WorkerVoice2.pdf?_ga=2.133094987.43744973.1612982836-685557270.1612982836.

[13] Potomac Institute, "Consortia Analysis and Recommendations Trade Study", December 2017, p. 15, available at https://potomacinstitute.org/images/studies/CARTSsm.pdf.

Demand certainty, on the other hand, has facilitated important manufacturing innovation. A salient example is presented by the development of the world solar photovoltaic panel (PV) industry. Until the late 1990's there was no mass market for PV's, there was limited production capacity for what was a niche product, and the cost of PV power was high. However, the decisions by the governments of Japan, Germany and Spain to subsidize the adoption of solar power created a surge in demand for solar panels.[14] Because the demand could not be met by existing PV companies, an opening was created for new entrants.

In the early 2000's several Chinese start-up companies entered the PV market, and now account for well over half of all PV's produced in the world.[15] Because of continuing technical improvements and scale economies in production, the cost of solar power has decreased dramatically, and some solar power is now competitive with other sources of electricity.[16]

The need for industrial policy

With the major exceptions of support for basic scientific research, and defense-related interventions by DARPA and other agencies, domestic policy has not systematically focused on manufacturing in recent decades. Given the challenges facing U.S. industry, and the pervasive public-goods obstacles to required investment, this neglect has been anything but benign. It is therefore remarkable and encouraging that several pieces of legislation passed in the 117th Congress represent important advances in industrial policy.

---

[14] Christian Binz and Laura Diaz Anadon, "Unrelated diversification in latecomer contexts: Emergence of the Chinese solar photovoltaics industry," *Environmental Innovation and Societal Transitions*, Vol. 28, 2018, p. 25, available at https://doi.org/10.1016/j.eist.2018.03.005.

[15] "The Solar-Powered Future is Being Assembled in China," Bloomberg News, September 14, 2020, available at https://www.bloomberg.com/features/2020-china-solar-giant-longi/.

[16] *See* Lazard, "Levelized Cost of Energy, Version 14.0", available at https://www.lazard.com/perspective/levelized-cost-of-energy-and-levelized-cost-of-storage-2020/.

The Infrastructure Investment and Jobs Act (IIJA) is a major step in restoring and upgrading basic public infrastructure, crucial to the daily lives of Americans, and to the efficient operation of manufacturing and other businesses. In addition to reauthorizing existing programs, the IIJA provides $284 billion over five years to improve the surface transportation network – roads and bridges, passenger and freight rail, airports, ports and waterways, public transit, and electric vehicle infrastructure, buses and transit. It includes an additional $266 billion over five years for core infrastructure -- power, water, broadband, environmental resilience, and environmental remediation.[17]

The CHIPS and Science Act provides substantial new support for basic scientific research in strategic areas, public-private partnerships with industry, and workforce training. It includes $200 billion to support STEM education, research and development, and workforce development through the NSF and Departments of Energy and Commerce. An additional $53 billion supports semiconductor manufacturing, R&D, and workforce development. There are $24 billion in tax credits for chip production, including support for National Institute of Standards and Technology.[18]

The Inflation Reduction Act (IRA) provides important incentives for private investment in clean energy and climate-related production over the next decade. Manufacturers will receive about $48 billion in tax incentives, which will include production of batteries and the critical minerals they require, and solar and wind energy components. Demand for electric vehicle production will be supported by about $43 billion in consumer tax incentives. In addition, IRA's

[17] McKinsey & Company, "The U.S. Bipartisan Infrastructure Law: Breaking it Down", November 12, 2021, available at https://www.mckinsey.com/industries/public-and-social-sector/our-insights/the-us-bipartisan-infrastructure-law-breaking-it-down; *see also* Brookings Institution, "Breaking Down the Infrastructure and Jobs Act", available at https://www.brookings.edu/interactives/brookings-federal-infrastructure-hub/.
[18] McKinsey & Company, "The CHIPS and Science Act: Here's What's in It", October 4, 2022, available at https://www.mckinsey.com/industries/public-and-social-sector/our-insights/the-chips-and-science-act-heres-whats-in-it.

large investment in green power will provide long-term benefits to manufacturing, other businesses, and households generally.[19]

Taken together, these three bills provide both public goods and private sector incentives that will strengthen our manufacturing competitiveness and national security. They will upgrade basic infrastructure, support basic science and its commercialization in strategic areas, and provide significant new support for workforce development. They also support investment and demand for climate-related manufacturing, which is needed to address the issue of climate change.

Conclusion

Competitiveness in advanced manufacturing delivers important benefits. It is a source of productivity growth and higher-wage employment. It also limits national security risks that arise when we lack access to frontier technology or lack dependable sources for important manufactured products.

At the moment our manufacturing sector faces important challenges. While in the aggregate much of U.S. manufacturing productivity remains at frontier levels, the competitive lead has been eroded. Productivity in other advanced economy competitors is converging to ours. U.S. manufacturing has also been challenged by competition from China – it has overtaken the U.S. as the world's leader in manufacturing value added, and leads the U.S. in manufacturing exports. In addition, the Chinese government is devoting considerable resources to move ahead in crucial areas such as artificial intelligence, advanced robotics, energy saving vehicles, and biopharma.

[19] McKinsey & Company, "The Inflation Reduction Act: Here's What's In It", October 24, 2022, available at https://www.mckinsey.com/industries/public-and-social-sector/our-insights/the-inflation-reduction-act-heres-whats-in-it.

To meet these challenges we need the help of effective industrial policy – one that supports basic science, applied research and development to invent prototypes and production processes, adequate standards and tests to control quality, and an extraordinarily well-trained workforce. We are fortunate that Congress has taken steps to meet these important policy needs.

Summary

- **The importance of manufacturing for competitiveness and security**

Competitiveness in advanced manufacturing delivers important benefits. It is a source of productivity growth and higher-wage employment. It also limits national security risks that arise when we lack access to frontier technology or lack dependable sources for important manufactured products.

- **Requirements for frontier-level advanced manufacturing**

At the moment our manufacturing sector faces important challenges. While in the aggregate much of U.S. manufacturing productivity remains at frontier levels, the competitive lead has been eroded. Productivity in other advanced economy competitors is converging to ours. U.S. manufacturing has also been challenged by competition from China – it has overtaken the U.S. as the world's leader in manufacturing value added, and leads the U.S. in manufacturing exports. In addition, the Chinese government is devoting considerable resources to move ahead in crucial areas such as artificial intelligence, advanced robotics, energy saving vehicles, and biopharma.

- **The need for industrial policy**

To meet these challenges we need the help of effective industrial policy – one that supports basic science, applied research and development to invent prototypes and production processes, adequate standards and tests to control quality, and an extraordinarily well-trained workforce. We are fortunate that Congress has taken steps – through IIJA, CHIPS, and IRS -- to meet these important policy needs.

Mr. BILIRAKIS. Thank you very much. I want to thank the witnesses for sticking to the 5 minutes—or under the 5 minutes. Good timing.

OK. Now we will recognize Ms. Sacks for her 5 minutes of testimony. Thank you.

STATEMENT OF SAMM SACKS

Ms. SACKS. Chairman Bilirakis, Ranking Member Schakowsky, thank you for the opportunity to testify today. I am a senior fellow at Yale Law School's Paul Tsai China Center and at New America. I am also a senior fellow for China with the Cross Border Data Forum. And I advise U.S. corporate clients on China's technology policies. I have been an analyst and a linguist focused on Chinese data and cybersecurity policies for over a decade.

While my expertise focuses on China, my view is that the most effective solution for strengthening U.S. competitiveness and leadership in governing emerging technologies requires an approach that is more comprehensive than our response to any single country.

Passing Federal privacy law that addresses how all companies collect, transfer, and process data will enhance competition while also addressing harms regardless of where that risk originates. U.S. lawmakers have an opportunity here to both address transnational threats while also advancing a more secure, ethical, and democratic global internet in its own right.

The Chinese leadership has embarked on an ambitious national data strategy with the goal of acquiring, collecting, and extracting value from large volumes of data. My written testimony provides more details on this issue. Beijing could use data collected and aggregated from overseas to build profiles of individuals with national security clearances or those with access to critical infrastructure, enabling the manipulation, coercion, and blackmail.

Now, for most Americans this is probably not going to be a top concern. But I do think that the impact on economic competition and U.S. global leadership in emerging technologies may be far more reaching. Access to data collected abroad provides Chinese companies insights into population and consumer behavior, risk tolerance, and other preferences. This helps to strengthen the competitiveness of Chinese firms by enabling them to develop products and services that are better tailored to markets beyond China. And it enhances the ability of those firms to then compete with U.S. companies. I am talking about markets beyond the United States or China, as both Beijing and Washington increasingly look to decouple from one another's markets.

The most significant step that U.S. lawmakers can take to strengthen U.S. global competitiveness, while also enhancing consumer privacy and addressing these pressing national security risks, is to pass comprehensive Federal privacy law. The goal is to address all harms related to data processing and to focus on securing the data itself, rather than a country of origin or any single company. Inaction by the United States means ceding leadership to Europe and to China in setting these global norms and standards.

In addition, the United States should work with like-minded governments to develop a common set of standards that would allow

data to flow. I would like to note the potential for the Global Cross Border Privacy Rules, a data transfer alliance that requires companies to certify to common standards for privacy protection while enabling cross-border transfers for those certified companies.

What this does is it creates a coalition of allies that are sharing data with the United States. The ability of U.S. firms to maintain high rates of innovation depends on access to global markets, to international data sets, and to talent. If U.S. firms cannot send data out of countries in which they operate overseas, this directly impacts economic growth and innovation and AI that is core to building applications that work across a variety of demographics.

I urge U.S. lawmakers to address national security risks and protect Americans' privacy by putting forward an affirmative vision for U.S. data governance. ADPPA marks an important step in this regard that merits further attention and discussion. Inaction will only make the United States less secure, less prosperous, less powerful, while allowing more space around the world for the CCP to set the rules and norms for technologies that will shape the future.

Thank you.

[The prepared statement of Ms. Sacks follows:]

TESTIMONY OF SAMM SACKS
Hearing: "How America Competes to Win the Future Versus China"
House Energy & Commerce Subcommittee on Innovation, Data, and Commerce

February 1, 2023

Chairman Bilirakis, Ranking Member Schakowsky, Chair Rodgers, Ranking Member Pallone, 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 at New America's International Security Program. I also am a Senior Fellow for China with the Cross Border Data Forum, a non-profit group that addresses international data transfer policy issues. 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 technology competition with China, particularly in the context of global cross-border data flows.

While my expertise focuses on China, my view is that the most effective solutions for strengthening U.S. competitiveness and U.S. leadership in governing emerging technologies requires an approach that is more comprehensive than our response to any single country. Some of these challenges do require tools that are specific to risks posed by China, but these policy challenges are bigger than China. Passing comprehensive federal privacy law that addresses how all companies collect, transfer, and process data will enhance competition while also addressing harms regardless of where risk

originates. 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 Evolving Data Regime

Data as a Strategic Asset

The Chinese leadership has embarked on an ambitious national data strategy with the goal of acquiring, controlling, and extracting value from large volumes of data. My previous testimonies provide further details about China's approach, including 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:

- 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

[1] https://www.finance.senate.gov/download/12072021-sacks-testimony; https://www.judiciary.senate.gov/meetings/protecting-americans-private-information-from-hostile-foreign-powers; https://www.judiciary.senate.gov/download/sacks-testimony. For further readings on China's data laws and policies, please see: Jamie Horsley, "How Will China's Privacy Law Apply to the State?" https://www.newamerica.org/cybersecurity-initiative/digichina/blog/how-will-chinas-privacy-law-apply-to-the-chinese-state/ and additional resources available by DigiChina Project, Stanford Cyber Policy Center, 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.

the 14th Five-Year plan called for "improving the market of data factors" (健全数据要素市场), and stressing the need to unlock the value of data to fuel the digital economy.[4]

- On November 30th of 2021, 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 & 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. (建立数据资源产权、交易流通、跨境传输和安全等基础制度和标准规范) 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] These data silos may be less of a

[4] Sina Online, "What Is the Meaning of the '14th Five-Year Plan' Outline (Draft) to Improve the Market of Data Elements? ("十四五"规划纲要【草案】提出健全数据要素市场有何深意)," March 5, 2021, https://finance.sina.com.cn/china/2021-03-05/doc-ikftssaq1688850.shtml.
[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

problem for data sharing than in the past, however, given the way that datasets were integrated to form the basis for the system of health apps used for COVID control.[6] Platforms aggregated information from multiple sources and across localities, including: the state-owned telecom companies, vaccination and testing from National Health Commission, and public transportation sources, and other government platforms containing public records.

Automotive Data

Beijing has also prioritized certain data-intensive sectors slated for greater state support and policy focus. The auto industry was among the first to be targeted by the Cyberspace Administration of China (CAC) for stricter data regulations.[7] The "Regulations on Management of Automotive Industry Data Security" (took effect October 2021) outline which types of data collected by smart cars are designated as belonging to categories that are subject to increased security protections. The regulations lay out obligations for handling different types of data collected or generated by the vehicle—including about the surrounding environment, drivers and passengers, and infrastructure—which is of use for entities ranging from manufacturers to Internet platforms.

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] Mia Zhong, "China's COVID Apps: A Primer," *DigiChina,* https://digichina.stanford.edu/work/chinas-covid-apps-a-primer/.

[7] Samm Sacks, Kendra Shaefer, Xiaomeng Lu, "With Auto Data, China Buckles In for Security and Opens Up for Future Tech," *DigiChina,* https://digichina.stanford.edu/work/with-auto-data-china-buckles-in-for-security-and-opens-up-for-future-tech/.

My assessment is that foreign automakers would have more difficulty gaining approvals for arrangements that would allow them to gather data from cars on Chinese roads and incorporate it into R&D efforts conducted outside China. For instance, two weeks after the auto data provisions were released, Tesla announced that all data generated by vehicles sold in China will be stored locally.

Driving the regulation is a recognition by China's leadership that automotive data holds significant economic value and creates security and privacy risks. It also illustrates the ways in which the Chinese government is moving forward in articulating a vision for how to control and manage data at a granular level, sector-specific level.

Risks to the United States

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 economic asset? It is important to distinguish national security and economic competitiveness risk.

From a national security perspective, potentially the concerning uses of aggregated data by the Chinese government would primarily impact only individuals with national security clearances or with access to critical infrastructure. 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 cyber attack on Marriott hotels

covering roughly 400 million records; and credit data from Equifax on roughly 145 million people.[8] 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.

The impact on economic competition between the United States and China may be potentially more significant, however. Access to large datasets collected abroad provides also Chinese companies insight into population-level and individual consumer behavior, risk-tolerance, and other preferences. This helps to strengthen the economic competitiveness of Chinese firms by enabling them to develop AI applications that better serve diverse demographics in markets around the world. Better tailored AI products and services strengthens the ability of Chinese firms to compete for market share with U.S. firms. The competition is playing out less in each other's countries, as Beijing and Washington pursue economic decoupling policies, but increasingly in other parts of the world from Europe to the Asia, where the competition for market share is increasing. Chinese firms access to more data for AI training models will provide fuel as AI and Quantum become differentiators for the 21st century and beyond.

Recommendations

The most significant step U.S. lawmakers can take to strengthen U.S. global competitiveness and enhance privacy protections is to pass comprehensive federal privacy law (American Data Privacy

[8] "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.

and Protection Act) to address the harms outcomes of all data processing, regardless of country of origin. Setting high standards on what data can be collected and retained by all companies will help protect U.S. personal and other sensitive data. Inaction by the United States means ceding leadership and influence in setting international standards to both Europe and China.

Bans on Chinese software applications are not an effective way to secure Americans' data. Even if TikTok were American-owned, for example, it and its competitors could still legally sell data openly to data brokers that could transmit it to China's security services. As a result, 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.

In addition, 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 in the Osaka Track of the G-20.[9] A multilateral approach should be based on creating a system of incentives for compliance. The objective would be to establish an interoperable data framework encouraging other countries in the world to set similar but not identical standards. 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 protection. The Organization for Economic Cooperation and Development (OECD) privacy guidelines, for example, could serve as a reference in creating a baseline for commercial data flows.[10] The OECD Declaration on Government Access to Personal Data held by Private Sector Entities

[9] 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/.
[10] "The OECD Privacy Framework," Organisation for Economic Co-operation and Development, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

on is an important step.[11]

I'd also like to note the potential for the Global Cross Border Privacy Rules Forum, a data transfer alliance that requires companies to certify to common standards for privacy protection and enables cross-border transfers for those certified companies. This U.S.-backed system offers the potential to address many facets of protecting American data, as it not only takes into consideration the country where data is traveling, but also requires that companies certify to a government-backed standard to be able to transfer data.

Such an approach creates a coalition of allies sharing data with the United States. The ability of U.S. firms to maintain a high rate of innovation depends upon access to global markets, talent, and international datasets. If U.S. firms cannot send data out of countries in which they operate overseas, this directly impacts economic growth and AI innovation that are core to building applications that work across a variety of different geographies, languages, cultures, and demographics. As the technology competition between the United States and China increasingly plays out less in each other's countries than in third countries around the world, data will fuel U.S. technological leadership that is vital to playing offense.

Technical measures to ensure that data is collected in a privacy protective way also should be part of the solution. Congress and the Administration should work with American companies to create incentives to develop privacy preserving technologies— which allow for computing on data without seeing it—and implement them in an open-source way available to everyone. Federated learning

[11] https://www.oecd.org/newsroom/landmark-agreement-adopted-on-safeguarding-privacy-in-law-enforcement-and-national-security-data-access.htm.

(which keeps the raw training data on the device) and differential privacy (providing data anonymization) are two examples. American companies are right now leading the global conversation on privacy preserving technologies and investment in these technologies by the government will enable companies of any size to implement these technological innovations.

Conclusions

I urge U.S. lawmakers to address national security risks by putting forward an affirmative vision for U.S. data governance. ADPPA marks an important step in this regard that merits further attention and discussion. Inaction will make United States less secure, less prosperous, and less powerful, and allow more space around the world for CCP to set the rules and norms for technologies that will shape the future.

Mr. BILIRAKIS. I appreciate it very much. Next is Mr. Pugh.
You are recognized for 5 minutes, sir. Thank you.

STATEMENT OF BRANDON J. PUGH

Mr. PUGH. Chairman Bilirakis, Ranking Member Schakowsky, and members of the subcommittee, thank you for considering my testimony and for the invitation to speak at the hearing.

Let me begin by thanking the subcommittee and the members of the entire Energy and Commerce Committee for the time dedicated to developing comprehensive Federal data privacy and security legislation last Congress.

We focus on finding consensus on a comprehensive Federal data privacy and security law in the United States. One key aspect of our ongoing work is the intersection of privacy and security, including how national security and data security should be key drivers in passing a Federal law. Data privacy and security are vital to both consumers and industry. However, such a law is vital to national security. This often under-appreciated aspect is the focus of my testimony. Given the topic of today's hearing, I will focus my analysis on China.

In 2020, the China Task Force found that the Communist Chinese Party has a record of using official government resources and companies with CCP affiliations to compromise the data of people around the world, and that the United States and its allies need to join the effort to secure data from the CCP surveillance state and other malign entities.

These concerns are especially prevalent in China itself, where advanced technology is used to track and monitor their citizens with few, if any, protections. I wish I could say that the concerns raised in 2020 are no longer valid. In fact, it is the opposite: They are worse.

Data can reveal everything from your shopping habits to sensitive parts of your life, like your health and location. This, in the hands of the adversary or malicious actor, can have devastating consequences, especially for vulnerable populations. As one recent example in the Russia-Ukraine War, data can even be amassed to target disinformation campaigns or direct even physical violence toward those in conflict. This is certainly not an isolated capability, and something that the United States should worry about.

It goes without saying that the United States' rivalry with China has taken on a digital nature. And China has been in a race with us in terms of technology for years, from artificial intelligence to military-specific technology. There are ways to help mitigate and reduce these concerns, even though China's collection and use of data will likely never end. A national data privacy and security law—much like the American Data Privacy and Protection Act, also known as ADPPA, last Congress—is the most logical next step. I will explore three main benefits, and how it could address the data collection crisis that my written comments expand on.

First, acting on privacy legislation makes America more competitive. Countries around the world have acted. Even China has privacy laws. Unfortunately, those are more likely to be disingenuous attempts by the Chinese Government to appear concerned about privacy and security than genuine efforts to promote privacy. This

is especially true given the continued surveillance abuses in China and the lack of security for even Chinese citizens' data.

Nevertheless, the United States still lacks a comprehensive privacy law and is becoming an outlier, especially as a country that leads in trade and is looked to as a norm setter. This has led to companies both American and global adopting other frameworks as the default. The lack of a privacy law also does not obligate most foreign companies to follow specific privacy or security rules while operating in the United States. Congress has the opportunity to change this by enacting a law and clearly conveying the United States' position.

Second, many aspects of ADPPA would help mitigate data privacy and security threats. For example, ADPPA contained data minimization principles, which means data should only be collected to the extent it is necessary or proportionate to provide a product or service. In addition to the value this adds to Americans individually in terms of privacy, it helps reduce the amount of data collected and available in the first place.

Other beneficial provisions include a requirement for privacy policies to alert individuals that their data is transferred to select countries like China, and establishing strong data security standards. Preemption is also a beneficial aspect because it creates one standard which would allow for threats from adversaries and bad actors to be dealt with consistently.

Third, data privacy and security legislation has broader impacts. TikTok has continued to raise concerns on a bipartisan basis. Several options exist to address TikTok. But regardless of the path chosen, it is only a partial solution.

First, TikTok is just one application from one country. Not only are there risks from other adversarial countries, there are also other current and future applications that will pose risks.

Second, many software and hardware products that pose risks like connected devices. While a Federal data privacy and security law might not be the full solution to those concerns, it would serve as a way to help reduce what information can be collected, who to share it with, require security, and provide for enforcement, should it be violated.

Failing to act on Federal legislation would ignore the broader risks posed by data, and leave threats from China and other malicious actors unmitigated.

The United States may lag behind other countries by not having a Federal data privacy and security law, but the 118th Congress has the opportunity to chart a path forward.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Pugh follows:]

SUBMITTED STATEMENT OF

BRANDON J. PUGH, ESQ.
POLICY DIRECTOR & RESIDENT SENIOR FELLOW,
CYBERSECURITY & EMERGING THREATS
R STREET INSTITUTE

BEFORE THE

SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON

ECONOMIC DANGER ZONE:
HOW AMERICA COMPETES TO WIN THE FUTURE VERSUS CHINA

FEBRUARY 1, 2023

ECONOMIC DANGER ZONE:
HOW AMERICA COMPETES TO WIN THE FUTURE VERSUS CHINA

STATEMENT SUMMARY

I. A comprehensive data privacy and security law offers benefits to consumers and industry. There is also a strong nexus between privacy and security. Both of these necessitate a privacy law being a priority of the 118th Congress.

II. The Chinese Communist Party (CCP) has a history of widespread data collection on its citizens and individuals worldwide, including Americans. Data in the hands of an adversarial nation-state or a malicious actor can lead to devastating consequences.

III. There are ways to help mitigate and reduce these concerns, even though China's collection and abuse of data is likely never going to end. A national data privacy and security law, like the American Data Privacy and Protection Act (ADPPA) from the 117th Congress, is the most logical next step.

IV. There are multiple benefits of a comprehensive data privacy and security law that could help address the data collection crisis, including: making America more competitive; implementing provisions that help minimize privacy and security threats; and addressing broader concerns around software, hardware and applications with a nexus to China.

Chairman Bilirakis, Ranking Member Schakowsky and members of the Subcommittee:

Thank you for considering my testimony and for the invitation to speak at this hearing. My name is Brandon Pugh and I am the policy director of and resident senior fellow for the Cybersecurity and Emerging Threats team at the R Street Institute, which includes our data privacy and data security portfolio. The R Street Institute is a nonprofit, nonpartisan, public policy research organization, whose mission is to engage in policy research and outreach to promote free markets and limited, effective government.

In addition to leading our team, my personal research focuses on finding consensus on a comprehensive federal data privacy and security law in the United States. We published a report last year in conjunction with the Harvard Kennedy School's Belfer Center to provide recommendations that address some of the most challenging aspects of a federal data privacy and security law.[1] Our research included consultations with over 125 entities of varying ideologies. One key aspect of our ongoing work is the intersection of privacy and security, including how national security and data security should be key drivers in passing a federal law. That is why today's hearing is of special interest to us.

Let me begin by personally thanking the subcommittee and the members of the entire Energy and Commerce Committee for the time dedicated to the American Data Privacy and Protection Act (ADPPA) last Congress. Notably, the leadership of Chairwoman Cathy McMorris Rodgers and Ranking Member Frank Pallone.

[1] Tatyana Bolton et al., "The Path to Reaching Consensus for Federal Data Security and Privacy Legislation," R Street Institute, May 26, 2022. https://www.rstreet.org/2022/05/26/the-path-to-reaching-consensus-for-federal-data-security-and-privacy-legislation.

Data privacy and security are vital to both consumers and industry. Consumers would benefit from a national privacy law by having protections and rights surrounding their data regardless of their state of residence. Unfortunately, only the residents of five states will enjoy any such protections in 2023.[2] Similarly, data privacy and security laws would benefit industry by providing certainty, clarity and uniformity instead of a patchwork of state-level privacy laws.[3] So far, at least 39 states have considered comprehensive privacy laws since 2018, and I expect this to expand.[4]

In addition to the benefits to consumers and industry, such a law is vital to our national security. This often underappreciated aspect of data privacy and security will be the focus of my testimony today. Given the topic of today's hearing, I will focus my analysis on the context of China.

In 2020, the China Task Force found that the Chinese Communist Party (CCP) "has a record of using official government resources and companies with CCP affiliations to compromise the data of people around the world" and that the United States and its allies need to join the "effort to secure data from the CCP's surveillance state and other malign entities."[5] These concerns are especially prevalent in China itself, where advanced technology is used to track and monitor their citizens with few protections.

Similar concerns are echoed by federal government leaders like Federal Bureau of Investigation Director Christopher Wray, who previously said "if you are an American adult, it is

[2] Anokhy Desai, "US State Privacy Legislation Tracker," International Association of Privacy Professionals, Jan. 27, 2023. https://iapp.org/resources/article/us-state-privacy-legislation-tracker.
[3] Tatyna Bolton et al., "Preemption in Federal Data Security and Privacy Legislation," R Street Institute, May 31, 2022. https://www.rstreet.org/2022/05/31/preemption-in-federal-data-security-and-privacy-legislation.
[4] "Privacy Matters in the US States," International Association of Privacy Professionals, Jan. 28, 2023. https://iapp.org/media/pdf/resource_center/infographic_privacy_matters_in_the_us_states.pdf.
[5] Michael McCaul et al., *China Task Force Report*, U.S. House of Representatives, September 2020. https://foreignaffairs.house.gov/wp-content/uploads/2020/11/China-Task-Force-Final-Report-11.6.20.pdf.

more likely than not that China has stolen your personal data."[6] He made even more pointed comments recently, saying that "China's vast hacking program is the world's largest, and they have stolen more Americans' personal and business data than every other nation combined."[7]

I wish I could say that the concerns raised during the 116th Congress are no longer valid. In fact, the opposite is true—it is worse. Data, in general, can reveal everything from your shopping habits to sensitive parts of your life like your health and location. This, in the hands of an adversary or malicious actor, can have devastating consequences, especially for vulnerable populations. Americans are not naïve to this threat. They understand their personal data is not secure, but they believe they are powerless to fix it.[8]

As one recent example in the Russia-Ukraine war highlights, data can even be amassed to target disinformation campaigns or direct even physical violence toward those in conflict.[9] This is certainly not an isolated capability and is an issue that the United States should worry about. Data can even be synthesized to help identify intelligence agents and "stymie U.S. efforts to cultivate sources of information and influence around the world."[10] It goes without saying that the United States' rivalry with China has taken on a digital nature and China has been in a race with us in

---

[6] Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States," Hosting Entity: Hudson Institute, July 7, 2020. https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

[7] Chloe Folmar, "FBI head: China has 'stolen more' US data 'than every other nation combined'," *The Hill*, Nov. 15, 2022. https://thehill.com/policy/cybersecurity/3737251-fbi-head-china-has-stolen-more-us-data-than-every-other-nation-combined.

[8] Brooke Auxier et al., "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," Pew Research Center, Nov. 15, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information.

[9] Jessica Dawson and Brandon Pugh, "Ukraine conflict heightens US military's data privacy vulnerabilities," *Defense News*, April 14, 2022. https://www.defensenews.com/opinion/2022/04/14/ukraine-conflict-heightens-us-militarys-data-privacy-vulnerabilities.

[10] Matt Gimovsky et al., "Congress Needs to Start Caring About Our Privacy as Much as China Does," R Street Institute, June 2021. https://www.rstreet.org/wp-content/uploads/2021/06/RSTREET232.pdf.

terms of technology for years—from artificial intelligence to military-specific technological capabilities.[11]

There are ways to help mitigate and reduce these concerns, even though China's collection and abuse of data will likely never end. A national data privacy and security law, much like the ADPPA from the 117th Congress, is the most logical next step. I will explore its benefits and how it could address the present data collection crisis.

Acting on privacy legislation makes America more competitive.

Countries around the world have acted on privacy legislation, a prime example being the European Union's General Data Protection Regulation (GDPR). Even China has privacy laws like the Personal Information Protection Law (PIPL) and the Data Security Law (DSL), which have led to rights for Chinese citizens and placed restrictions and obligations on foreign companies operating in China. Unfortunately, these are more likely to be disingenuous attempts by the Chinese government to appear concerned about privacy and security, and competitive with the world, than genuine efforts to promote privacy. This is especially true given the continuous surveillance abuses in China and lack of security for even Chinese citizens' data.[12]

Nevertheless, the United States still lacks a comprehensive privacy law and is becoming an outlier, especially as a country that leads in trade and is looked to as a norm setter. This has led to companies, both American and global, adopting other frameworks as the default. The lack of a privacy law also does not obligate foreign companies to follow specific privacy or security rules while operating in the United States (with some exceptions like entities in regulated

[11] Matt Gimovsky et al. https://www.rstreet.org/wp-content/uploads/2021/06/RSTREET232.pdf.
[12] Karen Hao and Rachel Liang, "Vast Cache of Chinese Police Files Offered for Sale in Alleged Hack," *The Wall Street Journal*, July 4, 2022. https://www.wsj.com/articles/vast-cache-of-chinese-police-files-offered-for-sale-in-alleged-hack-11656940488?mod=article_inline.

industries). In recommending a national data privacy and security law, the Cyberspace Solarium Commission summarized the risk well, noting that "in the absence of congressional leadership, these competing frameworks threaten to splinter the digital economy, confuse efforts to secure users' personal data, and imperil the ability of American companies to compete globally."[13]

Congress has the opportunity to change this by enacting a comprehensive law and clearly conveying the United States' position. It is critical that Congress do this instead of relying on or permitting overreaching federal agencies to decide data privacy and security policy on their own. For example, in the absence of congressional action, the Federal Trade Commission (FTC) is attempting to decide key policy questions on areas that would have major impacts on the nation and privacy in its vast 95 question advanced notice of proposed rulemaking (ANPR).[14]

Data privacy and security legislation provisions can help address privacy and security threats.

Many aspects of the ADPPA would help mitigate data privacy and security threats, but I will highlight several benefits for consideration in any future comprehensive privacy law.

Benefit of data minimization.

Data has many beneficial uses and is foundational to technologies that fuel our economy. However, over-collection of data, especially sensitive data, is not uncommon. This data can easily be misused and/or fall into adversarial control like the CCP. The ADPPA included data

[13] *CSC Final Report*, U.S. Cyberspace Solarium Commission, March 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QvjFqFkkf10MxIXJGT4yv/view.
[14] "Comments of the R Street Institute in Response to the Advanced Notice of Proposed Rulemaking," Docket No. R111004, Oct. 12, 2022. https://www.rstreet.org/wp-content/uploads/2022/10/R-Street-Institute-Comments-on-FTCs-ANPR-on-Commercial-Surveillance-and-Data-Security.pdf.

minimization principles, which means data should only be collected to the extent it is necessary or proportionate to provide a product or service, or for a defined permissible purpose. In addition to the value this adds to Americans individually in terms of privacy, it helps reduce the amount of data collected and available in the first place.

There will still be bad actors ignoring this principle, but that is where effective enforcement comes in. Likewise, there will still be entities that pull together publicly available data for malicious purposes, steal data or even purchase it. But steps to minimize it in the first place are beneficial.

Benefit of privacy policies.

An affirmative requirement for privacy policies to alert individuals if their data is transferred or stored in the People's Republic of China, Russia, Iran or North Korea is key. This allows Americans to not only know if this practice is happening, but to make an informed choice about whether they want to engage in the transaction if the data is going to one of those countries. It also promotes transparency by companies, which could even result in a given data transfer not occurring to avoid skepticism from customers.

Benefit of establishing security standards.

Comprehensive legislation should set baseline standards around administrative, technical and physical data security practices to protect data from unauthorized access and acquisition. This provision is essential to ensuring that collected data has safeguards to protect against unauthorized access, whether it be a cyber criminal or nation-state. Equally as important, security provisions should not treat all companies the same, because not all security needs are the same. Practices

should vary based on different factors like entity size, type of data, and cost and availability of tools, among others. Entity size should not always determine requirements, because we have seen small data brokers engage in some of the worst data practices, but it is a factor. Overall, you cannot have privacy without adequate security.

Benefit of strong preemption.

In light of existing state data privacy laws, solving preemption continues to be a roadblock preventing consensus on a federal law. Without a uniform standard across the United States, we would not have a united approach in addressing both privacy and security concerns. The same is true if we do not have a national law at all and states continue to enact laws on an ad hoc basis. For example, one state could require provisions about securing data, but another state might require something completely contradictory or have weaker protections. A citizen's data in one state should not be any less protected than in another. Congress taking the lead on legislation and creating one standard allows for threats from adversaries and bad actors to be dealt with consistently.

Data privacy and security legislation has broader implications.

TikTok has continued to raise concerns on a bipartisan basis. Notably, concerns that user data could be accessed in China and that the platform could be used to spread pro-China propaganda.[15] There are many options for dealing with this, including potential resolution through

[15] Cecilia Kang, "ByteDance Inquiry Finds Employees Obtained User Data of 2 Journalists," *The New York Times*, Dec. 22, 2022. https://www.nytimes.com/2022/12/22/technology/byte-dance-tik-tok-internal-investigation.html#:~:text=%E2%80%9CThis%20new%20development%20reinforces%20serious,Warner%20said.

the Committee on Foreign Investment in the United States (CFIUS) through what is known as "Project Texas," partial bans at the federal and state levels, and a full ban.

Regardless of the path chosen, it is only a partial solution. I say this for two reasons. First, TikTok is just one application from one country. Not only are there risks from other adversarial countries, there are also other current and future applications that will pose risks. Taking a more holistic approach is the key to avoiding potential blind spots. This could entail considering action and review directed at multiple countries and products like some states have proposed in standalone executive orders and directives, including New Jersey.[16] Second, there are many software and hardware products that pose risks like connected devices. For example, there are reports of baby cameras spying on children, electronic locks being remotely opened and robot vacuum cleaners recording people in the bathroom. This has led to some calls for baseline standards and even labels for Internet of Things (IoT) devices, which reflects the National Security Council's current efforts.[17]

While a federal data privacy and security law might not be the full solution, it would serve as a way to help reduce what information can be collected, who it is shared with, require a degree of security, and provide for enforcement should it be violated. Failing to act on federal data privacy and security legislation would ignore the broader risks posed by data and leave threats from China and other malicious actors unmitigated.

[16] Office of Homeland Security and Preparedness, "Joint Circular," State of New Jersey, Jan. 9, 2023. https://nj.gov/infobank/circular/23-01-NJCCIC-OIT-DPP.pdf.
[17] Brandon Pugh, "Is an "energy star label for cyber" the solution to IoT device security and privacy?," R Street Institute, Oct. 21, 2022. https://www.rstreet.org/2022/10/21/is-an-energy-star-label-for-cyber-the-solution-to-iot-device-security-and-privacy.

Conclusion

The United States may lag behind other countries by not having a comprehensive federal data privacy and security law, but the 118th Congress has the opportunity to chart a path forward. This would result in strong benefits to consumers, industry and security. Given competition concerns, increasing threats from adversarial nations and malicious actors, this is more urgent than ever.

Thank you to the Subcommittee on Innovation, Data, and Commerce for holding this hearing. If I can be of any assistance to members of the Committee, please feel free to contact me or my colleagues at the R Street Institute.

Mr. BILIRAKIS. Thank you very much for moving along nicely. I want to thank you for your testimony. I appreciate all the witnesses. We will now move to the question-and-answer portion of the hearing.

I will begin the questioning and recognize myself for 5 minutes. I would like to start with Mr. Farrah.

Congrats again on your new role with AVIA. I hope the broad coalition you have assembled demonstrates the imperative of breaking the deadlock on this lifesaving technology.

To me, the mobility benefits are very important. I was disappointed that last Congress my amendment was blocked from being considered that—it focused specifically on providing a path for AVs to serve those living with disabilities, such as the visually impaired.

I also wanted to recognize John Pare—if you could raise your hand, sir, I would appreciate that—who is with us today from the National Federation of the Blind. Thank you. Welcome, sir.

He and NFB have been tremendous advocates for the living—those living with disabilities, as well as the great benefits that self-driving cars will have—a mode of mobility for the community. So very important. I can tell you that we need them in my congressional district, that is for sure.

I would like to request unanimous consent to enter into the record the amendment and the letter from NFB in support of the amendment I have submitted.

Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mr. BILIRAKIS. Mr. Farrah, can you elaborate on the ability for China to turn the dials up on testing these technologies in contrast with what we have faced here in the United States?

It seems like the CCP can just flip a switch, tell a province they are going to clear it for full AV testing, and race past the U.S., while we delay and argue over small political differences and regulatory approach. If you could, address that.

And how can we instead show the world that America's approach is superior by unleashing American innovation, American innovators such as those flourishing in my home State of Florida and across the United States, please?

Mr. FARRAH. Mr. Bilirakis, thank you very much. Mr. Bilirakis, thank you very much for the question, and thank you very much for highlighting the role that John and the National Federation for the Blind play. I think that mobility for individuals that have physical disadvantages is a key aspect of what it is that our industry is trying to achieve. And I have been fortunate to work closely with John and his organization and hear him talk passionately about the level of independence that AVs would deliver to individuals within his organization.

Relative to your question, sir, I think it is important to note here that we obviously have incredibly different systems from the People's Republic of China in the United States. And while I think it is important to look at China as an important example of a country that has aims to be a leader on autonomous vehicles, by no means do we need to replicate what it is that they are doing in their country.

We, obviously, have been successful in being global innovation leaders for decades in the United States, and we have our own American brand of innovation. And so I think that you all shining a light on this problem is very important, but we also need to make sure we solve this in an American way.

I think that one thing that I do elaborate on in my written testimony is the need for a Federal legislative framework. This is something where we are very eager to work with members of this committee to determine your priorities, but also to do things like address the exemption caps for novel vehicles, address issues with the FAST Act, address issues with the "make inoperative" provision, also look at a lot of NHTSA rulemakings that are going on. And so these are things we are very eager to do, and thank you again for the leadership.

Mr. BILIRAKIS. I appreciate it very much. Thank you. I want to get to Ms. Sacks.

You have just heard my concern, of course, Ms. Sacks, about how China can decide the future of this technology, God forbid. Can you provide some more color and analysis for what happens when we fall behind on technology like this, and what it means to American jobs and supply chains?

This seems to—you know, this—we don't want it to happen again, what happened with Huawei. So if you could expand on your testimony, we would appreciate it very much. And I guess you have got about 35 seconds.

Ms. SACKS. America should lean into our own strengths and having open markets, free expression, and use those strengths to target investments, incentivize R&D in these areas, as well as the governance structures of those. And I am happy to provide more color in written form, because I recognize that we are close on time.

Mr. BILIRAKIS. I now will go to Ms. Schakowsky for her 5 minutes of testimony—excuse me—questions. But it could be testimony, if you like. It is your 5 minutes.

Ms. SCHAKOWSKY. So I am so happy to hear the broad discussions about data privacy. And it has certainly helped us in the past with American competitiveness, globally. But for decades, America—while America did lead the world in technological innovation, we are now seeing that there are threats by our lack of the—of a comprehensive privacy piece of legislation.

So, according to the first page of Ms. Sacks' written testimony, you had a passage about—let's see—about passing—about the importance of passing a comprehensive Federal privacy legislation. And I would just like to—I think, Mr. Pugh, you commented on that.

But I would also ask Mr. Farrah and Mr.—I am sorry, pronouncing your name—what do you feel about the—about privacy legislation and its importance in the conversation that we are having today?

Mr. Farrah.

Mr. FARRAH. Thank you very much for the question. I think that privacy is, obviously, incredibly, incredibly important. Our industry does not have a position on the previous legislation, but insofar as this subcommittee is active in that regard this Congress, we would be eager to work with you and share our views.

Ms. SCHAKOWSKY. As we move forward on autonomous vehicles, I think privacy is going to be a big issue.

Yes, sir.

Mr. PUGH. I would agree that a rational, comprehensive approach to privacy is important. Invasions of privacy have real significance for individuals and households in the U.S. I think that is one of the reasons why the FTC is currently considering rulemaking with respect to online privacy. And I think, as other testimonies make clear—and I think it is pretty well known—that differential access to data within our economy and compared, say, to the Chinese economy has competitive significance, as well. So I think legislation that addresses issues of privacy thoroughly and comprehensively could be incredibly valuable.

Ms. SCHAKOWSKY. And I think on this subcommittee we are so proud that we were able to get almost unanimous support on both sides of the aisle to pass it out of committee. And now we just have to go the next step.

Ms. Sacks, I wanted to ask you—and I think we—and I want to hear more from Mr. Pugh, but—on the issue of minimization, and why that is so important in your presentation.

Ms. SACKS. Thank you. You know, I am not a privacy law expert, so I will defer to others on how specifically to think about that issue. But what I will say is that it is important to keep in mind a balance between two important areas.

One is that the data collected and retained and not secured properly will be vulnerable to all bad actors, whether you are talking about a sophisticated state actor, a data broker, or those that are transferring it openly on the commercial market. You know, Equifax's security flaws were well documented, even though you had a sophisticated hack from China.

At the same time, we also have to keep in mind the balance, right? Because as I mentioned in my testimony, AI depends on access to quality and quantity of data, and U.S. firms need access to that in order to innovate in AI. So certain things like a flashlight app, does it need to collect location data? I would say probably not. And so there need to be guardrails around—the purpose that that data is collected.

In other areas, we need to make sure that we are not being overly restrictive because of the need for AI to use quality and quantity of data. So how do we strike that balance? I think that is an area that very much merits deeper discussion.

Ms. SCHAKOWSKY. Thank you.

Mr. Pugh, did you want to comment on that, on the minimization issue?

Mr. PUGH. Yes, I would be happy to. So data minimization is one of the key reasons why ADPPA or whatever future bill it may be is essential to national security. We are essentially limiting the data that is available in the first place to—as we just heard, we don't want to make it too constrained that we don't have the data necessarily for technology, but making sure we only have the data that is necessary and proportionate, using the bill's language, is so critical, and it helps minimize what could potentially fall in the hands of the Chinese Government.

Ms. SCHAKOWSKY. Mr. Pugh, your testimony mentioned reports of baby cameras spying on children. And I wondered if you would comment on that, there right now is no Federal law that would stop that, even China doing that. And, you know, I think those of us who are parents here and around the country would be very concerned about protecting that data. Did you want to comment on that?

Mr. PUGH. I would be happy to. I think, to your example, Congresswoman, that is a—baby camera spying on babies is definitely a real possibility.

We also see vacuum cleaners mapping out homes. I think those are real concerns that we need to address. And it really ties into the benefits of IoT, or Internet of Things, but also some of the risks.

Mr. BILIRAKIS. Thank you.

Ms. SCHAKOWSKY. My time is up, and I thank you.

Mr. BILIRAKIS. I appreciate it very much. Now I will recognize the chair of the full committee, Mrs. Rodgers, for her 5 minutes.

Mrs. RODGERS. Thank you, Mr. Chairman.

Last year Congress passed legislation to encourage the building of semiconductor chips in the United States. I believe Mr. Pallone references this legislation. And without a doubt, it is critical that we are manufacturing semiconductor chips in the United States.

I just wanted to let people know that I raised with Secretary Raimondo, legislators, and manufacturers themselves that we should be pairing permitting reform with any Federal subsidies to semiconductor manufacturers. Unfortunately, that seemed to fall deaf—on deaf ears. They—really interested in the money.

So now we have manufacturers that are coming to us looking for exemptions from NEPA because the Federal dollars are triggering long and erroneous environmental reviews for them. Now, I wish that they would have been open to those concerns before the legislation passed. So now the largest manufacturers may receive exemptions from the President. I am not so sure about the startups or others across this Nation, and it just highlights the importance.

And I wanted to add to the record without—add to the record an article on Intel's horrible quarter revealed an inventory glut and underused factories.

Mr. BILIRAKIS. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Mrs. RODGERS. So, you know, we—I agree that the NEPA process needs serious reforms, and I hope that the Semiconductor Manufacturers Administration and members of this committee will work with us on bringing commonsense reforms to NEPA so that we can get America back into the business of building things.

The number one barrier to building anything in the United States is the permitting processes. It is the number one barrier to manufacturing, building, doing anything in the United States. So we are going to go to work on that too.

Back to privacy. Back to privacy and the importance of a national data security law. And as has been referenced, we passed the bill out of committee last year, with ADPPA. I believe this is foundational. This is foundational for our global leadership and se-

curing personal information for every American, especially from foreign threats.

So to Ms. Sacks, we know that China has stolen our data, and we know that they are not going to stop. So how do you—would you speak to ADPPA in protecting us from future threats, while also promoting new technologies?

Ms. SACKS. The goal that I think this bill achieves is that it both manages to address the transnational threat, a range of bad actors, but also protects consumers and secures that data here at home.

You know, I have—traditionally, I think that it is not a good idea to look at domestic issues always through a China/national-security-threat lens. And I think skeptics might raise that question. This is a position, however, that I have long advocated, which is if we want to both address bad foreign actors and better enhance privacy protections at home, this is the baseline that we need to do it.

And in terms of fostering innovation, as I have mentioned, U.S. firms need access to global data flows. But how do we do that in a safe, secure, and ethical way? We establish high baselines of—around how the data is collected and transferred and retained. And that is the balance that I think U.S. Federal privacy law needs to strike.

Mrs. RODGERS. Thank you. I wanted to—I referenced the legislation, the America COMPETES Act, that I had worked on in the 116th Congress, and it really was asking—requiring the Department of Commerce to drill down on emerging technologies and give us some recommendations on how we make sure that we are leading on AI, as well as others. Would you—we are still waiting on those recommendations, but would you just speak to what you believe we need to be doing to safeguard our data, while finding a balance to lead on AI?

Ms. SACKS. You know, I think here we play offense and we play defense.

From an offensive perspective, we probably should not think about any single country, but how do we invest and incentivize innovation at home, with a focus on digital infrastructure, fiber optic networks? How do we create better space for U.S. firms to compete overseas?

And cooperation with allies and partners. The EU–U.S. Tech and Trade Council is one area. Working with Japan is another.

I think it is also important to take what has been referred to as a small-yard/high-fence approach. Let's be selective about what we are protecting. Not everything is a national security issue, and in fact, with AI sometimes there is a symbiotic relationship, and it is hard to prevent code from crossing borders. So let's be smart, and use a risk-based approach.

Mrs. RODGERS. Mr. Farrah, I understand you worked for the National Venture Capital Association. I would love to talk to you further and hear more about how you believe the regulatory framework is impacting our market leadership. So anyway, but I ran out of time.

I will yield back.

Mr. BILIRAKIS. I thank the chair, and I will recognize the ranking member of the full committee, Mr. Pallone, for 5 minutes.

Mr. PALLONE. Thank you, Chairman. I want to echo the sentiments of Ranking Member Schakowsky about the need to enact the American Data Privacy and Protection Act, which, of course, is bipartisan with Chairwoman Rodgers and myself.

But I also—I am concerned about, as I said in my opening, what the Republican leadership is planning on with regard to the debt ceiling. You know, they have threatened to leverage the debt limit to enact crippling budget cuts to bedrock American programs.

Experts have warned that defaulting on our Nation's debt obligations—a debt that was amassed during both Democratic and Republican Congresses—could wreak havoc on our financial markets, potentially causing the stock market to plummet and capital markets to freeze.

So let me start with Mr. Jarsulic.

How would defaulting on our national debt affect American competitiveness?

Mr. JARSULIC. So, I think that it is pretty well recognized on the basis of the previous incidents in 2011, 2013, where we came close to hit a debt limit, that the economic consequences can be relatively severe. I think we can expect upward spikes in Treasury rates if the default process went on long enough. There would be a translation of that, those interest rate increases, into mortgages, into consumer credit cost, because those interest rates are based off Treasury rates.

I think we could expect equity market declines. I think we can expect hits to consumer confidence, all of which—demand, slow the economy at a moment when people have concerns about tipping into a recession. That creates a big risk.

In the slightly longer term, repeated run-ups to debt limits and potential of default has already had an effect on the way that the world views Treasury securities. S&P downgraded us from the highest possible rating for sovereign debt, and that downgrade has persisted. If we go through another incident—instance where we actually hit the limit, I think that there is a possibility that, in the long term, foreign investors in Treasury securities will re-evaluate the risk, and they will demand more of a risk premium in order to [inaudible].

So I think that the aggregate demand effects, the long-term cost effects of a default, are really quite significant.

Mr. PALLONE. Well, thank you. Let me ask Mr. Farrah. Your testimony states that we must have a strong capital market to "continue to lead on AV development and deployment." Now, how would defaulting on a national debt and destabilizing the financial sector affect your members' ability to develop and deploy AVs?

Mr. FARRAH. Ranking Member Pallone, thank you very much for the question.

As I write, the capital markets are incredibly important because we have both innovative startup companies that are trying to deploy autonomous technology. We also have larger companies with experience scaling in the transportation sector that are financing a lot of the research that I mentioned and testing that is going on. And so certainly, this is something that is very important to the health of our industry so that we can bring the promise of AVs to your constituents.

That said, we do not have a position as an industry on the default that you mentioned.

Mr. PALLONE. But your testimony also provides several recommendations from DOT that could—that they could adopt to support the deployment of AVs. Would the DOT be better positioned to carry out these recommendations if their budget is dramatically cut?

Mr. FARRAH. The Department of Transportation is a very important partner to us, obviously. That is something that we very much value—the collaboration. We have recommendations that we have put forward to DOT in terms of doing things like updating the Federal Motor Vehicle Safety Standards, and that is an ongoing conversation.

In terms of overall funding levels, that is something—we, obviously, defer to Congress and your judgment as to what those funding levels might be.

Mr. PALLONE. All right.

And, Mr. Jarsulic, how would stringent budget cuts affect our Nation's ability to compete?

Mr. JARSULIC. So really large budget cuts probably will affect the ability of the Federal Government to provide things that are important for the normal functioning of the economy. The Federal expenditure supports healthcare, supports infrastructure, supports scientific research and development. And if those things are compromised, the functioning of the economy is clearly going to be affected.

In addition, large cuts in expenditures will create an immediate shock to demand, and that can have important employment and—effects, as well.

Mr. PALLONE. Thank you.

Thank you, Mr. Chairman.

Mr. WALBERG [presiding]. I thank the ranking member, and now I recognize the gentleman from Indiana, Mr. Bucshon.

Mr. BUCSHON. Thank you, Mr. Chairman. I want to congratulate Mr. Jarsulic for sticking to his talking points on the debt ceiling to help out Chairman Pallone on that narrative. But the reality is we have never defaulted, and it always gets raised.

The other thing I want to point out is that the CHIPS Act was included in a larger bill. We all know this, right? It had many, many policies the Republicans just couldn't support. And, you know, it is disingenuous to say we didn't support the concept. Look, I understand the politics, and this probably won't be the last time we hear that narrative as it goes along this year.

That said, thanks, Chairman Bilirakis, for calling today's important hearing. Ensuring American businesses and innovators can keep our competitive edge against China is an extremely important issue, and we must facilitate U.S. leadership in new technologies and ideas.

One industry in which the U.S. has been a leader but is in danger of being passed internationally, particularly by China, is that of autonomous vehicles. I strongly believe in the potential of this technology. Last Congress, I co-led legislation to study crash avoidance systems to help make AVs safer for all road users, and I led a letter asking NHTSA to update safety standards for AVs, and

continue to advocate—continue advocating for a national regulatory framework for AVs.

So, Ms. Sacks, I have a question for you. I foresee a world in which the Federal Government may eventually procure AVs for certain types of vehicle fleets, and want to be certain that, if that happens, those vehicle fleets are protected from Chinese data collection and storage. Do you have any recommendations on how we could prevent technological vulnerabilities in such AVs or in AVs in general?

Ms. SACKS. I will defer to my colleague, who is an AV expert, but I can speak to the broader question of how we protect the broader tech stack, and I think this is an area that is bigger than China, right? There are best practices for accessing—for assuring hardware security in products, regardless of whether you are talking about a counterfeit, whether you are talking about a component that is made in China. And the same goes for building cybersecurity at the software level, where the U.S. Government does have standards around that.

So again, I would encourage the committee to think about this in—bigger than any single country, and we need to also invest and incentivize it ourselves, and play to our own strengths. But I defer to my AV expert colleague for specific——

Mr. BUCSHON. Yes, I just want to agree with you real quickly—and then we will go on to Mr. Farrah—about not a single-country strategy. We want America to be competitive against our competitors, some of which don't like us and many of which do.

So, Mr. Farrah, do you want to comment on the AV—the cybersecurity and hardware security in AVs?

Mr. FARRAH. I would like to. But first, sir, I would like to thank you for your leadership on autonomous vehicles in previous Congresses, and look forward to the conversation continuing.

I think, from our perspective, cybersecurity is very important. Obviously, our industry is very motivated to make sure that the vehicles are kept safe, that those riding in the vehicles are also kept safe.

And so this is something where there are obviously cyber threats out there. We support a risk-based approach where we can take a comprehensive view and look at how it is that we can best protect American equities. This is something where, obviously, the AV industry would like to be at the table on that. But at the same time, we are not different in many respects. I think there are many in the automotive sector, the technology sector that need to be at the table so we can kind of get a comprehensive approach.

Mr. BUCSHON. Yes, and I would say in the AV space, you know, it is not just foreign actors, that, you know, cybersecurity is critically important because if you just have somebody stand on the side of the road and—hacks into someone's—an AV and diverts it off the road, you know, that is a problem. So this is—you know, this is an issue that we will have to address.

Another possible area where I have some concern is the CCP's improperly accessing America's data through the CCP's new Blockchain-based Service Network, or BSN. BSN has been advertised as a one-stop shop blockchain foundation which others can easily build on top of. While the last few years have shown how

prevalent scams and frauds are in NFTs and other blockchain applications, something our committee must work to address, we cannot allow the CCP or other actors or anyone else to corrupt America's infrastructure once again.

So Ms. Sacks, you have written a lot about protecting America's privacy information from the CCP. What dangers do you see in adopting a CCC-created foundation for blockchains? And can we secure America's information if we allow other actors' components into our tech stack?

And we only have a few seconds, so——

Ms. SACKS. I would be happy to submit some more——

Mr. BUCSHON. That would be great. Thank you very much.

Mr. WALBERG. I thank the gentleman for yielding, and now I recognize the gentlelady from Florida, Representative Castor.

Ms. CASTOR. Thank you, Mr. Chairman. And thanks to our witnesses for your testimony today, and welcome to the new members.

And I do want to say at the outset here at our first hearing it is especially important for this subcommittee to get to work on comprehensive privacy protections sooner rather than later. And I hope this will include the long-overdue protections for children and teens online. Their safety is at risk. They are being constantly surveilled and targeted with ads. It is weighing on them, in addition to all of the fundamental security issues that put them at risk.

But I want to talk a little bit about AVs—EVs, because we are also suffering the costly impacts of the climate crisis. It is—those costs are weighing on our neighbors back home, on farmers, on the Federal budget as extreme events continue to escalate.

But it also provides an important opportunity. The race for cleaner, cheaper energy provides opportunities for American workers and American businesses. The transportation sector is the largest source of greenhouse gas pollution in the United States.

But—and I know Representative Dingell will agree with me that electric cars and trucks offer an innovative solution. We want American companies and workers to win the race for the future, but we are behind right now. That is one of the reasons that we devoted so much attention to—in the Inflation Reduction Act—new incentives for American-built cars and trucks, electric vehicles, and the Bipartisan Infrastructure Law. We dedicated about $7.5 billion for electric vehicle chargers.

So, Mr. Farrah, how do you see that investment going so far for the electric vehicle charging across America, and what are your hopes in that area?

Mr. FARRAH. Thank you very much for the question. I would just note that Florida has been a leader nationwide on AV deployment, and that is something I would love to discuss in greater detail with you.

Relevant to the Inflation Reduction Act, that is something that—our organization was not involved in that legislation, does not have a position specifically on the bill.

I will say, however, that if you look out at the landscape of autonomous vehicles, many of them are electric vehicles, and that is something that will hopefully lead to a generational shift towards electric vehicles. We think we can be of assistance in that regard.

Ms. CASTOR. Are you plugged in to the charging infrastructure, the planning that is going on at DOT and at the State level?

Mr. FARRAH. We can give you an industrywide view of that, to what degree we are plugged in to that. And that is something that I think we value sharing the perspective.

But the final point I would just make is that, even for those AVs that are not electric vehicles, you also have a number of environmental benefits in terms of smoother driving, less idling, the ability to operate at night, and things of that sort.

Ms. CASTOR. Well, we have some challenges, because in 2018 Chinese production accounted for more than half of all lithium battery cell manufacturing capacity and nearly half of all global EV sales, while the United States, we were—EV sales are just really starting to take off.

Congressional Democrats and the Biden administration have really focused on this. And the Inflation Reduction Act is going to provide that relief and those incentives to consumers, and then to the manufacturers, and to the workers.

Mr. Jarsulic, why is it important for the United States to lead the world when it comes to electric vehicles' design, production, and deployment?

Mr. JARSULIC. You know, I think it is pretty clear that because of the risk created by carbon emissions, the world is going to move away from internal combustion engines in autos, trucks, busses. And if our auto companies are going to remain competitive, they are going to have to produce EVs.

There's a lot of employment and output associated with this. The auto industry comprises about 3 percent of GDP. And if the U.S. successfully transitions to the manufacturing of EVs, that kind of employment and income doesn't vanish.

I think it is also important to remember that new techniques are being developed in the production of EVs. And if you want to learn techniques in manufacturing, you have to engage in learning by doing. So the sooner we can make the transition to producing EVs at scale, the sooner our manufacturers can join in that process of learning by doing, and push the frontier forward, and improve their competitive condition.

Ms. CASTOR. We want to win the future. We want to build those EVs in America and supply them to the world, and at the same time create millions of good-paying jobs all across the supply chain. So thank you.

I will yield back.

Mr. WALBERG. I thank the gentlelady, and I certainly agree. We want to lead the world.

I also want to make sure that it is clear that, as our chair indicated, Republicans on this committee are fully committed to passing a comprehensive Federal privacy and data security standard. We are committed to that.

Let me also state before I recognize myself for my 5 minutes that—just to make it clear, and as respectfully as I can—Democrats are the only ones anywhere talking about cuts to Social Security or Medicare or defaulting on the debt. That is clear, what has been stated.

Let me go to my 5 minutes of questioning, and thank you to the panel for being here.

China is actively using U.S. customer data to better develop their artificial intelligence, whether through mining and scraping purchasing data or third parties, or through apps like TikTok sharing information with the Chinese Communist Party.

Mr. Pugh, at a time when Republicans and Democrats agree that AI is a national security economic imperative, shouldn't we be more cognizant of the amount of data we are making available to our adversaries?

And secondly, what steps can we take to prevent U.S. data from being accessed by the CCP?

Mr. PUGH. Well, thank you, Congressman. So data in itself is essential. We need it for our economy and we need it for innovation.

To your point, the issue is when it falls in the hands of adversary nations and malicious actors, which we see happening on a second-by-second basis with China, unfortunately. And that is something that I really implore this Congress to address. And I think the best way to do that is by acting on a comprehensive data privacy and security law today.

Why it would benefit consumers and industry? The security nexus cannot be under—you know, overstated. And what I mean by that is just one aspect. This contains data security provisions. It would require data to be safeguarded. And if that actor chose not to follow that, then there could be enforcement as a result.

Mr. WALBERG. OK. Thank you.

Michigan, my State, is the Motor State. Representative Dingell and I would certainly agree strongly on that. It is the Motor State, and I want it to stay that way—and expand, in fact. But China continues to push forward on autonomous vehicle development and deployment. I think a roadblock to U.S. leadership in this space is consumer comfort, consumer comfort with the whole issue.

I myself have expressed concerns about how autonomous vehicles handle the safety of pedestrians, motorcycles. I am a motorcyclist. I am very concerned that we do this right, and more.

Mr. Farrah, I noticed you didn't use "self-driving," and I thank you. I thank you because there is an auto company, at least one, that has used that, sold cars on it, and they don't self-drive. Driver-assisted, all of that, we are there, and it is working well in most cases. And I think we ought to hold off on using that term, "self driving," for a while until we get it right.

How are your members approaching public education about the safety of autonomous vehicles so that the United States can continue to lead on this important technology?

Mr. FARRAH. Thank you very much, Congressman. I appreciate the question. And thank you for your previous leadership on the SELF DRIVE Act and the dialogue we have had around some of your safety concerns.

Mr. WALBERG. And I hated that title.

Mr. FARRAH. I should note at the outset, though, that we acknowledge that public consideration of autonomous vehicles is very important, and our industry is doing a considerable amount to get out and talk to the American public because your constituents are going to increasingly be seeing these vehicles on the roads, whether

they are delivering groceries, taking them to destinations, trucks driving on the highway. It is important that people understand why these are safer than the alternative. So that is something that we take seriously. We have a number of initiatives that we can talk about in further detail.

I think one issue that I want to address, though, that you got at here is a lot of the confusion around driver-assist technology, as compared to autonomous vehicles.

Mr. WALBERG. Autonomous.

Mr. FARRAH. That is something that is absolutely critical, that people who are in the vehicle understand what they need to be doing. If they are required to perform any aspect of the driving task, they are in a driver-assist vehicle.

Secretary Buttigieg said it very clearly: "If you can buy it in the showroom today, it is not an autonomous vehicle." That is important. Our industry is very clear in the language that we use, and we appreciate your attention.

Mr. WALBERG. And it will give much more comfort as we keep that clear. So thank you.

Today we have smart phones, smart light bulbs, refrigerators, everything. Though these sensors are working to a great degree, we still have challenges. While the United States has been taking steps to remove Huawei and secure our networks that are involved with many of these things, Tuya has slid under the radar.

I have an article by Klon Kitchen and Hal Brands which outlines the dangers Tuya poses that I would like unanimous consent to enter into the record.

Hearing none, it will be entered.

[The information appears at the conclusion of the hearing.]

Mr. WALBERG. Mr. Pugh, how can we secure our network if the smart devices we rely on are compromised by design?

Mr. PUGH. So, Congressman, you are right. This is a critical issue. We rely on IoT devices on a daily basis, and the number of devices by 2030 are supposed to be 29-plus billion.

The issue is we don't have a baseline for our IoT devices. So that is a great starting point, seeing—is there a baseline that these device manufacturers should be meeting?

Secondly, making more of them in America. I have more faith in American companies that do privacy- and security-enhancing things than I do with a CCP-backed company.

Mr. WALBERG. Thank you. I yield back.

I recognize now my good friend and colleague from Michigan, Representative Dingell.

Mrs. DINGELL. Thank you, Mr. Chairman. As my Democratic colleagues have pointed out today, I do believe that we made some steps in the last—Democrats made some progress in enacting serious and significant legislation to strengthen our competitive edge on the world stage. But we all know that there is so much work we need to do to solidify our long-term economic might and define our national competitive advantage with countries like China.

I associate myself with many of the comments that have been already made, and I am very grateful to hear so many people talk about autonomous vehicles and the need to do something, because we don't always hear that.

Electric vehicles are also critical in all of this and further mitigating risks from U.S. supply chains in bringing them back, and I have 5 minutes and could talk for 5 hours or more. But let me move to AVs quickly.

Cutting-edge technologies like autonomous vehicles hold the promise of improving safety, expanding mobility, and strengthening our economy. At the moment—and it is only at the moment, as you and I know—we hold a competitive edge in developing and deploying AVs. According to KPMG, the United States ranks higher in preparedness for AVs than Japan, Germany, and China.

But here is the reality: We have got to preserve and expand this advantage by ensuring that the United States, not countries like China, write the rules of the road for this new transformative technology. That is why I have spent years collaborating with my colleagues and the stakeholders to establish that national framework. I know that, under the Republican leadership with my—we are going to get it done this year, or this Congress. I guess I should be realistic.

But here is our truth: Autonomous vehicles are here, and every day we do not have a Federal framework in place for the safe deployment of AVs, we are risking falling behind the rest of the world. China gets what is at stake. If the United States is going to stay at the forefront of innovation in AV technology, keep those jobs here in this country, not cede leadership to any other country. We have got to get motivated and act.

So, Mr. Farrah, how can lawmakers and regulators lay the foundation for the continued development and deployment of AV technology to ensure the future of this technology stays in the United States?

Mr. FARRAH. Representative Dingell, thank you very much. And I share your passion for AVs, and specifically around the safety and mobility benefits that we have spoken about in the past. And so this is something that I think—we are talking about, literally transforming how it is people and goods move around this world, and that is tremendous.

And so we are very hopeful to work with this subcommittee this Congress, hopefully this year, to pass AV legislation that would set up that framework. There is also, frankly, work that needs to be done at the agencies, as well, in terms of updating a system that is many decades old.

In terms of legislation, there's a number of issues that I detail in my written testimony. A few of them that are worth flagging here is that we have an outdated process as it relates to the exemptions process for so-called novel vehicles, where you—this needs to be updated. This is something that the committee has addressed before on a bipartisan basis.

We also need to make sure that certain rulemakings are ultimately executed on and finished.

And so these are things where we are very committed to doing this, and certainly appreciate the opportunity to work with you and your team.

Mrs. DINGELL. So I have a minute and 30, and I want to get to supply chain. But could you very quickly tell the committee how the absence of the Federal AV framework affected the develop-

ment—is affecting every single day the development, and putting them on the road, of autonomous vehicles?

Mr. FARRAH. Absolutely. I would make two quick points.

I think the first one is that—and I mentioned before the exemptions process. There are U.S. companies that want to be manufacturing these vehicles. They want to be deploying these vehicles. But right now they are limited under this exemptions for novel vehicles to 2,500 vehicles per year for a maximum of 2 years. That is the wrong message for the Federal Government to be sending to companies that want to be producing these companies and ultimately benefiting the United States.

So that is something that I think needs to be addressed, and it needs to be addressed very soon. And so that is something that we can address in legislation, and I appreciate your help.

Mrs. DINGELL. Thank you.

Mr. Chairman, I am down to 33 seconds, sir. I am going to want to put some questions in the record.

But I do want to focus on strengthening the U.S. supply chains. I think most people don't realize how vulnerable we left ourselves from both an economic and national security issue until the COVID–19 public health crisis hit. And we saw that the private sector alone cannot identify, monitor, and address supply chain vulnerabilities.

You know, we are so dependent upon China for the electric vehicles that you are talking about. Most people do not understand. Lithium has gone up $1,500 in the last 6 months, and a battery—EVs are—I mean, we got to develop our supply here. We have got to work on that.

I am a proud author of the Supply Chain Security and Resilience Act. I am going to ask you, Mr. Jarsulic, for the record—and some other questions—what are some best practices to help us improve our Nation's supply chain resilience.

I am over. You are going to have to write the answers to this, what can—there's just so many issues that all of you can answer.

This is the future of our country. Thank you. I yield back the seconds I don't have.

Mr. WALBERG. I thank the gentlelady.

[Audio malfunction.]

Mr. WALBERG. This proves that—I don't know if somebody else has a—yes, that would work better.

So thank you for yielding back. Now I recognize the gentleman from South Carolina.

Mr. DUNCAN. Thank you. Thank you, Mr. Chairman. I wonder if Michigan is the Mitten State or the Motor State. I am confused on that, but——

Mr. WALBERG. It is both.

Mr. DUNCAN. OK. I want to applaud what is going on in South Carolina with BMW, Volvo, and Mercedes, and what they are doing with the EVs, along with other vehicle manufacturing.

[Audio malfunction.]

Mr. DUNCAN. And I apologize for this sound.

But I want to remind my colleagues on the other side of the aisle that we are $31 trillion in debt, and we are spending money that is borrowed. I say that because what is the role of government in

subsidizing our funding these type of things? I point to government spending on Cash for Clunkers. It was a failed program at the initial—on the onset, the Obamacare rollout, the problems that it had.

I believe in innovation at the private-sector level. I think myself that we have more machinery of government than is necessary, too many parasites living on the labor of the industrious.

A government big enough to supply everything you need is big enough to take everything you have. The course of history shows that, as the government grows, liberty decreases. That was a Founding Father, Thomas Jefferson, that quoted that.

Liberty is the liberty to innovate and invent, and capitalize off the profits of that innovation.

I am fascinated with AVs. I think the appropriate initial step is what I see happening in the trucking industry: point-to-point delivery, oftimes at night, with commodities, distribution center to distribution center, maybe local carriers. I think that is a way we can prove that AV works, AV is safe, and I would love to see the innovation within the trucking industry as the future of AVs before we entrust that to the populace to get in an AV that maybe is driverless—I know we are not using that term—in the future. But I do see that as the wave of the future, both in trucking and passenger vehicles.

So I want to shift gears a little bit, and Ms. Sacks, while the U.S. banned Huawei from building 5G infrastructure, Chinese state-owned automotive companies like AutoX and Pony.ai continue to operate pilot programs in the United States with limited oversight. What types of information these companies collect that could pose a national security risk if shared with the foreign adversaries that could exploit such information?

Ms. SACKS. So AV companies collect, like, many different kinds of data. And Mr. Farrah might be able to comment in more depth on what that is. I am not familiar with these specific companies.

I can say, more broadly, from understanding, you know, how the industry works from a data security standpoint, I think that there is not only potentially information about the infrastructure, the mapping, but I would also sort of push back and say, you know, are they collecting information about mapping and streets that is any different from what you might find on Google Maps or that is available openly?

So there are different kinds of data. And so one question might be, what kinds of data are they collecting and what are the—who has access to it? And I would ask that not just for these particular companies of Chinese ownership but any AV company more broadly, and what are the data security practices?

You know, the point that I have made in this hearing repeatedly is that we should focus on—certain kinds of data have different levels of sensitivity. Who has access to it, how is that being secured, rather than necessarily looking at a sort of country of origin or nationality when that data might be openly available on the commercial market in other forms.

Mr. DUNCAN. Yes, I think that is strong.

I am not concerned about this, I am just stating this for the record: Uber already has—if I use an Uber to go to Walmart, they know how many times I went to Walmart or that I ate fast food.

Now, what—who collects that information, how it is shared with others about my traveling habits, my shopping habits, my eating habits? And I think that is a concern of many Americans, what AVs will collect as you travel around.

Mr. Farrah, as a follow-up to that question, it has become abundantly clear that Chinese-owned companies are testing the U.S. and sending information they collect back home. However, if an American company were to test their AVs in China, they would not be able to send that information back home. Is that correct?

Mr. FARRAH. Thank you very much for the question.

First of all, I note—and thank you for the appreciation for AV trucking, which is a very exciting trend line in our industry.

I think that market access overseas is a big concern, generally speaking, for our industry. We want to make sure that, as these companies scale and grow, that they have access to those markets. And so my understanding is that is a huge consideration in a place like China, where we don't have that same level of reciprocity, and I would certainly be happy to dialogue with you and your team further about that.

Mr. DUNCAN. Absolutely. There's going to be a lot of hearings on this type stuff, and I look forward to that conversation.

And with that I yield back.

Mr. BILIRAKIS [presiding]. Thank you. Now the Chair recognizes Representative Blunt Rochester for her 5 minutes.

Ms. BLUNT ROCHESTER. Thank you, Mr. Chairman, and congratulations, as well. And thank you also to Representative Kelly and to the witnesses.

I agree with my Republican colleagues that U.S. economic competition is the issue of the moment. Businesses and working people up and down my State of Delaware report severe supply chain issues that hamper their businesses and livelihoods. U.S. manufacturing has declined in recent decades, and with it so has the resilience of critical supply chains. My colleagues across the aisle are right: U.S. leadership over standards and regulation are important.

But U.S. leadership is just a means, not an end in itself. Ultimately, American families are counting on us to improve their economic opportunities. Talk alone will not create good-paying jobs that American families need. This moment demands all of us come together in a comprehensive, credible, and resourced strategy.

This week my colleagues and I will meet the moment by introducing comprehensive legislation to build resilient supply chains that ensure we can compete with China, Russia, or any adversary that intends to undermine our economic and national security.

I hope my Republican and Democratic colleagues will join me on these bills. These measures invest in the central pillar of the U.S. competitiveness by investing in critical supply chains. They are also endorsed by over 150 businesses and trade associations, including the Information Technology Industry Council, Consumer Brands Association, National Association of Manufacturers, and the Motor Equipment Manufacturers Association.

Mr. Chairman, I ask unanimous consent to insert a letter and its appendix into the record.

Mr. BILIRAKIS. Without objection, so ordered.

[The information appears at the conclusion of the hearing.]

Ms. BLUNT ROCHESTER. This is a transformational policy. And as we saw with ADPPA and with the CHIPS and Science Act, this committee knows transformational policy is necessary to solve the issues hindering economic growth.

Mr. Jarsulic, to reverse the declines in U.S. manufacturing, should we take a whole-of-government and whole-of-economy approach and incentivize reshoring of manufacturing? And does that include investments in production practices and workforce programs?

Mr. JARSULIC. As I indicated in my testimony, competitiveness in manufacturing really is a source of productivity growth, and productivity growth is necessary for growth in wages and profits. We really need that.

And therefore, what you can do—what we can do through policy to strengthen manufacturing and strengthen its competitiveness has real economic importance.

I think that the elements that are in the three acts I talked about, which are designed to overcome obstacles to private investment and to productivity growth in important areas ranging from semiconductors to biopharma, are going to make an enormous contribution. But I think there is much more that can be done.

People who look at advanced manufacturing recognize that, in addition to large corporations who are making investments, those corporations need to have the support of clusters of small and medium-sized enterprises who provide inputs and services to those corporations. And so work that can be done to bring those SMEs to the technical frontier and allow them to participate in advanced manufacturing is really important. There is—a lot of that is embedded especially in the CHIPS Act. More can be done.

Ms. BLUNT ROCHESTER. You mentioned the CHIPS Act and you also mentioned the semiconductors. And I think that is an example of us failing to evolve fast enough. Can you share with us any examples of industries or products that are at risk of falling behind unless we make these significant investments?

Mr. JARSULIC. Well, we have talked a lot about EVs here, and I think it is very clear that some of the inputs necessary for the expansion of that industry really need to be looked at carefully. For example, batteries depend on certain kinds of critical minerals: lithium, cobalt, nickel. And the supplies of those materials are not necessarily available in ways that could be secure or economically viable for us. For example, I think—oh, sorry.

Ms. BLUNT ROCHESTER. Sorry, my time has expired. But I will follow up with you, because I want to follow up on the issue of not just the raw materials, but also there is a report from the Center for Strategic and International Studies that speaks also to our national security risk, as well, which I would also like to enter into the record, Mr. Chairman.

Mr. BILIRAKIS. Very good.

Ms. BLUNT ROCHESTER. Thank you, and I yield back.

Mr. BILIRAKIS. Without objection, so ordered.[1]

[1] The Center for Strategic and International Studies report has been retained in committee files and is available at https://docs.house.gov/meetings/IF/IF17/20230201/115346/HHRG-118-IF17-20230201-SD024.pdf.

Mr. BILIRAKIS. We have my good friend from the great State of Florida, Mr. Dunn, please.

Dr. Dunn.

Mr. DUNN. Thank you. Thank you very much, Mr. Chair. It is a great State too, by the way.

As we are all aware, in December the Chinese Communist Party issued its 14th 5-year plan outlining China's ambitions to become the global leader in the digital economy by 2025. In order to protect our private data and independence from the Chinese Communist Party, we have to focus on nearshoring and friendshoring our supply chains in conjunction with fair trade deals.

We have to expose the CCP's pattern of commercial aggression against America and our allies. You know, examples abounded during the pandemic of massive impact on supply chains. But for example, in the medical world we imported billions of dollars' worth of drugs and APIs from China annually. And this dependance on China is a national security concern.

I look forward to working with this committee and my colleagues and my colleagues on the China Select Committee to enact policies that will bring critical supply chains back to the U.S. and to trusted allies to help free us all from Dependance on China for critical commodities and pharmaceuticals.

Mr. Pugh, first question. I agree with your statements that data privacy and security are vital to consumers and industry. Understanding that the CCP has repeatedly compromised our data and that the ADPPA from the last Congress was a good first step in combating this data gathering, can you please speak to the seriousness of delaying that legislation?

Mr. PUGH. Well, thank you, Congressman. That is a phenomenal point, and every day we wait—or every second we wait, I should say—is just the more data that the Chinese Government, the CCP, is collecting and potentially exploiting against Americans.

I mean, we see their collection happening in the United States, outside the United States but still directed at Americans, and then we can't diminish the fact that they continue to just steal and even sometimes buy it. And that can, unfortunately, be used to target both intelligence professionals, those in the military, children. So I think it is just paramount that this is the key priority and is done without delay.

Mr. DUNN. Are there specific progrowth policies you would like to see from America?

Mr. PUGH. I think one of the best policies would be, first, acting on the comprehensive data privacy and security law. And I think one of the benefits of ADPPA was the intent of trying to get at the fact that not all companies are the same, is that we need to take into account that small and medium-sized businesses have different needs and different capabilities than our largest international players. Not to say they—they all may not have privacy risks, but a mom-and-pop business on Main Street cannot comply in the same way that—or no have the same risk.

So I do think that is something that we should act on now, a comprehensive law, and vary the—some of the provisions.

Mr. DUNN. Thank you for your reasonable approach to that.

Ms. Sacks, you commented on the importance of a multicountry approach for creating a network of trusted trading partners in which we lower barriers to trade in order to create resilient, reliable allied supply chain. This makes so much sense. Can you expand on that issue and perhaps say which allies, which partners we should be working on first?

Ms. SACKS. Well, perhaps I will highlight a number of initiatives that are underway which are really positive steps in this direction.

So I mentioned Global CBPRs, which is an expansion of the Asia Pacific-based framework. In addition, the OECD recently issued a set of principles around government access to data which would facilitate more data flows among OEC members, and the Japanese Government under former Prime Minister Shinzo Abe had put forward the data free flows with trust concept, which again is this idea to encourage a coalition of allies and partners to share data but with certain safeguards in place.

What does that look like and what does that mean in practice is a question that I think experts are actively debating. And this spring at the Hiroshima summit, my understanding is there may be further movement there. So these are all important initiatives, and definitely merit further attention.

Mr. DUNN. Well, I—thank you for your words. And I will tell you I sit on the economics committee of NATO as well as these other things, and it is a common theme among our NATO allies that—you know, to friendshore trade. And so I hope we can find a way to work our way through these trade barriers that we have erected to each other. And this is all—this is like friendly fire when we are in NATO.

So thank you very much for—the entire panel, a very erudite group.

I yield back.

Mr. BILIRAKIS. I appreciate it very much, Doctor. OK. Now we will recognize Representative Kelly for her 5 minutes.

Ms. KELLY. Thank you, Mr. Chair, and thank you to the witnesses.

During a time of crisis, the United States relies on its manufacturing base to withstand economic disruptions and respond to national emergencies. But the COVID–19 public health crisis exposed, as you know, serious gaps in our critical manufacturing supply chains that harmed our efforts to combat COVID–19, crippling shortages of N95 masks, gowns, surgical apparel, gloves, and testing supplies. The shortages were so severe that nurses substituted trash bags for gowns, doctors wore modified snorkels as masks, and essential medical personnel reused single-use N95 masks for days on end.

These crippling shortages contributed to the spread of the disease, causing preventable illnesses, hospitalizations, and death. Our healthcare system neared overload. Our healthcare heroes were placed under enormous strain. And the U.S. domestic manufacturing base was incapable of meeting the surging demand for critical healthcare equipment. Instead, hospitals and consumers turned to overseas fly-by-night brokers and opportunists selling standard PPE.

Last Congress, when the Democrats were in the majority, we made meaningful strides to strengthen our global economic landscape to ensure our competitors like China don't leave us competitively disadvantaged. Just one example is the America COMPETES Act, which would have invested 46 billion for a whole-of-government approach to monitoring and supporting critical manufacturing supply chains instrumental to our economic welfare and national security.

Unfortunately, that provision did not become law last term, but I am hopeful that we can get meaningful supply chain legislation over the finish line this Congress.

Mr. Jarsulic, in your written testimony you discuss the importance of supply chain resilience and, specifically, how important elements of the supply chain are subject to events in other countries and can, therefore, be subject to Chinese Government interference. How severe is the threat, and why hasn't the private sector been able to proactively identify and address such supply chain vulnerabilities?

Mr. JARSULIC. Well, I think we have seen multiple instances where significant gaps in the supply chain manifest themselves to—and produce significant economic impacts. A salient example which I talk about is the shortage of chips for manufacturing autos. The production of autos in physical terms was down, like, 40 percent, relative to the precrisis level, just because the chips that are needed to make those autos run weren't available.

There are lots of other examples where shortages were revealed in the crisis—are not here, they are manufactured elsewhere, and the ability to access them was stressed during that period.

I think that it is quite important to take a systematic view of the places where there are potential risks. The incentives for individual corporations to meet risks beyond their own business needs are not necessarily there. And where those systemic risks are identified, steps can be taken to anticipate potential problems. There are simple kinds of things that could be done, you know, stockpiling of materials that are needed, but there are analogies to other areas where there are risks that might apply here.

For example, in power generation, many power authorities commission the construction of residual generation capacity, which corporations agree to bring online if there is a surge in demand for power. So we might think about the production of things that we really need and might need in an emergency, and find ways to build that kind of backup or residual production capacity to prevent risks from becoming significant problems.

Ms. KELLY. And let me ask you this. Last Congress I was proud to co-lead the bipartisan Supply Chain Act, which would create an office of supply chain resiliency and crisis response within the Department of Commerce to monitor supply chains of critical goods and materials and plan for, as you are saying—respond to supply chain disruptions.

Could supply chain resilience improve if the Federal Government played more of an active role in monitoring critical supply chains and identifying vulnerabilities?

Mr. JARSULIC. I think, you know, studying and monitoring of these issues can make a very important contribution. You don't know where the problems are until you identify them.

Ms. KELLY. Sure, and I yield back. Thank you.

Mr. BILIRAKIS. Thank you. Thanks very much. And now I will recognize the gentlelady from Arizona, my good friend Mrs. Lesko, for 5 minutes, please.

Mrs. LESKO. Thank you, Mr. Chair. I am excited to once again return to this subcommittee. It has such broad jurisdiction, and it is great.

I am very excited about the future of autonomous vehicles. I have a huge senior citizen population in my district, and I am already a senior citizen. I can still drive, but there is going to be a point where I won't be able to drive.

And a lot of my constituents are having problems getting to their doctors, getting to the grocery stores, and there is not enough public transportation available for them. They use the dial-a-ride, but they have to wait, like, a long time. And, you know, they complain about it, right? So I think this is a solution, and it is a solution for the blind, it is a solution for disabled, and I am excited about it, quite frankly.

Now, I think you know that in Arizona, under our former Republican Governor, Doug Ducey, he was very excited about autonomous vehicles, as well. And so we have several companies that operate in Arizona. One of them is Waymo, owned by Google. It is partnered with the Chinese automaker Geely. Waymo currently has a fleet of autonomous rides in Phoenix.

So I have a question for you, Mr. Pugh: Do you—should I worry—should we worry about the partnership with a Chinese automobile company with autonomous vehicles as far as will our data be secure or will the Chinese Communist Party use it?

Mr. PUGH. Well, thank you, Congresswoman. I am not as familiar with that, the partnership that you referenced. But what I can say at a high level is that, when the Chinese Government does have involvement with a company, it is something we need to be very careful and mindful of, and ensure that they are not collecting data, and ensure it is not going back to the CCP.

And then we also need to ensure what we are collecting is safeguarded and secured. I think those two go hand in hand, and you can't have privacy without security, and vice versa. So in that particular example I would—I think we need to make sure that the privacy and security is accounted for.

Mrs. LESKO. Thank you.

And Mr. Farrah, how would you anticipate the global AV supply chain to be set up if the U.S. continues to limit the ability of the U.S. AV industry to develop here while China has the backing of an eager government?

So, you know, I think of—I remember California a number of years ago, they wanted to shut down the AV autonomous vehicle testing, and we picked up the slack in Arizona. So how is that going to affect it, if we don't change our policy here in the United States?

Mr. FARRAH. Well, first of all, I want to thank you for your enthusiasm for autonomous vehicles. We, obviously, share it. And

your home State has been tremendous in terms of a partnership. I think you detail one of our great member companies, and there are others, as well.

I think that the next point I would make here is that, with regard to supply chain, autonomy has an amazing contributing factor here as it relates to supply chain challenges. I will just give you one example, which is around autonomous trucking.

We have a situation now in this country where we have a truck driver shortage of nearly 80,000 truck drivers across the country. That is going to double by 2031. And so autonomous trucking really offers a solution, and I think it gets to trying to alleviate the supply chain crisis that a number of your colleagues have flagged today.

And so that is something where—I have been privileged to ride in these autonomous trucks. I see the way in which they are operating. They are viewing things, they are responding to incidents on the road that a human could never have a hope of being able to see. And so I think it is going to lead to more safety for people on the roads, for truck drivers, but better movement of goods.

Mrs. LESKO. Well, I think so, too, because, you know, as you said, what is it—like, right now isn't the first vehicle to have a driver, and it—and then there is, like, a caravan of other trucks that are autonomous and hooked up to it? Tell me more about that.

Mr. FARRAH. Not so much a caravan, but there are—so different developers, obviously, are approaching this in different ways. And there are situations where, in places like your home State of Arizona, there are autonomous vehicles that are operating without a human driver sitting in the seat that can grab control of the wheel.

There are other trucking examples where there is development that is going on, and there is currently a driver that is there in case. I have ridden in these autonomous trucks myself, and there is—they are entirely safe, and they are operating now.

And so it is really a diversity of approaches, but we are very eager and pouring a lot of resources into trying to get these out in the market in greater numbers.

Mrs. LESKO. Well, great. And I am running out of time, but I was just curious if, when you are answering somebody else's questions, if you can tell me, any of you, if you realize that security cameras that are made in China call back—if you are hooked up to the internet, they call back to China. And so a lot of the security cameras we use on our homes are made in China. Just curious about that.

Thank you, and I yield back.

Mr. BILIRAKIS. Yes, let's take that question for the record, please. That is so very important. Thanks for bringing it up.

Next we have my good friend from the State of Florida—we have a lot of Floridians—that is a good thing, that is a good thing—on both sides of the aisle.

So, Representative Soto, you are recognized for 5 minutes.

Mr. SOTO. Thank you, Chairman. It—Florida is in the House.

Mr. BILIRAKIS. That is right.

Mr. SOTO. First, I am happy to talk about our economic future as the United States, as it goes vis a vis our economic rivals, China.

I want to take a moment to set the table for my constituents. The U.S. GDP, our overall economy right now, is first in the world at $25 trillion. But definitely, China is on our tail, right? Chinese GDP is $18.32 trillion, according to the IMF. When you look at our populations, we are at a scrappy 334 million, according to the census, while China's National Bureau of Statistics has them at 1.4 billion.

So imagine. We are, pound for pound, the economic powerhouse of the world. And if you feel like, as Americans, you are working hard, well, it shows. We are the most productive nation in the world per capita by far.

Population growth is another interesting thing. Ours is slowing down. We had a 0.4 percent increase in population growth in 2022. The vast majority is from immigration, actually, not even from natural population birth. So as we are talking about immigration reform and the importance of immigration, we would be declining in population if we didn't actually have immigration. The Chinese, they are declining in population: 850,000 population drop in 2022.

So both of us face challenges, and we are at a crossroads. So when we come to the topic today of how Americans compete to win the future, the good news is the 117th Congress was the most productive in 50 years.

The infrastructure law to help us rebuild America. There is a big headline in Florida about Governor DeSantis proposing a $7 billion Moving Florida Forward plan. Over 3 billion of that plan comes from the new infrastructure law, and over 16.7 billion over 5 years to help redo I–4 and boost SunRail, and Brightline, and Poinciana Parkway, and other areas in the district.

And then we passed the CHIPS and Science Act, boosting microchip manufacturing. We are right now only making 10 percent of the chips, globally. This will help bring us forward with areas like NeoCity in my district that makes aerospace microchips and micropackaging and just received a $51 million Build Back Better grant with more to come.

And then the Inflation Reduction Act, a $369 billion investment to advance clean energy, to lower pollution, combat climate change, boosting electric vehicles, which we talked about a lot, solar, wind, more efficient appliances, nuclear, and carbon capture.

So the first thing I think is critical is that we don't push America to default on our debts. That has been talked about quite a bit already.

The second is we need to find areas of common ground like the privacy—internet privacy bill that we passed out last year that I expect will be one of the biggest things we do this term.

But also implementation of these laws are going to be key.

Mr. Jarsulic, you know, China faces air pollution, water pollution, plastics. Their soil is toxic with cadmium and other heavy metals. And the rallying cry of the last generation has gone viral by young Chinese people vowing not to have children. We want to have a different future here in the United States. So how critical is it to our economic success that we implement the Inflation Reduction Act to combat pollution, to boost clean energy for our economic future vis a vis competition with China?

Mr. JARSULIC. Well, I think that the effects of a degraded environment on health, labor force participation, productivity are significant. And so, to the extent that we can limit that, we—that contributes to the competitiveness of the U.S.

And it is also the case that the world is being pushed in the direction of production and economic behavior that limits carbon emissions. And so the more that we can do to make that transition efficiently, the more economic competitiveness we will have.

And so the kind of support that IRA gives to electric vehicles, to solar power, and to other forms of—and to the establishment of other forms of energy—incredibly important. The support that CHIPS gives to developments, both in basic science and the manufacture of semiconductors, means that we will have a better technical base to implement the kinds of things that will reduce those carbon emissions.

So I think that there is a lot that is being done that will contribute significantly to our long-term economic competitiveness and make up for the kind of disadvantages that we might face in the marketplace when we are dealing with a competitor who kind of disregards——

Mr. BILIRAKIS. Well, thank you. I thank the gentleman. The gentleman's time has expired. I appreciate it. Now we welcome the gentleman from Georgia.

Welcome to the committee, and the Chair recognizes you for 5 minutes.

Mr. ALLEN. Thank you, Mr. Chairman, and I thank the witnesses for being here with us today. And thank you again, Mr. Chairman. And it is a privilege to serve on this committee under your leadership.

Mr. BILIRAKIS. Best committee in Congress.

Mr. ALLEN. Yes.

Mr. BILIRAKIS. Don't forget that.

[Laughter.]

Mr. ALLEN. Well, it has been very interesting here today, I will tell you this.

Mr. Pugh, first I want to thank you for your service, for your work with the Army Cyber Institute. The Army Cyber Command Center is located in the 12th district of Georgia, my district. And it is good to see how expertise can be shared across the public and private sectors for data security purposes.

We are not engaged in cybersecurity warfare here, but how do you see passing a national data privacy framework providing for more cooperation among allied countries against current and political adversaries—how do you see that framework?

Mr. PUGH. Well, thank you, Congressman, and I am thrilled to see the Army represented in Georgia. I spent a lot of time in Fort Benning, so I appreciate that.

And to your point, I think the biggest issue now, Congressman, is we don't have a privacy law here. So it is forcing American companies to follow other frameworks around the—really, like GDPR and the European Union that is just not as friendly to businesses. So I think this is, really, a key opportunity for us to develop a framework, and hopefully others follow what we view as the American vision.

And I think the critical aspect is there are several provisions that promote security. Just to flag one of them is the notice if a consumer's data goes to China, North Korea, Iran, and Russia. Right now, data can flow there and the average consumer is totally unaware of it. And that is just a deep concern.

Mr. ALLEN. Well, obviously, that is our property, and we have the right to protect it, and we certainly need to do something about this.

Ms. Sacks, you have done a lot of work with security-focused think tanks. Again, you know, of course we passed the CHIPS Act, which, you know, I think totaled over 250 billion—$252 billion. And now it looks like we have got a glut of chips, of semiconductors in the country. What—has your think tank looked at, you know, what happens when the government pours money into something, and then it creates market problems, market issues as far as supply and demand?

Ms. SACKS. Well, I can speak from a personal capacity, rather than my organization's.

Mr. ALLEN. OK.

Ms. SACKS. I have not looked at that specific issue. I mean, I think you raise an important question, which is once—when governments pick winners and losers, we have to be very smart about how those resources are allocated, and particularly because we don't want to mirror China as a nation focused on industrial policy.

So how do we use State funding and facilitate productive partnerships between the private sector and public institutions to understand how do we allocate those resources to avoid exactly those issues that you have discussed?

Mr. ALLEN. And we don't seem to look down the road at the implications of this, as far as the free market.

And Mr. Farrah, the first thing is how much do these these vehicles cost? I mean, what is the price range?

Mr. FARRAH. Congressman, currently it is—as so-called level four autonomy is being deployed out into the United States, they are not currently available for private ownership. And so you have companies that are operating their own fleets of AVs. They are doing things such as robo taxis and—with the passenger cars, unmanned delivery pods that are delivering groceries and whatnot, AV trucks that I mentioned.

And so, while private ownership may be in the future, that is not where we are currently.

Mr. ALLEN. So we haven't gotten a market base on the price of manufacturing those vehicles? OK.

Mr. FARRAH. That is correct.

Mr. ALLEN. You are an innovator. Obviously, this is a great—this is going to be a great tool for the American people. What is the best driver of innovation in this country? Is it free market or government?

Mr. FARRAH. Sir, what I can speak to is that our industry has led in terms of private capital investment into this industry. Certainly, this has been a private-sector-driven exercise in terms of deployment of AVs to this point.

But it is important that policymakers shine a light on this industry because there is, obviously, a lot of work that needs to get done,

both from a Federal legislative perspective as well as at a regulatory perspective.

Mr. ALLEN. Right.

Mr. FARRAH. And so it truly is a partnership, and we need your help.

Mr. ALLEN. Well, Ms. Sacks, I think you hit—I mean, you hit the nail on the head where how does the government do this, because they are picking winners and losers. And it affects all the markets.

So with that, Mr. Chairman, I yield back.

Mr. BILIRAKIS. I appreciate that very much. OK, now I recognize the representative Mrs. Trahan for 5 minutes.

I appreciate it, thanks for your patience.

Mrs. TRAHAN. Thank you, Mr. Chairman.

It is no secret to anyone here today the United States has been losing the manufacturing race for a long time. It is certainly not a surprise to anyone in my district, which is where our Nation's industrial revolution was born, and where once-great mills have sat empty for years.

The offshoring of manufacturing jobs has hurt almost every sector, particularly as supply chain issues erupted during the COVID–19 pandemic. But perhaps the most glaring example of this dangerous trend is our semiconductor industry. Since 1990, the U.S. share of global semiconductor manufacturing dropped from 37 percent to 12, and in that time countries like China have surpassed us in semiconductor manufacturing capacity.

Mr. Chairman, this trend poses a serious threat not just to our Nation's economic competitiveness but to our national security. And supply chain disruptions have shown in excruciating detail, as we have waited on foreign shipments of semiconductors that have been bogged down in supply chain disruptions.

Like many of my colleagues on this committee, I have heard how this issue is impacting businesses and families that I represent. Massachusetts companies up and down the supply chain, from manufacturers of cancer screening technology to defibrillators, have been sounding the alarm about the disruption's impact on their business and the patients and hospitals depending on them.

Families looking to buy a used car to make sure they can get their kids to school on time have had to pay ridiculous prices, in part because of chip shortages in the automotive industry. It is for this exact reason that we voted in a bipartisan manner last Congress to pass the CHIPS Act, the CHIPS and Science Act, which includes unprecedented Federal funding to jumpstart our semiconductor industry and reestablish our Nation's manufacturing leadership.

And when I think about our competitiveness—frankly, our winning—I do think about the major pieces of legislation that we passed last year. My colleague from Florida talked about the Inflation Reduction Act, CHIPS and Science, of course, but also the bipartisan infrastructure bill.

So, Mr. Jarsulic, I am hoping that you can speak about the impact that the $52 billion included in the bipartisan CHIPS in Science Act, as well as the billions of dollars allocated by the infrastructure law to revitalize our roads, our bridges, railways, electric vehicle charging stations, high-speed internet, all that supportive

infrastructure, will have on U.S. domestic semiconductor manufacturing. And frankly, should we expect more private investment in this critical technology?

Mr. JARSULIC. Yes, I think those $52 billion are divided into two big parts. One is 11 to support basic science research and development that are related to semiconductor manufacturing. I think that that helps to overcome the real public good problem of doing that kind of basic research. But there is another $39 billion, the majority of which, 24 billion, provides investment tax credits for private investment.

And that means that the decision making about what is going to be built over what time frame really rests with the private sector. That is, these are credits. They are going to have to put private capital at risk in order to—you know, to get those credits and expand manufacturing capacity. So I think that the notion that there isn't a market-based, a competitive-based allocation of these funds is a little bit misleading.

That said, those two major efforts, both in terms of basic research and in terms of incentivizing investment, should do a lot to increase semiconductor manufacturing capacity. But any business needs an efficient and effective infrastructure to operate: good transportation, good water, good power supply. And I think that the support for that in bipartisan infrastructure will also benefit semiconductor manufacturing, as it will most business in the U.S.

Mrs. TRAHAN. Thank you, I appreciate that.

I will see if I have enough time to switch gears, because I was so excited to hear so many of my colleagues discuss privacy. Because the truth is many of the critical devices that require semiconductors also collect, store, and transmit personal and even sensitive consumer data.

My team and I thought about this quite a bit during the markup of the bipartisan and bicameral ADPPA last summer, and strong data minimization and data loyalty language allows consumers to escape constant consent popups, which are particularly useless in a world where sensors devoid of a screen monitor our vital signs, our sleep patterns, and the location of our pets to create comprehensive profiles of our lives that can be used in a range of predictive analytics.

So, Mr. Pugh, maybe for the record, hoping you can speak to the importance of data minimization to this Nation's cyber and national security.

Mr. BILIRAKIS. I appreciate it. You can take that for the record.

Thank you for the question, and the gentlelady yields back.

And I will recognize the gentlelady from the great State of Tennessee, home of the number one Florida Gator, Steve Spurrier, Johnson City.

Mrs. HARSHBARGER. Oh, you would have to mention that, Mr. Chairman.

Mr. BILIRAKIS. Of course, of course.

[Laughter.]

Mrs. HARSHBARGER. I am trying to forgive him.

Mr. BILIRAKIS. You are recognized for 5 minutes.

Mrs. HARSHBARGER. Thank you. My question goes—the first one—to Mr. Pugh. But let me read a little statement.

As a mother and a grandmother, I am deeply concerned about the ways TikTok is manipulating our Nation's children. You know, I have seen reports that detail China's version of TikTok, which offers the friendly version with educational videos and learning tools and time limits set on what the children look at in China. And then you come over here and you see the opium version, which, you know, addicts our children in front of their phone. And that educational tool isn't offered over here, like it is in China.

What are the current data privacy protections for children, and how could a comprehensive data security standard help strengthen those protections?

Mr. PUGH. Well, Congresswoman, thank you. Our current standards, simply put, are inadequate. I mean, we have COPPA. There were some other attempts to look at children's privacy legislation. But I think the real answer is a comprehensive approach, not the diminished attempts that are specifically at—directed at children. But really, privacy is a concern for all Americans. And I do think that was a—really, a hallmark of ADPPA last Congress was, regardless of age, there were protections there to help you.

Specifically with children, there were several phenomenal ones, everything from additional resources at the FTC directed specifically at kids to rules around target advertising for kids. You could tell that kids were definitely a focus in that bill, and I think that should be the case going forward.

Mrs. HARSHBARGER. Well, and I said this when I was on Homeland. I am like, if your children are on TikTok, get them off. Get them off. Adults, you are responsible, but children are not.

Ms. Sacks, I think that we both have questions for you with—concerning TikTok. And it is—you know, I am tremendously concerned about TikTok, but I am sure there's many other Chinese apps that you would suggest that we be watching. And I guess my question is, what other Chinese companies are you concerned about, and what should we be asking?

And then the second part is, can you describe how the CCP is encouraging the adoption of emerging technology like artificial intelligence and its defensive capabilities, and how the Beijing's unprecedented emphasis on intellectual property theft in this sector factors into those efforts?

Ms. SACKS. Thank you, and a lot to unpack there.

Mrs. HARSHBARGER. Yes.

Ms. SACKS. I guess I will start with the TikTok issue. You know, I think that there are two important issues on the table. One is data security—who has access to what—and the other is the potential to push misinformation online, the recommendation algorithm.

My understanding is that there is a national security agreement on the table, and I think it—and I have published an article which sort of details what exactly that looks like.

You know, from a data security standpoint, if the—if Oracle has the data in the cloud, there are multiple third-party auditors and an oversight board that reports to CFIUS. I think that that would be pretty much locked down.

The question around what kind of information the recommendation system pushes forward is an important one, and that also under this agreement would potentially—and it is called Project

Texas, and I have published about it just a week or so ago—would be, again, subject to verification source code review, essentially vetted by CFIUS.

I think it is important that the public understand what that national security agreement would look like, and then have a debate. Is this enough to address those concerns? And to what extent would other social media companies also need to meet those?

You know, I think that, as a mother, I am very concerned about what information my young children will be looking at online. And I am terrified, because right now I think it is a free-for-all. When we focus on specific companies, we can lock down that information, but it doesn't solve the issue.

Mrs. HARSHBARGER. Right.

Ms. SACKS. We can ban TikTok, force a divestiture. When my boys are teenagers I hope that there will be a more comprehensive solution, because it is not going to address the way that misinformation is addicting children. And so that is a much bigger issue than any single company.

Mrs. HARSHBARGER. Well, absolutely. And not to mention, you know, when Director Wray says that is a national security threat—and I know we are not talking about that —but the tracking of users' data, that is a concern. That is a huge concern.

And my grandsons are soon to be 6 and 8. So my son and daughter-in-law just better never bring TikTok to the table, OK?

And I guess, with that, I will yield back, Mr. Chairman.

Mr. BILIRAKIS. The gentlelady yields back. And I will recognize the—my good buddy from the State of Florida, Kat Cammack, for 5 minutes.

Mrs. CAMMACK. Yes, Steve Spurrier. Land of Steve Spurrier. Go, Gators.

Thank you, and congratulations to my good friend Chairman Bilirakis for hosting this very important hearing today. Thank you to our witnesses. We are coming to the end, so hang in there with us.

This topic, our competitive edge against an adversarial nation who uses the existing multilateral system to bend the rules in their favor, the Chinese Communist Party, is one of the most important issues of our time. Indeed, the CCP has very little regard for basic human rights, environmental protections, or the rule of law as they continue on their quest for global dominance.

So I believe that the greatest value that we have as a nation is our people, our constitutional republic, and our CQ, our creative quotient. We are innovators.

From the space race to the deployment of the internet, the United States has been an international leader on scientific innovation and achievement. Our free market model, paired with our national creative quotient, including private R&D efforts, no doubt drives much of our success as a leader in the world. So the work that we do here today will lead and carry us through the next several decades.

Without question, the U.S. and our allies must lead the world in privacy regulations and technological innovation. Otherwise, we risk allowing malign actors like the CCP to create a counter set of rules predicated on debt-trapped economies that will be enticed to

leave the rules-based system and adopt a model made to benefit authoritarian countries run by groups like the CCP.

So jumping right in, Mr. Pugh, you said in your testimony—and my good friend from Tennessee alluded to this—you know, the protections and privacy laws are wholly inadequate, by and large. How do we balance that patchwork of State laws?

How can we do a preemptive Federal privacy and data security law that specifically allows for those protections, while prohibiting the stifling of entrepreneurs or new market entrants into tech-related industries, quantum computing, social media, AI, et cetera?

Mr. PUGH. Congresswoman, thank you. And I think you really answered the question kind of yourself, because preemption is key. And I think ADPPA was a great substantive step in terms of how preemption was resolved.

I mean, that is exactly the thing. We need one Federal standard, not this patchwork that is emerging. Granted, only 5 States will have privacy laws in 2023. We have already seen dozens and dozens introduced this year and last year. So I think the real potential of having even more laws this year or next is going to be there.

And it hurts our small and medium-sized companies, because they don't largely have the resources to follow all the developments, the constant amendments at a State level. Whereas, if they have one standard to look to, it may still take resources, but at least it is one standard. So I think that is the key, and making sure preemption is strongly reflecting a Federal bill.

Mrs. CAMMACK. I appreciate that. And I am going to follow up again on my good friend from Tennessee.

We were sitting over here talking about TikTok. You know, I am the millennial in the room. And so this is a generation—grandmother, millennial. But, you know, this is a concern to me, my peers, and the generation coming directly right after me, the Gen Zs.

I grew up with social media, MySpace, Facebook—today Meta. These have real-world impacts. Privacy concerns? Heck, one social media platform can be directly attributed to a political revolution in nations abroad. So we know that there are real-world impacts that we have to contend with. So obviously, TikTok being a huge one.

Representative Harshbarger alluded to the fact that, in China, on TikTok children 14 and younger are shown patriotic videos, educational videos, history videos, and they are limited to 40 minutes. In the United States, they have the algorithms set to do shorter videos that are meant to create dopamine hits in your brain.

There was a survey done between the United States and China, a 14-year-old, asking, "What is the most aspirational career you want to have?" In the United States the number-one answer was social media influencer. In China they said they wanted to be an astronaut. If you want to look at the future of our two nations, start here. That is why we need to be very serious about how we contend with TikTok and other apps like TikTok.

So my question—and I know I am running short on time—is how can we protect our kids, our data, while simultaneously respecting free market economics in these applications?

The balance is a really tricky one, but we need to have a game plan moving forward on how we contend with this. And if any other witnesses want to answer this, I am open to hearing your thoughts.

Mr. BILIRAKIS. Let's——

Mrs. CAMMACK. In 9 seconds.

Mr. BILIRAKIS. Yes, very brief, and then we are going to take the question for the record. It is a very important question, so I want you to have as much time to answer it. This is what we are facing in this country. Please, briefly.

Mr. PUGH. The short answer, Congressman and Chairman, is passing a national comprehensive data privacy and security law. We did a report last year with 125 different entities across all ideologies, in conjunction with Harvard. And we think that really is the answer of solving some of these national security and privacy concerns.

Mr. BILIRAKIS. Thank you.

Mr. PUGH. Thank you.

Mr. BILIRAKIS. Thank you, thank you, I appreciate it. I now recognize the vice chairman.

Congratulations, Mr. Vice Chairman of the full committee, Mr. Armstrong. You are recognized for 5 minutes.

Mr. ARMSTRONG. Thank you, Mr. Chair.

Ms. Sacks, whether it is national security threats from aggression, nation states, or data protection regimes, it seems as if the trend is towards data localization. You have recently and even today mentioned Project Texas, TikTok's proposed mitigation agreement to address U.S. national security concerns, as a potential accelerant to data localization requirements. And you were speaking with Congressman Dunn about data free flows with trust.

Does our experience with the challenges of the EU–U.S. privacy framework and broader international concerns about U.S. surveillance capabilities make that a realistic proposal in the near term?

Ms. SACKS. Thank you for raising the issue of data localization, because I think this gets at an inherent tension here, right?

Governments around the world, the U.S., in Europe, in China, in India are increasingly concerned with foreign government access to data, as well as private-sector access. And so I think what is happening is the response to this is increasing requirements would require data to be stored on local servers and undergo extensive vetting before it is sent abroad.

Project Texas, from my understanding of what has been released publicly, would address U.S. Government concerns around who has access to the data by storing it in an Oracle cloud with a number of third-party vetters, auditors, to vet that in terms of the data that leaves. But it also potentially creates a blueprint to accelerate this trend of digital sovereignty, which we have seen around the world beyond the U.S. and China.

And so this question of how do you strike a balance between facilitating greater data flows which are needed for innovation and economic competitiveness while also addressing legitimate data security questions, this is sort of the key question, and I think it is one that merits much further discussion.

Mr. ARMSTRONG. I literally just came up here from asking questions about the Chinese Government—or a hacking group in Chi-

nese—either with coordination with the Chinese Communist Party, or definitely with the permission of the Chinese Communist Party actually going after our COVID relief funds. So, I mean, this is coming from every different place.

But we often discuss CCP's collection of U.S. person data by citing the 2015 OPM hack, as well as the hacks on Marriott and Equifax. The followup question is usually how the CCP might operationalize that data. I think we understand the ramifications of weaponizing that data against national security officials or Chinese dissidents to blackmail or develop kompromat. Can you explain the risks of the CCP aggregating all the data they have obtained, and the type of risks it might reveal at the demographic or population levels?

Ms. SACKS. Yes. I mean, to be honest, I think that creating profiles based on aggregate data is primarily a counterintelligence concern for individuals with national security clearances, in the military, or access to sensitive information. For your average American, what that—what the impact would probably be more in terms of would that population or individual preference information—could that be used to push information that would make, say, a spear phishing attack more appealing?

It might be more likely that someone would be a—would click on a link because it appealed to them based on information that was collected. And so I would say it is—I would look at it from that angle.

But what I highlighted in my testimony, the more sort of far-reaching impact is on economic competitiveness, which is a distinct issue, right? It is on Chinese firms who are able to access diverse international data sets beyond China. What that allows them to do is train AI models that could be more competitive in markets outside of China, where they are competing head to head with U.S. firms.

So I would bucket the risk. You have national security issues, you also have targeted misinformation that could be used from that, as well as economic competitiveness between the U.S. and Chinese firms. And it is important to sort of be clear about those distinct buckets of risk.

Mr. ARMSTRONG. Mr. Pugh, I am going to ask you the same question. You got, I mean, 45 seconds to follow up, so that was easy.

But, I mean, I think we always operationalize this at the national security, but it is hard to get it down to my 15-year-old daughter, who is on TikTok way more than she should be, and all of these different issues about the data collection.

Mr. PUGH. I think the key point to recognize, Congressman, is data is not just universal. There's different types of data. So even when it comes to geolocation data—yes, maybe I am an exception because I served in the military. But outside of that, I don't want another country knowing where I am in a moment, where I am going, where my movements are, regardless——

Mr. ARMSTRONG. I don't want my own country knowing that.

[Laughter.]

Mr. PUGH. So I think that that is a risk. And then off of that, not only they collect the data, they are really bad at securing it, evidenced by the breach they had in the Shanghai Police Depart-

ment last summer. So they are collecting it, and they are not even making it safe. So even other third parties and adversaries are getting it.

Mr. ARMSTRONG. And I would just end with I didn't want to be a social influencer or an astronaut. I wanted to be a fireman. So I became a lawyer and a politician.

Thank you. I yield back.

Mr. BILIRAKIS. Oh, well, who are you going to blame for that?

Folks, well, thank you. We are off to a good start, and I appreciate everything. Seeing there are no further Members wishing to be recognized, I want to thank the ranking member. Again, I want to thank the witnesses for being here today.

And I have got a little housekeeping here. So, pursuant to the committee rules, I ask unanimous consent to enter the following documents into the record: a letter from the Alliance for Automotive Innovation; a report from the Alliance for Automotive Innovation titled "Ready to Launch: Autonomous Vehicles in the U.S.;" a presentation by the Alliance for Automotive Innovation titled "Policy Roadmap to Advance Automated Vehicle Innovation;" a letter to the Secretary of Transportation, Mr. Buttigieg, regarding the Huawei Technologies; the September 2020 China Task Force report; an amendment offered to the INVEST in America Act; a letter from the National Federation of the Blind supporting an amendment to the INVEST in America Act; a press release from the Jacksonville Transportation Authority regarding their partnership with Beep and NAVYA to safely transport COVID–19 samples; an article by Klon Kitchen and Hal Brands entitled "Tuya may be the China threat that beats Russia's ransomware attacks;" a letter regarding the FCC's Secure and Trusted Communication Networks Reimbursement Program; a letter from the Consumer Brands Association and Information Technology Industry Council; a letter from the Advocates for Highway Safety regarding emerging vehicle technologies and autonomous vehicles; a report from the Center for Strategic and International Studies entitled "Empty Bins in a Wartime Environment: The Challenge to the U.S. Defense Industrial Base;" and finally, a letter from the National Association of Manufacturers.

[The information appears at the conclusion of the hearing.[1]]

Mr. BILIRAKIS. OK, very good. We got that in.

Pursuant to the committee rules, I remind Members that they have 10 days, 10 business days, to submit questions for the record. And I ask the witnesses to respond to their questions promptly.

Members should submit their questions by the close of business on February 15.

If there is no other business, without objection, this subcommittee is adjourned. Thank you.

[Whereupon, at 1 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

---

[1] The China Task Force report and the Center for Strategic and International Studies report have been retained in committee files and are available at https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=115346.

ALLIANCE FOR AUTOMOTIVE INNOVATION

February 1, 2023

The Honorable Gus Bilirakis
Chairman
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Innovation, Data, and Commerce
House Committee on Energy and Commerce
2322 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky,

On behalf of the Alliance for Automotive Innovation ("Auto Innovators"), I appreciate your attention to preserving and enhancing U.S. competitiveness. The global auto industry is undergoing a generational transformation and the next decade may well define which nations shape the future of automotive innovation and manufacturing. Amid intense global competition, we must work collaboratively to support the development, commercialization, and acceptance of the innovative technologies that will redefine motor vehicle transportation for decades.

Auto Innovators was formed in 2020 to serve as the singular, authoritative, and respected voice of the automotive industry in the United States. Our members represent the full automotive industry, from the manufacturers producing most vehicles sold in the U.S. to autonomous vehicle innovators to equipment suppliers, battery producers and semiconductor makers. As the nation's largest manufacturing sector, the automotive industry is responsible for nearly 10 million U.S. jobs and represents 5.5 percent of the country's gross domestic product.

Leadership in automotive technology and manufacturing has underpinned a century of U.S. economic growth. As we look to the future, however, the industry's economic footprint will be defined by our leadership, acceptance and integration of the innovative technologies - including electrification, automation and connectivity - that will shape the future of our industry. It is no longer a question of when these technologies will prosper. Rather, it's a question of where - and nations around the world are moving aggressively to lead, and define, the next generation of personal mobility.

One area of innovation at the center of this global competition to define the future of the auto industry is autonomous vehicles (AVs). The U.S. has long been a leader in the advancement of AV technologies, placing it at the forefront of innovations that will transform personal mobility, transportation, and the movement of goods. At their core, AVs are safety technology. This could not be more critical following multiple years of increased fatalities on American roads - reversing decades of decline. Of all automotive innovations and technologies, AVs offer the greatest opportunity to reduce the number of tragedies on our roadways.

While safety remains a core principle in the need for and development of AVs these technologies have more to offer beyond safer streets. For example, they have the potential to provide life-changing

opportunities for those who are not adequately served by existing mobility options, such as seniors, persons with disabilities, and those who require accessible transportation. As demonstrated during the COVID-19 pandemic, AVs also offer new transportation and delivery solutions to communities and individuals in need.[1] And they open the door to new possibilities for reducing congestion and improving the environment, as well as opportunities to create more efficient, worker-friendly supply chains.

As a global leader in the development of AV technologies, the U.S. has the opportunity to drive AV innovation. In December 2022, Auto Innovators released a comprehensive report on the AV industry in the U.S. which documents 84 AV companies operating in 120 cities across 30 states.[2] This includes nearly 170 on-road autonomous technology programs operating throughout the U.S. These programs further research and validation of key technologies, bringing with it not only technological leadership, but jobs, investment, tax revenue and local economic growth.

As these technologies mature, however, the nation needs updated federal regulations and a pathway to scale their development with appropriate oversight in order to realize many of the promises of this technology. That is why a responsible federal framework for the safe development, testing and deployment of AVs in the United States is so important. Consistent with the Department of Transportation's principles for innovation, this will help to preserve U.S. leadership in these potentially life-saving and life-changing technologies and ensure U.S. innovations benefit the traveling public and our economy for decades to come.

Other nations - in particular China and European Union - are not throwing in the towel and waiting for U.S. leadership on AVs. Quite the contrary; they are supporting the development of this new industry, regulating AVs, and seeking to become the global center of AV development and deployment. In particular, China is moving quickly to advance their national progress in developing AV technologies and three of the seven AV developers approved for testing in California are Chinese companies.

As we have witnessed in other technologies and sectors, the nations that lead the development of AVs will guide the development of international standards, control supply chains, and define international markets. With a technology like AVs, the implications will be felt far beyond transportation. For example, AVs are directly tied to the development of artificial intelligence systems. As noted in a recent report by CSIS:

> The AV sector is a critical lynchpin to U.S. leadership in Artificial Intelligence (AI). In 2019, the AV industry led all other AI sectors as a destination for global investment. As autonomous vehicles (AVs) move toward commercialization, the regulatory environment can be a source of advantage. Yet, in the global AV race, Beijing currently holds the regulatory advantage due to its commitment to being a first-mover in AI and AV, giving

---

[1] See e.g., Jane Lanhee Lee. Nathan Frandino, *Reuters*, "Self-driving vehicles get in on the delivery scene amid COVID-19," (April 29, 2020) *available at* https://www.reuters.com/article/us-health-coronavirus-self-driving-deliv/self-driving-vehicles-get-in-on-the-delivery-scene-amid-covid-19-idUSKBN22B2LZ.

[2] https://www.autosinnovate.org/posts/papers-reports/AV%20Report.pdf

> Chinese companies more freedom to test vehicles and collect valuable data. In order to compete with China, the United States must adopt a regulatory framework that allows space for US companies to continue to gather additional data of their own that can be used to innovate and keep pace with competitors.[3]

This is not simply a question, therefore, of global or economic competitiveness. It is about defining the future of this technology - and associated infrastructure - in a manner that emphasizes safety, responsibility, and opportunity for more citizens to benefit from this transformative shift in mobility.

The U.S. is well positioned to continue its long-standing leadership in automotive innovation, however, in the face of clear global competition, we cannot be complacent. To foster the safe and responsible deployment of AVs in the U.S., the U.S. DOT needs to accelerate efforts to update existing motor vehicle safety standards to accommodate AVs and use its existing authority to grant targeted exemptions to AV companies that have demonstrated safety equivalence. In addition, in December 2020 Auto Innovators released the *AV Policy Roadmap* which includes fourteen specific recommendations that can be implemented by federal policymakers over the coming years to facilitate the near-term testing and deployment of AVs at scale.[4] These recommendations are focused on reforming regulations, harmonizing policies, and laying the foundation to achieve longer-term objectives - including expanding the number of exemptions that U.S. DOT can provide on a case-by-case basis - with safety oversight and full enforcement powers - which can then provide the data necessary to support future Federal Motor Vehicle Safety Standards for AVs.

We are approaching a pivotal moment in the evolution of this technology and have an opportunity to work collaboratively to chart a course that sustains U.S. leadership and innovation in these critical safety and mobility solutions for decades to come. It is not just about the future of the auto industry - it is about the nation's global competitiveness and economic security. We look forward to continuing to work with you and your colleagues in Congress, as well as the Administration and other stakeholders, to realize the benefits of a safer, more environmentally friendly, accessible, and equitable U.S. transportation future.

Sincerely,

John Bozzella
President & CEO
Alliance for Automotive Innovation

---

[3] https://www.csis.org/analysis/ai-strategies-and-autonomous-vehicles-development

[4] https://www.autosinnovate.org/innovation/AVRoadmap.pdf


ALLIANCE
FOR AUTOMOTIVE
INNOVATION
Ready to Launch
Autonomous Vehicles in the U.S.
Tracking the current (and future) AV landscape
December 2022

Here to Stay: Autonomous Vehicles in the U.S.

Alliance for Automotive Innovation surveyed the entire autonomous vehicle landscape. We found a thriving AV industry in the United States and huge progress on autonomous technology in many states.

Among the findings?

- 84 AV companies in 30 states and 120 cities;
- Nearly 170 autonomous technology programs operating in Michigan, Washington, Arizona, Texas, Florida and Pennsylvania among other states.
- AVs regularly move passengers in San Francisco, Phoenix and Las Vegas; deliver goods in Houston; and transport freight across the southwest.

The question on everyone's mind: When will AVs be on roads in large numbers?

The biggest obstacle to achieving that kind of scale is not technology and not a lack of corporate investment. We found numerous announced AV partnerships in this report.

Government is the biggest obstacle.

A federal regulatory framework with oversight and a commitment to move beyond testing to more (and faster) commercial deployment is what's needed now.

Policymakers should:

- Update existing motor vehicle rules to accommodate AVs;
- Raise the cap on the number of AVs able to operate at a time; and
- Launch a national AV pilot or demonstration program.

The longer it takes to get that regulatory structure in place, the more skittish (and less patient) AV developers are going to get. Even if the U.S. government doesn't get its act together, AV technology isn't going away. Global AV leadership will migrate to China and other nations setting the right conditions to make AVs more available.

On top of the safety benefits, AVs provide accessible transportation options for seniors and individuals with disabilities and a way to reduce traffic congestion and create new jobs.

A federal framework with safeguards, oversight, rules, regulation – and mostly a degree of predictability and certainty for the market – will release the power and potential of AVs.

John Bozzella
President and CEO
Alliance for Automotive Innovation

ALLIANCE FOR AUTOMOTIVE INNOVATION

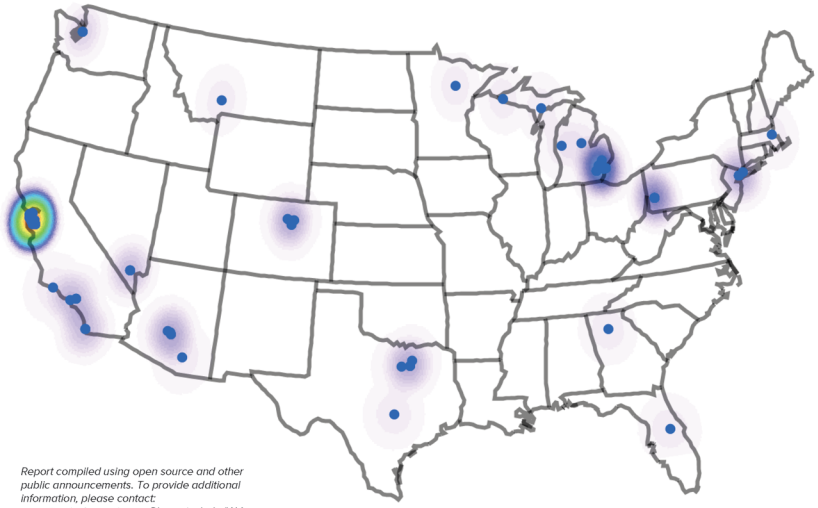
www.autosinnovate.org/AVs

AV Companies in U.S.

69 Companies

112 Facilities

16 States



Report compiled using open source and other public announcements. To provide additional information, please contact: press@autosinnovate.org. Please include "AV Report" in the subject line.

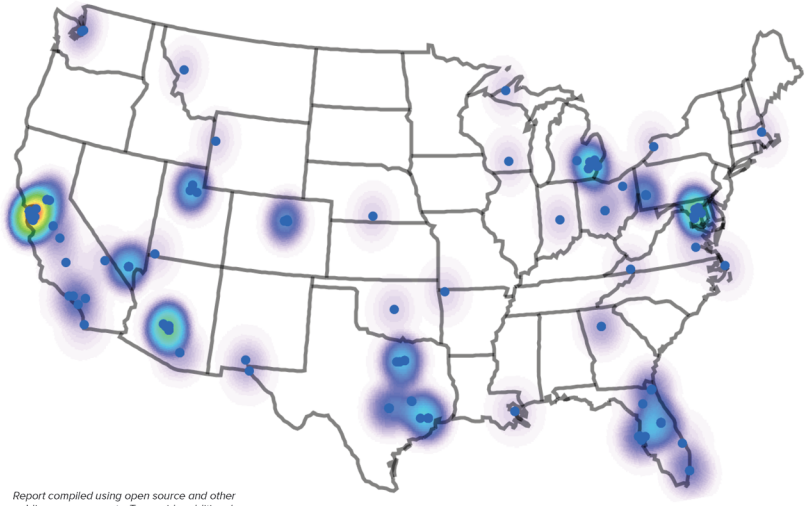
**See Appendix A*

On-Road AV Operations in U.S.

40 Companies

167 Programs

27 States



Report compiled using open source and other public announcements. To provide additional information, please contact: press@autosinnovate.org. Please include "AV Report" in the subject line.

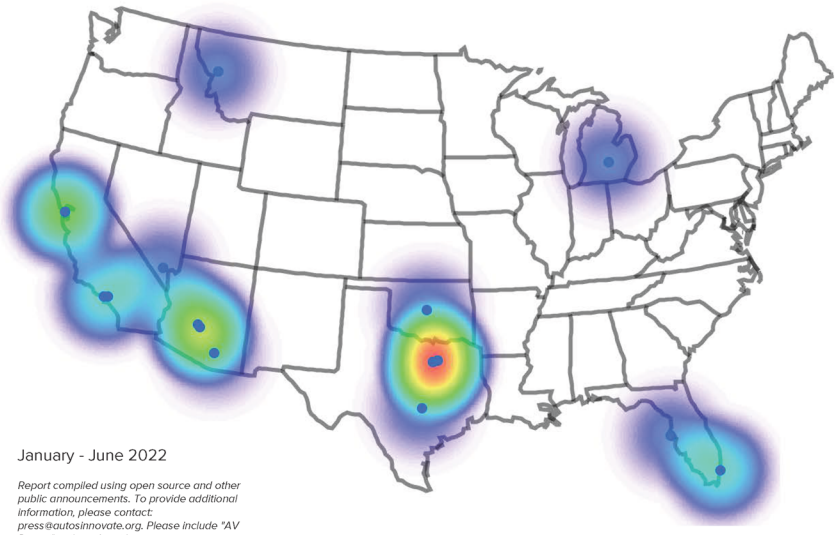
**See Appendix B*

New in 2022: On-Road AV Programs in U.S.

22 Programs

15 Cities

8 States



January - June 2022

Report compiled using open source and other public announcements. To provide additional information, please contact: press@autosinnovate.org. Please include "AV Report" in the subject line.

*See Appendix C

Autonomous Vehicle Company Activity

January - June 2022

Company	Activity Type	Month Announced	Program/Announcement Description	Additional Information
ADASTEC CORP	Testing	May	Michigan State University has debuted its electric, autonomous bus after months of trial runs. . . . The autonomous bus project is a collaboration between the state of Michigan, bus manufacturer Karsan and Detroit-based automotive software engineering firm ADASTEC.	Learn More
Apex.AI	Partner	May	Apex.AI announced that it received a strategic minority investment from Daimler Truck	Learn More
Argo AI, LLC	R&D Facility	Feb	Argo AI announced the opening of a new engineering and development office in Los Angeles.	Learn More
Argo AI, LLC	R&D Facility	Apr	Argo AI is establishing a new test facility in South Carolina.The $2.6 million investment in Greenville County is expected to create 40 new jobs.	Learn More
Argo AI, LLC	Testing	May	Argo AI announced the start of driverless testing in Austin, TX.	Learn More
Argo AI, LLC	Testing	May	Argo AI announced the start of driverless testing in Miami, FL.	Learn More
Aurora	Partner	Feb	Aurora is teaming up with freight carrier U.S. Xpress to study the best ways to find commercial applications for the technology as shippers contend with a driver shortage and supply-chain snags. As part of the collaboration Aurora will gather data from Variant, U.S. Xpress' digital platform, to study where and on what types of routes its AI-enabled driving system could be deployed most effectively.	Learn More
Aurora	Partner	May	Aurora and Covenant Logistics Group, Inc. announced a collaboration to explore ways to optimize Covenant's long-haul operations with Aurora's autonomous trucking product.	Learn More
Aurora	Product & Program Announcement	Mar	Aurora Innovation, Inc. has launched Aurora Driver Beta 2.0, the second release of its integrated hardware and autonomy system.	Learn More
Aurora	R&D Facility	Jun	Aurora expands presence in the City of Bozeman, MT with a brand new 78,000 square foot R&D facility to build future generations of FirstLight Lidar to support commercial fleets.	Learn More
Aurora	Testing	Mar	Aurora Innovation is launching a small test fleet of custom-designed self-driving Toyota Siennas for future ride-hail operations. The company will test its vehicles on highways and suburban streets in the Dallas-Fort Worth, Texas area, with a focus on high-speed routes.	Learn More
Aurora	Testing	Apr	Aurora and Werner Launch Commercial Pilot to Autonomously Haul Freight in Texas	Learn More
Beep	Testing	Jan	Through April 2022, the City of Peoria, Beep and the Maricopa Association of Governments (MAG) will be testing an autonomous shuttle service called, RoboRide Medical, as part of a four-month pilot program.	Learn More
Beep	Testing	Apr	The Pinellas Suncoast Transit Authority's (PSTA) Autonomous Vehicle, known as AVA, is returning to Dunedin after a successful six-week pilot on Clearwater Beach.	Learn More
Bosch	Acquisition	Apr	Bosch announced that it would be acquiring Five.ai, the autonomous driving startup.	Learn More
Bosch	Partner	Jan	Bosch and the Volkswagen Group subsidiary Cariad have agreed to form an extensive partnership to make partially and highly automated driving suitable for volume production, and thus available to the broad mass of consumers.	Learn More
Cruise	Testing/Deployment	Feb	Cruise launched delivery service in Phoenix	Learn More
Cruise	Testing/Deployment	Jun	Cruise launched commercial service in San Francisco	Learn More
Einride	Testing	Jun	Einride was granted a permit by the National Highway Traffic Safety Administration for a public road pilot project.	Learn More
Embark Trucks	Partner	Mar	Embark will partner with Texas A&M to research and test autonomous trucking and technology as it prepares for its self-driving pilot runs in 2023.	Learn More
Embark Trucks	Partner	May	Embark announced that U.S. Xpress has joined the Embark Partner Development Program and plans to add its terminals to the Embark Coverage Map. This partnership marks a significant milestone by adding a fleet's properties into an autonomous truck developer's transfer point network.	Learn More
Embark Trucks	Product & Program Announcement	Feb	Embark Trucks and Phoenix-based Knight-Swift Transportation are launching what they are calling a Truck Transfer Program. Rather than using Embark employees, the program will allow Knight-Swift drivers to operate the autonomous trucks during the testing phase.	Learn More
Embark Trucks	Testing	May	Embark Trucks announced the successful completion of on-road testing in snowy conditions in Montana. The testing was conducted to demonstrate the performance and safety of Embark's patent-pending Vision Map Fusion (VMF) technology in geographies that experience severe winter weather.	Learn More

Autonomous Vehicle Company Activity

January - June 2022

Company	Activity Type	Month Announced	Program/Announcement Description	Additional Information
Faction	Product & Program Announcement	Feb	Faction Technology, Inc. and Arcimoto, Inc. showcased a next-generation driverless delivery vehicle based on the Arcimoto FUV platform at the new Arcimoto RAMP manufacturing facility in Eugene, Oregon today. Equipped with Faction's DriveLink™ and TeleAssist™ technologies, the completely driverless Faction D1 combines autonomy with remote human teleoperation.	Learn More
Gatik AI Inc.	Product & Program Announcement	Jun	Gatik will start using its self-driving trucks this summer to deliver Georgia-Pacific paper goods like Dixie cups and Quilted Northern toilet paper to several dozen Sam's Club stores in the Dallas-Fort Worth area.	Learn More
General Motors	Investment	Mar	GM buys SoftBank's $2.1 billion stake in Cruise self-driving unit.	Learn More
General Motors	Investment	Apr	General Motors will spend $2 billion this year on its self-driving subsidiary Cruise.	Learn More
Honda	Investment	Jan	Honda Motor Co. has made an investment in Helm.ai's $30M Series B financing, to strengthen the ongoing development of cutting edge artificial intelligence software.	Learn More
Hyundai	Product & Program Announcement	May	Motional - a joint venture from Hyundai and Aptiv - has just announced that their latest driverless IONIQ 5 based robotaxi will be available from 2023.	Learn More
Intel/Mobileye	Partner	Jan	Mobileye and Geely are joining forces to develop a consumer-ready autonomous vehicle that will be ready by 2024.	Learn More
Intel/Mobileye	Product & Program Announcement	Feb	Intel Corp's Mobileye unit plans to build and deploy self-driving electric shuttle vehicles with its partners in the United States in 2024, in a bid to scale up its automated driving systems beyond taxis and delivery vehicles. Mobileye, Benteler EV Systems and Beep will launch the on-demand driverless shuttles, which will feature 12 to 14 seats and no steering wheel or pedal.	Learn More
Intel/Mobileye	Testing	Apr	Intel's Mobileye subsidiary has begun testing its autonomous vehicles in Miami to help build self-driving cars that can handle a variety of factors, such as weather conditions, urban layout, traffic signals and driving styles.	Learn More
Kodiak	Partner	Mar	CEVA Logistics announced it has teamed up with Kodiak Robotics to deliver freight autonomously between Dallas Fort-Worth and Austin.	Learn More
Kodiak	Partner	Apr	Kodiak Robotics, Inc. announced that it has teamed up with U.S. Xpress, one of America's largest carrier fleets, to launch Level 4 autonomous freight service between Dallas-Fort Worth and Atlanta using Kodiak's self-driving trucks.	Learn More
Kodiak	Testing	Mar	CEVA Logistics announced it has teamed up with Kodiak Robotics to deliver freight autonomously between Dallas-Fort Worth and Oklahoma City.	Learn More
Kodiak	Testing	Mar	Kodiak Robotics and Ceva Logistics have become the first companies to deliver freight autonomously in the state of Oklahoma.	Learn More
Locomation	Partner	Mar	Locomation, a leading provider of autonomous trucking technology solutions, today announced an eight-year agreement with Christenson Transportation, Inc., a top mid-sized transportation provider, to boost its fleet capacity with Locomation autonomous truck technology.	Learn More
Luminar	Partner	Jan	Luminar announced today a partnership with Mercedes-Benz to accelerate the development of future highly automated driving technologies for Mercedes passenger cars.	Learn More
Magna	Acquisition	Jan	Magna announced that it was acquiring the technology, IP and assets of Optimus Ride, a Boston AV startup	Learn More
May Mobility	Partner	Apr	May Mobility is putting accessibility at the forefront and partnering with BraunAbility, the world's leading manufacturer of mobility transportation solutions, to modify the May Mobility Toyota Sienna Autono-MaaS (S-AM) fleet to include ADA-compliant vehicles.	Learn More
May Mobility	Testing	Apr	After a successful one-year pilot, Arlington RAPID has been renewed through 2024.	Learn More
Mercedes-Benz	Product & Program Announcement	May	Mercedes-Benz will offer Drive Pilot, the first Level 3 autonomous driving system approved for European public roads, as an option on S-Class and EQS models starting May 17.	Learn More
Motional AD LLC	Product & Program Announcement	May	Motional's autonomous vehicles are now conducting end-to-end food deliveries on the Uber Eats network in Santa Monica, CA and West Hollywood, CA.	Learn More
Motional AD LLC	Testing	Feb	Motional and Via announce the launch of a new robotaxi service in Las Vegas, which will provide free self-driving rides to passengers in downtown Las Vegas.	Learn More

Autonomous Vehicle Company Activity

January - June 2022

Company	Activity Type	Month Announced	Program/Announcement Description	Additional Information
NURO	Product & Program Announcement	Jan	Nuro has introduced its third-generation electric autonomous delivery vehicle. This new vehicle improves on the previous design and is ready to be produced at scale.	Learn More
NURO	Product & Program Announcement	Apr	Expanding On-road Operations in Southern California	Learn More
Pony.AI	Partner	Jan	Pony.ai Forms joint venture with Sinotrans, one of China's leading logistics firms, to further deployment of autonomous driving technologies.	Learn More
Pony.AI	Product & Program Announcement	Jan	Pony.ai debuted its 6th generation autonomous driving (AD) system, with leading-edge sensors, NVIDIA DRIVE computing platform solutions, and styling and design features for L4 automotive-grade mass production fleets. The first model equipped with this system, Toyota S-AM, a seven-seat hybrid electric platform for autonomous mobility, will start road testing in China this year and be deployed within Pony.ai's public-facing robotaxi operations in the first half of 2023.	Learn More
STEER Tech, LLC	Testing	Apr	STEER Tech, announced that it was awarded funding under the North Central Texas Council of Governments (NCTCOG) Automated Vehicles Program to develop a cutting-edge testbed at the Dallas Fort Worth International Airport (DFW) that will demonstrate a comprehensive automated parking ecosystem.	Learn More
Stellantis	Partner	Jun	Valeo will supply Stellantis with its third-generation Scala lidar to enable SAE Level 3 autonomous driving in the automaker's models, starting in 2024.	Learn More
TuSimple	Product & Program Announcement	Jan	TuSimple develops autonomous domain controller using NVIDIA DRIVE Orin to bring level 4 autonomous trucking to market at scale.	Learn More
TuSimple	Product & Program Announcement	Feb	Union Pacific Railroad, the largest Class I railroad in the U.S., will become the first customer to move freight on TuSimple's fully-automated trucking route between the Tucson and Phoenix, Arizona metro areas.	Learn More
Udelv	Product & Program Announcement	Jan	Udelv unveiled the first cab-less autonomous electric delivery vehicle for multi-stop delivery, the Transporter, driven by Mobileye, at the Consumer Electronics Show (CES).	Learn More
Volvo	Product & Program Announcement	Jan	Volvo Cars will introduce its unsupervised autonomous driving feature Ride Pilot to customers in the state of California first.	Learn More
Vueron	Testing	Jun	The California Department of Motor Vehicles approved LiDAR-only autonomous vehicle testing permits for Vueron. After that, it succeeded in driving 383 miles from Los Angeles to San Francisco via Interstate 5 and Interstate 580, for 6 hours at a maximum speed of 70mph.	Learn More
Waymo LLC	Partner	Jan	J.B. Hunt Transport Services Inc. announced a long-term, strategic alliance with Waymo Via that will advance innovative efforts to integrate commercial autonomous driving technology in transportation and logistics, with ultimate plans to complete fully autonomous transport in Texas in the next few years. The expanded collaboration will include multiple pilots to analyze the operational capacity of Waymo Via, the company's autonomous Class 8 trucking unit powered by the Waymo Driver, to address customer needs in realistic scenarios.	Learn More
Waymo LLC	Partner	Feb	C.H. Robinson and Waymo Via, the trucking and local delivery unit of autonomous driving technology company Waymo, have formed a long-term strategic partnership to mutually explore the practical application of autonomous driving technology in logistics and supply chains.	Learn More
Waymo LLC	Testing	Feb	Waymo has scored a permit with the California Public Utilities Commission that allows it to charge riders for ride-hailing trips in its autonomous vehicles in San Francisco.	Learn More
Waymo LLC	Testing	Mar	Waymo has started giving employees driverless rides in San Francisco in a Jaguar I-Pace SUV.	Learn More
Waymo LLC	Testing	May	Waymo employees will be able to hail fully autonomous rides in Downtown Phoenix.	Learn More
Waymo LLC	Testing	May	Waymo opens autonomous service to select Phoenix passengers	Learn More
Waymo LLC	Testing	Jun	Waymo will deploy self-driving trucks on UberFreight network	Learn More

AV Companies in U.S.

Appendix A

State	City	Company	Facility Type	Number of Facilities
Arizona	Chandler	LM Industries Group Inc	Headquarters	1
	Chandler	Waymo LLC	R&D Facility	1
	Phoenix	Imagry	R&D Facility	1
	Tempe	NURO	R&D Facility	1
	Tucson	TuSimple	R&D Facility	1
California	Belmont	Volkswagen	R&D Facility	1
	Berkeley	HERE Technologies	R&D Facility	1
	Burlingame	Udelv	Headquarters	1
	Cupertino	Apple	Headquarters	1
	Emeryville	BlueSpace.AI	R&D Facility	1
	Foster City	Zoox	Headquarters	1
	Fremont	DeepRoute AI	R&D Facility	1
	Fremont	Inceptio	R&D Facility	1
	Fremont	Pony.AI	Headquarters	1
	Fremont	Zoox	R&D Facility	1
	Los Altos	Toyota Research Institute	Headquarters	1
	Menlo Park	Cyngn	Headquarters	1
	Menlo Park	Didi Research America	R&D Facility	1
	Menlo Park	Helm.Ai	R&D Facility	1
	Mountain View	aiMotive	R&D Facility	1
	Mountain View	Aurora	R&D Facility	1
	Mountain View	Gatik AI Inc.	Headquarters	1
	Mountain View	Ghost	Headquarters	1
	Mountain View	Kodiak	Headquarters	1
	Mountain View	NURO	Headquarters	1
	Mountain View	Qcraft	R&D Facility	1
	Mountain View	Waymo LLC	Headquarters	1
	Palo Alto	Apex.AI	Headquarters	1
	Palo Alto	Ford	R&D Facility	1
	Palo Alto	Luminar	R&D Facility	1
	Palo Alto	Woven Planet	R&D Facility	1
	Pasadena	Coast Autonomous	Headquarters	1
	Pasadena	General Motors	R&D Facility	1
	San Carlos	Zoox	R&D Facility	1
	San Diego	Qualcomm Technologies	Headquarters	1
	San Diego	TuSimple	Headquarters	1
	San Diego	Zoox	R&D Facility	1
	San Francisco	Aurora	R&D Facility	1
	San Francisco	Comma.ai	Headquarters	1
	San Francisco	Cruise	Headquarters	1
	San Francisco	Einride	R&D Facility	1
	San Francisco	Embark Trucks	Headquarters	1
	San Francisco	Faction	Headquarters	1
	San Francisco	Plus.ai	Headquarters	1
	San Francisco	Pronto.ai	Headquarters	1
	San Francisco	Waabi	R&D Facility	1
	San Francisco	Wayve	R&D Facility	1
	San Francisco	Zoox	R&D Facility	1
	San Jose	Black Sesame Technologies	R&D Facility	1
	San Jose	Cisco	Headquarters	1
	San Jose	Imagry	R&D Facility	1
	San Jose	NIO USA	Headquarters	1
	San Jose	NIO USA	R&D Facility	1
	San Jose	Pegasus Technology	Headquarters	1
	San Jose	Vueron	R&D Facility	1
	San Jose	WeRide	R&D Facility	1
	Santa Barbara	Continental	R&D Facility	1
	Santa Clara	Ambarella	Headquarters	1
	Santa Clara	Nissan	R&D Facility	1
	Santa Clara	Xmotors.ai	R&D Facility	1
	Santa Monica	Motional AD LLC	R&D Facility	1
	Silicon Valley	AutoX	R&D Facility	1
	Sunnyvale	Apollo Autonomous Driving	R&D Facility	1
	Sunnyvale	Mercedes-Benz Research & Development North America, In	R&D Facility	1
	Sunnyvale	Bosch	R&D Facility	1

AV Companies in U.S.

Appendix A

State	City	Company	Facility Type	Number of Facilities
Colorado	Boulder	HERE Technologies	R&D Facility	1
	Brighton	Outrider AI	Headquarters	1
	Denver	EasyMile	R&D Facility	1
	Louisville	Aurora	R&D Facility	1
Florida	Lake Nona	Beep	Headquarters	1
	Orlando	Luminar	Headquarters	1
Georgia	Alpharetta	HERE Technologies	R&D Facility	1
Massachusetts	Boston	Motional AD LLC	Headquarters	1
Maryland	Annapolis Junction	STEER Tech, LLC	Headquarters	1
Michigan	Ann Arbor	Ford	R&D Facility	1
	Ann Arbor	May Mobility	Headquarters	1
	Ann Arbor	M-City	R&D Facility	1
	Ann Arbor	Refraction AI	Headquarters	1
	Dearborn	Ford	Headquarters	1
	Detroit	General Motors	Headquarters	1
	Detroit	Intel/Mobileye	R&D Facility	1
	Detroit	Luminar	R&D Facility	1
	Flat Rock	Bosch	R&D Facility	1
	Lake Orion	General Motors	Manufacturing	1
	Novi	Harman	R&D Facility	1
	Plymouth	Bosch	R&D Facility	1
	Troy	Magna	R&D Facility	1
	Warren	General Motors	R&D Facility	1
	Wixom	Aurora	R&D Facility	1
Minnesota	Grand Rapids	May Mobility	R&D Facility	1
Montana	Bozeman	Aurora	R&D Facility	2
Nevada	Las Vegas	Motional AD LLC	R&D Facility	1
	Las Vegas	NURO	R&D Facility	1
	Las Vegas	Zoox	R&D Facility	1
New York	New York	Cortica	R&D Facility	1
	New York	Einride	R&D Facility	1
	New York	Waymo LLC	R&D Facility	1
	Port Washington	Autel	Headquarters	1
Pennsylvania	Pittsburgh	Argo AI, LLC	Headquarters	1
	Pittsburgh	Aurora	Headquarters	1
	Pittsburgh	Locomation	Headquarters	1
	Pittsburgh	Motional AD LLC	R&D Facility	1
	Pittsburgh	Waabi	R&D Facility	1
	Pittsburgh	Waymo LLC	R&D Facility	1
Texas	Austin	Einride	R&D Facility	1
	Dallas	Aurora	R&D Facility	1
	Dallas	Waymo LLC	R&D Facility	1
	Fort Worth	TuSimple	R&D Facility	1
	Plano	Ghost	R&D Facility	1
Washington	Seattle	Aurora	R&D Facility	1
	Seattle	Zoox	R&D Facility	1

On-Road AV Operations in U.S.

Appendix B

State	City	Company	Company Type	Number of Projects
Arkansas	Bentonville	Gatik AI Inc.	Self Driving Startup	1
Arizona	Chandler	Waymo LLC	Technology	4
	Peoria	Beep	Network/Fleet/Mobility	2
	Phoenix	Embark Trucks	Self Driving Startup	1
	Phoenix	Waymo LLC	Technology	1
	Phoenix	Cruise	Automaker	2
	Scottsdale	NURO	Self Driving Startup	1
	Tucson	TuSimple	Self Driving Startup	2
California	Atwater	Mercedes-Benz Research & Development North America, Inc.	Core Auto	1
	Atwater	Waymo LLC	Technology	1
	Badwater	Waymo LLC	Technology	1
	Barstow	Mercedes-Benz Research & Development North America, Inc.	Core Auto	1
	Bay Area	Mercedes-Benz Research & Development North America, Inc.	Core Auto	1
	Concord	LM Industries Group Inc	Network/Fleet/Mobility	1
	Contra Costa	NURO	Self Driving Startup	1
	Fontana	Embark Trucks	Self Driving Startup	1
	Fremont	DeepRoute AI	Technology	1
	Fremont	Hyundai	Core Auto	1
	Irvine	Pony.AI	Self Driving Startup	1
	Los Altos	Toyota	Core Auto	1
	Los Angeles	Mercedes-Benz Research & Development North America, Inc.	Core Auto	1
	Los Angeles	Vueron	Self Driving Startup	1
	McFarland	Mercedes-Benz Research & Development North America, Inc.	Core Auto	1
	Menlo Park	Didi Research America	Technology	1
	Mountain View	ailMotive	Self Driving Startup	1
	Mountain View	Aurora	Self Driving Startup	1
	Mountain View	NURO	Self Driving Startup	2
	Mountain View	Qcraft	Technology	1
	Mountain View	Waymo LLC	Technology	1
	Palo Alto	Argo AI, LLC	Self Driving Startup	1
	Palo Alto	Gatik AI Inc.	Self Driving Startup	1
	Rancho Cordova	LM Industries Group Inc	Network/Fleet/Mobility	1
	Sacramento	LM Industries Group Inc	Network/Fleet/Mobility	2
	Sacramento	Mercedes-Benz Research & Development North America, Inc.	Core Auto	1
	Sacramento	NURO	Self Driving Startup	1
	San Diego	Mercedes-Benz Research & Development North America, Inc.	Core Auto	1
	San Diego	Qualcomm Technologies	Technology	1
	San Francisco	Aurora	Self Driving Startup	1
	San Francisco	Cruise	Automaker	1
	San Francisco	Embark Trucks	Self Driving Startup	1
	San Francisco	Uber Advanced Technologies Group	Network/Fleet/Mobility	1
	San Francisco	Vueron	Self Driving Startup	1
	San Francisco	Waymo LLC	Technology	1
	San Francisco	Zoox	Technology	1
	San Jose	Imagry	Technology	1
	San Jose	WeRide	Technology	1
	San Mateo	Valeo	Self Driving Startup	1
	Santa Clara	Ambarella	Technology	1
	Santa Monica	Motional AD LLC	Self Driving Startup	1
	Sunnyvale	Apollo Autonomous Driving	Technology	1
	Sunnyvale	Apple	Technology	1
	Sunnyvale	Mercedes-Benz Research & Development North America, Inc.	Core Auto	2
Colorado	Denver	EasyMile	Network/Fleet/Mobility	1
	Golden	EasyMile	Network/Fleet/Mobility	3
	Westminster	EasyMile	Network/Fleet/Mobility	1
District of Columbia	Washington	Argo AI, LLC	Self Driving Startup	1
	Washington	Uber Advanced Technologies Group	Network/Fleet/Mobility	1

On-Road AV Operations in U.S.

Appendix B

State	City	Company	Company Type	Number of Projects
Florida	Clearwater Beach	Beep	Network/Fleet/Mobility	1
	Dunedin	Beep	Network/Fleet/Mobility	1
	Gainesville	TransDev Gainesville	(blank)	1
	Jacksonville	Beep	Network/Fleet/Mobility	1
	Jacksonville	Jacksonville Transportation Authority	(blank)	2
	Miami	Argo AI, LLC	Self Driving Startup	1
	Miami	Intel/Mobileye	Technology	1
	Miami	Waymo LLC	Technology	1
	Orlando	Beep	Network/Fleet/Mobility	5
	Port Saint Lucie	Beep	Network/Fleet/Mobility	1
	Saint Petersburg	Beep	Network/Fleet/Mobility	1
	Tampa	Beep	Network/Fleet/Mobility	1
Georgia	Peachtree Corners	Beep	Network/Fleet/Mobility	1
	Peachtree Corners	LM Industries Group Inc	Network/Fleet/Mobility	1
Indiana	Indianapolis	May Mobility	Network/Fleet/Mobility	1
Louisiana	New Orleans	Gatik AI Inc.	Self Driving Startup	1
Massachusetts	Boston	Motional AD LLC	Self Driving Startup	1
Maryland	Annapolis	STEER Tech, LLC	Self Driving Startup	1
	Baltimore	STEER Tech, LLC	Self Driving Startup	1
	Columbia	STEER Tech, LLC	Self Driving Startup	5
	Elkridge	STEER Tech, LLC	Self Driving Startup	1
	Jessup	STEER Tech, LLC	Self Driving Startup	1
	National Harbor	LM Industries Group Inc	Network/Fleet/Mobility	1
Michigan	Ann Arbor	May Mobility	Network/Fleet/Mobility	1
	Ann Arbor	NAVYA, Inc.	Network/Fleet/Mobility	1
	Ann Arbor	Toyota	Core Auto	1
	Ann Arbor	Yandex Inc	Technology	1
	Auburn Hills	EasyMile	Network/Fleet/Mobility	1
	Dearborn	Argo AI, LLC	Self Driving Startup	1
	Detroit	Intel/Mobileye	Technology	1
	East Lansing	ADASTEC CORP	Self Driving Startup	1
	Grand Rapids	May Mobility	Network/Fleet/Mobility	1
	Novi	Waymo LLC	Technology	1
Montana	Missoula	Embark Trucks	Self Driving Startup	1
North Carolina	Kill Devil Hills	EasyMile	Network/Fleet/Mobility	1
Nebraska	Lincoln	NAVYA, Inc.	Network/Fleet/Mobility	1
New Mexico	Las Cruces	Embark Trucks	Self Driving Startup	1
Nevada	Las Vegas	aiMotive	Self Driving Startup	1
	Las Vegas	Mercedes-Benz Research & Development North America, Inc	Core Auto	1
	Las Vegas	Motional AD LLC	Self Driving Startup	2
	Las Vegas	NAVYA, Inc.	Network/Fleet/Mobility	1
	Las Vegas	NURO	Self Driving Startup	1
	Las Vegas	STEER Tech, LLC	Self Driving Startup	1
	Las Vegas	Zoox	Technology	1
New York	Buffalo	LM Industries Group Inc	Network/Fleet/Mobility	1
Ohio	Akron	LM Industries Group Inc	Network/Fleet/Mobility	1
	Columbus	EasyMile	Network/Fleet/Mobility	2
Oklahoma	Oklahoma City	Kodiak	Self Driving Startup	1
Pennsylvania	Pittsburgh	Argo AI, LLC	Self Driving Startup	1
	Pittsburgh	Aurora	Self Driving Startup	1
	Pittsburgh	Motional AD LLC	Self Driving Startup	1
	Pittsburgh	Uber Advanced Technologies Group	Network/Fleet/Mobility	2

On-Road AV Operations in U.S.

Appendix B

State	City	Company	Company Type	Number of Projects
Texas	Arlington	May Mobility	Network/Fleet/Mobility	2
	Austin	Argo AI, LLC	Self Driving Startup	1
	Austin	Cruise	Automaker	1
	Austin	EasyMile	Network/Fleet/Mobility	1
	Austin	Refraction AI	Self Driving Startup	1
	Austin	Waymo LLC	Technology	1
	Bryan	Embark Trucks	Self Driving Startup	1
	College Station	NAVYA, Inc.	Network/Fleet/Mobility	1
	Dallas	Aurora	Self Driving Startup	2
	Dallas	EasyMile	Network/Fleet/Mobility	1
	Dallas	Kodiak	Self Driving Startup	1
	Dallas	STEER Tech, LLC	Self Driving Startup	1
	El Paso	Embark Trucks	Self Driving Startup	1
	Fort Worth	Gatik AI Inc.	Self Driving Startup	1
	Houston	NURO	Self Driving Startup	4
	Houston	Waymo LLC	Technology	1
	Katy	Embark Trucks	Self Driving Startup	1
Utah	Farmington	EasyMile	Network/Fleet/Mobility	1
	Park City	EasyMile	Network/Fleet/Mobility	1
	Salt Lake City	EasyMile	Network/Fleet/Mobility	3
	Sandy	EasyMile	Network/Fleet/Mobility	1
	St. George	EasyMile	Network/Fleet/Mobility	1
	West Valley City	EasyMile	Network/Fleet/Mobility	1
Virginia	Arlington	LM Industries Group Inc	Network/Fleet/Mobility	1
Washington	Kirkland	Waymo LLC	Technology	1
	Seattle	Zoox	Technology	1
Wisconsin	Madison	NAVYA, Inc.	Network/Fleet/Mobility	1
Wyoming	Yellowstone	Beep	Network/Fleet/Mobility	1

New in 2022: On-Road AV Programs in U.S.

Appendix C

State	City	Company	Company Type	Number of Programs
Arizona	Peoria	Beep	AV Startup	1
	Phoenix	Waymo LLC	AV Startup	1
	Phoenix	Cruise	Automaker	1
	Tucson	TuSimple	AV Startup	1
California	Los Angeles	Vueron	AV Startup	1
	San Francisco	Cruise	Automaker	1
	San Francisco	Vueron	AV Startup	1
	San Francisco	Waymo LLC	AV Startup	1
	Santa Monica	Motional AD LLC	AV Startup	1
Florida	Dunedin	Beep	AV Startup	1
	Miami	Argo AI, LLC	AV Startup	1
	Miami	Intel/Mobileye	Technology	1
Michigan	East Lansing	ADASTEC CORP	AV Startup	1
Montana	Missoula	Embark Trucks	AV Startup	1
Nevada	Las Vegas	Motional AD LLC	AV Startup	1
Oklahoma	Oklahoma City	Kodiak	AV Startup	1
Texas	Arlington	May Mobility	AV Startup	1
	Austin	Argo AI, LLC	AV Startup	1
	Dallas	Aurora	AV Startup	2
	Dallas	Kodiak	AV Startup	1
	Dallas	STEER Tech, LLC	AV Startup	1

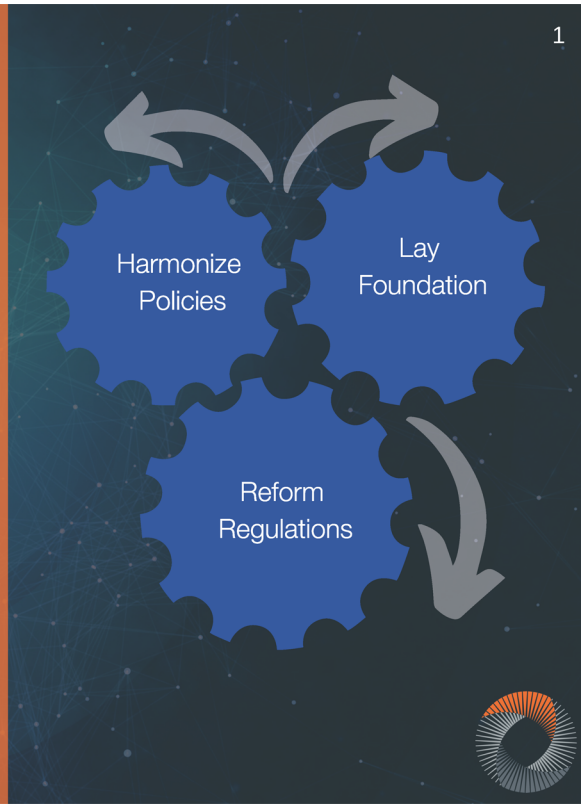
January - June 2022


ALLIANCE
FOR AUTOMOTIVE
INNOVATION
POLICY ROADMAP TO ADVANCE
AUTOMATED VEHICLE INNOVATION
A Four-Year Plan to Revolutionize Transportation

We are at a pivotal time on the pathway to a cleaner, safer, and smarter transportation future. There is no doubt that Level 3-5 automated vehicles (AVs) are an important component of this future.

Focused and sustained leadership from policymakers is required to ensure this technology and the benefits it can deliver are realized. To that end, the Alliance for Automotive Innovation puts forward this FOUR-YEAR ACTION PLAN for federal policymakers to significantly advance the testing and deployment of AV technologies in the United States.

The 14 specific recommendations contained within this plan fall within the following pillars: (1) Reform Regulations to Allow for AV Deployment at Scale; (2) Harmonize Federal, State, and International Policies; and (3) Lay the Foundation to Achieve Longer-Term Objectives.



PILLAR 1
REFORM REGULATIONS TO ALLOW FOR AV DEPLOYMENT AT SCALE

RECOMMENDATION 1
CREATE A NEW VEHICLE CLASS FOR AVs

The U.S. Department of Transportation (DOT) should create a new vehicle class within the Federal Motor Vehicle Safety Standards for AVs. Since the current regulations were not written with AVs in mind, a number of existing standards assume the presence of a human driver and therefore present a barrier to the deployment of AVs without conventional driver controls. An AV class would enable the DOT to efficiently identify and categorize existing motor vehicle safety standards that should apply to AVs without impacting the applicability of those standards for conventionally driven vehicles. Although this approach would allow for AVs to be incorporated into the existing regulatory framework sooner, if a new vehicle class is not established, DOT should complete its efforts to update existing motor vehicle safety standards as expeditiously as possible.

RECOMMENDATION 2
CLARIFY APPLICABILITY OF "MAKE INOPERATIVE" PROHIBITION

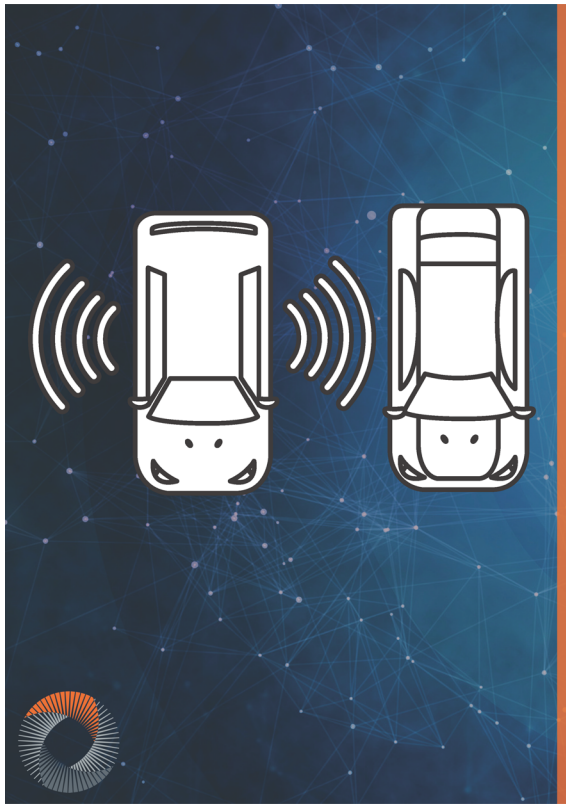
Existing DOT regulations prohibit manufacturers from knowingly making inoperative any feature or system installed on or in a motor vehicle in compliance with an applicable motor vehicle safety standard. This prohibition could have unintended implications for "dual mode" vehicles that are equipped with selectable AV features that temporarily deactivate conventional driver controls while the vehicle is operating safely in "autonomous mode." To address this, DOT should confirm that the deactivation of conventional driver controls in "dual mode" vehicles, when the vehicle is in AV mode, does not fall under the "make inoperative" prohibition if the vehicle is compliant with all applicable motor vehicle safety standards while in manual driving mode.

RECOMMENDATION 3
ESTABLISH A NATIONAL AV PILOT PROGRAM

DOT should establish a robust national pilot program for AV testing and deployment. Such a program would not only provide a venue to advance DOT research objectives relating to AVs, but also provide AV developers that choose to participate with an alternative pathway to AV testing and deployment. A focused pilot program carried out under DOT's oversight could increase public exposure to the technology and provide the DOT with the data that it will need to create new safety regulations for AVs.

RECOMMENDATION 4
IMPROVE THE EXEMPTION PETITION PROCESS

Current law authorizes DOT to grant manufacturers exemptions from existing safety standards provided that vehicle safety is upheld. As the safety standards are being updated in line with RECOMMENDATION 1, DOT should simplify and streamline the existing exemption process for AVs to provide greater clarity to manufacturers. As part of this effort, DOT should issue guidance that specifies what data is required as part of the exemption application.



RECOMMENDATION 5
RAISE THE CAP ON EXEMPTIONS FOR AVs

To provide for meaningful AV deployments, the U.S. Congress should enact legislation to increase the existing cap on temporary exemptions that can be granted to AVs. Under existing law, exemptions are limited to 2,500 vehicles per manufacturer annually and valid for a two-year duration. Increasing this limit will promote continued development of this technology in the United States by providing certainty to AV developers that there is a near-term path to deploy AV technologies. Raising the cap will also lead to the generation of more real-world data to support any efforts by DOT to enact new AV-specific regulations.

RECOMMENDATION 6
EMBRACE INNOVATIVE REGULATORY APPROACHES

DOT should embrace innovative regulatory approaches that are appropriately matched to the current pace of technological advancement. As part of the federal motor vehicle safety regulatory compliance and the exemption petition process, DOT should permit manufacturers to submit vehicle-specific technical design and/or build documentation. This “technical documentation” approach would accommodate unique design solutions and would empower manufacturers to use innovative safety assurance techniques, such as virtual testing with validated simulators. In addition, DOT should allow for the use of a surrogate vehicle (i.e., a vehicle that shares the same platform as the AV but has conventional driver controls) to perform certain regulatory compliance tests.

PILLAR 2
HARMONIZE FEDERAL, STATE, AND INTERNATIONAL POLICIES

RECOMMENDATION 7
MAINTAIN TRADITIONAL FEDERAL AND STATE ROLES

The U.S. Congress should enact legislation to clarify federal and state roles related to AVs. The federal government should maintain responsibility for the design, construction, and performance of motor vehicles, while states should continue to oversee licensing of human drivers, registration, insurance, and traffic laws.

RECOMMENDATION 8
COORDINATE STATE AV POLICIES

The current patchwork of AV laws and regulations at the state level presents challenges for manufacturers seeking to test and deploy AVs in multiple states. AV testing and deployment across state lines could be significantly improved if states coordinated with each other and sought to ensure consistency of AV laws and regulations. A federal grant program could be established to provide funding to states that agree to work together to harmonize policies that govern the testing and deployment of AVs. In addition, a unified approach to AV licensing and registration should be encouraged.

RECOMMENDATION 9
ALIGN STATE TRAFFIC LAWS

Variation in state traffic laws creates additional challenges for AV developers. AV developers must translate each state's traffic laws into the system's programming and capture even the slightest differences, and then continuously monitor state laws for any updates or changes. To the extent possible, states should be encouraged to harmonize traffic laws and regulations, particularly those that apply to the operation of AVs on public roads. Uniformity of state traffic laws and regulations would provide benefits not only to AV developers, but also to any road user who crosses state lines. At a minimum, a single resource of state traffic laws and real-time updates to those laws that is accessible to AV developers should be created. In addition, states should review their existing laws and identify any provisions that would prevent the deployment of AVs.

RECOMMENDATION 10
LEAD IN INTERNATIONAL FORUMS

Many AV companies, including those developing this technology in the United States, may deploy in global markets. For this reason, international alignment on AV testing and deployment regulations is helpful. DOT should actively participate in international forums, like the United Nations Economic Commission for Europe, where AV policy is being developed. DOT should also strive to implement a national AV policy framework that is reasonably aligned with international rules within the bounds of the U.S. self-certification regulatory regime.

PILLAR 3
LAY THE FOUNDATION TO ACHIEVE LONGER TERM GOALS

RECOMMENDATION 11
PROMOTE INDUSTRY STANDARDS

Industry consensus standards play an important role in the deployment of new vehicle technologies. Standards Developing Organizations (such as ISO, IEEE, and SAE) provide a neutral forum for technical experts to reach consensus on foundational elements of AV design. This alignment around effective practices helps to advance safety and increase public trust in the technology. To that end, policymakers should support and appropriately leverage the development of these industry standards.

RECOMMENDATION 12
BUILD KNOWLEDGE FOR A SAFETY ASSURANCE FRAMEWORK

DOT should encourage research and seek input from industry stakeholders to inform the development of a national AV safety assurance framework. Above all, to provide the necessary leadership and to facilitate meaningful progress on the testing and deployment of AV technology in the United States, it is important that DOT stay abreast of the latest advancements in AV technology.

RECOMMENDATION 13
PREPARE ROADWAY INFRASTRUCTURE FOR AVs

Roadway infrastructure can help facilitate the deployment of AV technology. For example, AV performance will benefit from consistent and well-maintained lane markings, signage, and traffic control devices. DOT should revise the Manual on Uniform Traffic Control Devices (MUTCD) to include items that will support and facilitate AV deployment. States should be encouraged and even incentivized to update their infrastructure consistent with any AV-related MUTCD update.

RECOMMENDATION 14
SUPPORT U.S. LEADERSHIP ON AVs

In addition to creating a regulatory environment that allows for AV deployment in the United States (as described in the above recommendations), policymakers should explore additional policies to ensure that the United States maintains a leadership role in the development of AV technologies. This could include specific tax or other incentives that support the research, development, manufacturing, and deployment of AVs in the United States. In addition, policymakers should adopt policies that strengthen the AV workforce pipeline and create a pathway for qualified AV developers to safely test their vehicles on public roads with NHTSA oversight. Finally, restrictions on the ability of developers to commercialize AV technologies should be avoided or eliminated.

BENEFITS OF THIS FOUR-YEAR ACTION PLAN

Includes two pathways to AV deployment, both with DOT oversight

Since the current exemption process might not make sense for some AV developers, a new pilot program would create a second option, designed specifically for AVs and created with existing DOT authorities.

Defines federal and state roles

With a clear alignment of state and federal roles, each are empowered to take actions that strengthen - rather than confuse - the policy landscape.

Paves the way for long-term national success

The steps policymakers take today will have implications for years to come. If we work together to get it right, we will reap the benefits of a safer, cleaner, and smarter transportation system.

FRANK PALLONE, JR., NEW JERSEY
CHAIRMAN

CATHY McMORRIS RODGERS, WASHINGTON
RANKING MEMBER

ONE HUNDRED SEVENTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115
Majority (202) 225-2927
Minority (202) 225-3641

September 9, 2021

The Honorable Pete Buttigieg
Secretary
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, D.C. 20590

Secretary Buttigieg:

The Committee on Energy and Commerce has a long bipartisan history in ensuring that the United States remains the leader and premier destination to innovate and deploy emerging technologies like artificial intelligence (AI). The single greatest safety application of AI we will see for our citizens and our economic security is in the automotive sector, and specifically its application in autonomous vehicles (AV). We are very concerned by recent reports of U.S. officials approving licensing applications for Huawei Technologies Company (Huawei), China's blacklisted telecommunications company, to purchase semiconductors for its next generation vehicles.[1]

The previous administration sought to minimize Huawei's ability to obtain U.S. semiconductors when the Department of Commerce (DOC) added the company and many of its non-U.S. affiliates to its Entity List and issued a final rule restricting Huawei from acquiring foreign-produced semiconductors that are the direct product of certain U.S. software and technology.[2] Furthermore, the Federal Communications Commission (FCC) designated Huawei as a national security threat due to its strong ties to the Chinese Communist Party (CCP), which uses the country's laws to assist in espionage activities and exploit known cybersecurity risks

[1] https://www.reuters.com/business/autos-transportation/exclusive-us-approves-licenses-huawei-buy-auto-chips-sources-2021-08-25/
[2] https://sanctionsnews.bakermckenzie.com/us-commerce-department-expands-huawei-and-entity-list-related-rules-further-restricting-huaweis-access-to-semiconductors-produced-from-us-technology-and-software/

and vulnerabilities in equipment.[3] These policies have long been bipartisan initiatives, and we should not retreat from them, especially when our standing on the world stage is being challenged.

During your confirmation hearing, you spoke of advancing the next generation automotive sector. As the Secretary of the Department of Transportation (DOT), you have the opportunity to help the American automotive workforce keep their jobs in the decades ahead and avoid what happened to the communications equipment sector. AVs are also essential for the future mobility of our seniors and those with disabilities as a new source of freedom. We must not surrender to China and its efforts to dominate our high-tech sectors, including AVs. It is concerning that, unlike other cabinet secretaries, neither you nor the National Highway Traffic Safety Administration (NHTSA) were consulted as part of the process to review these transfers to Huawei.

While the export laws are clear about the confidentiality of what is approved, it is important that what is considered a mature component for cameras and sensors, for example, may not consider that "the whole is indeed greater than the sum of its parts." The news of the approval last week unfortunately reflects how Democrats in Congress continue to ignore this next generation technology, walking away from landmark, bipartisan AV legislation that unanimously passed the House just a few years ago. They have ignored seniors and those with disabilities who need this technology as a new means of mobility. They have surrendered both to the Teamsters, who are making unrelated demands concerning commercial vehicles, and trial lawyers, who hope to profit from frivolous litigation.

As you know, news of the approvals also arrives with the backdrop of a semiconductor shortage for many U.S. sectors, from automotive to health to energy. As the world continues to rebound from COVID-19 and related supply chain shortages, we must do everything we can to protect and secure our domestic sector needs. We believe that was the intent of the Senate when it passed the U.S. Innovation and Competition Act (USICA), which would establish grant programs to incentivize the supply chain of semiconductors and microelectronics here at home.

Therefore, we ask that you respond to the following no later than September 23, 2021:

1. Are you aware of Huawei's intentions to purchase semiconductors and further its automotive ambitions?

2. Should Huawei have the ability to purchase semiconductors for next generation vehicles? If yes, please explain.

3. Has DOT reviewed the security of U.S. interests in the global semiconductor supply chain and whether U.S. companies are able to accommodate their domestic interests? Please explain how the approval of semiconductor technology transfers, whether mature or leading-edge technology, will or will not benefit the U.S.

---

[3] https://docs.fcc.gov/public/attachments/DOC-365255A1.pdf

4. According to a Reuters report, automotive chips are not generally considered sophisticated when compared to chips in other sectors. The report also refers to comments made by a Huawei spokesperson who said "[They] are positioning [themselves] as a new component provider for intelligent connected vehicles. . . ." Do you believe Huawei intends to do with the automotive sector what it did to the communications equipment sector?

5. How will the purchase of non-Chinese automotive semiconductor technology impact the economic pressure facing Huawei, both for the company in general and its 5G telecommunications division specifically? Are you concerned that such transactions ease the pressure on China's supply chain for the automotive sector so it may further prioritize its state-sponsored goal in winning the race to 5G?

6. Are you concerned that Huawei will look for a foothold in developing components for future vehicles in order to gather information on Americans and our transportation infrastructure?

7. Will any component designed for an intelligent automobile licensed or manufactured by Huawei be prohibited from being used in automobiles destined for the U.S.?

8. Will you consult and coordinate with the other cabinet secretaries and share any concerns that efforts to support Huawei will ultimately benefit the CCP at the expense of U.S. jobs and the economy, including entrenching China's state-sponsored supply chains?

9. Will you commit that neither you nor NHTSA will approve such technology transfers in the future?

10. Please provide your estimates on how many American manufacturing jobs will be lost if the U.S. does not lead in enacting a national framework for AVs.

11. Please provide your estimates on how much revenue will be lost and not contributed to the U.S. economy if the U.S. does not lead in enacting a national framework for AVs.

12. Will you commit to supporting the inclusion of bipartisan AV legislation in USICA before it comes the House floor for consideration?

In President Biden's April speech announcing the withdrawal from Afghanistan, he emphasized the need for the U.S. to focus on China, saying "We have to shore up American competitiveness to meet the stiff competition we're facing from an increasingly assertive China."[4] Bloomberg reported in May that the U.S. lead in automotive semiconductors is slipping, and China has a much more favorable regulatory environment.[5] AV development and deployment is a clear case of American competitiveness being compromised. We hope you and the

[4] https://www.wsj.com/articles/afghanistan-u-s-withdrawal-china-russia-power-relations-11630421715

[5] https://www.bloomberg.com/news/newsletters/2021-05-04/hyperdrive-daily-china-ramps-up-its-autonomous-vehicle-development

Administration will work with Republicans to enact AV legislation, which will support the U.S. automotive sector.

If you or your team have any questions about our request, please contact Tim Kurth at the Committee on Energy and Commerce at (202) 225-3641. We appreciate your prompt attention to this matter.

Sincerely,

Cathy McMorris Rodgers
Republican Leader

Gus M. Bilirakis
Republican Leader
Subcommittee on Consumer Protection
and Commerce

Robert E. Latta
Member of Congress

Michael C. Burgess, M.D.
Member of Congress

Adam Kinzinger
Member of Congress

H. Morgan Griffith
Member of Congress

Larry Bucshon, M.D.
Member of Congress

Earl L. "Buddy" Carter
Member of Congress

Neal P. Dunn, M.D.
Member of Congress

Debbie Lesko
Member of Congress

Greg Pence
Member of Congress

John Joyce, M.D.
Member of Congress

Kelly Armstrong
Member of Congress

AMENDMENT TO RULES COMMITTEE PRINT 117-8

OFFERED BY M__. _____

Page 1508, after line 13, add the following new section (and update the table of contents accordingly):

SEC. 10109. DISABILITY LICENSING ACCESSIBILITY.

(a) LICENSING.—

(1) IN GENERAL.—A State may not issue a motor vehicle operator's license for the operation or use of a highly automated vehicle in a manner that discriminates on the basis of disability (as defined in section 3 of the Americans with Disabilities Act of 1990 (42 U.S.C. 12102)).

(2) DEFINITIONS.—In this subsection:

(A) AUTOMATED DRIVING SYSTEM.—The term "automated driving system" means the hardware and software that are collectively capable of performing the entire dynamic driving task on a sustained basis, regardless of whether such system is limited to a specific operational design domain.

(B) HIGHLY AUTOMATED VEHICLE.—The term "highly automated vehicle" means—

(i) means a motor vehicle equipped with an automated driving system; and

(ii) does not include a commercial motor vehicle (as defined in section 31101 of title 49, United States Code).";

(b) DISABILITY EXEMPTION CLASS.—Paragraph (3)(B) of section 30113 of title 49, United States Code, is amended—

(1) in clause (iii), by striking "; or" and inserting a semicolon; and

(2) by striking clause (iv) and inserting the following:

"(iv) compliance with the standard would prevent the manufacturer from selling, introducing, or delivering into interstate commerce a motor vehicle with an overall safety level at least equal to the safety level of nonexempt vehicles; or

"(v) the exemption would provide—

"(I) transportation access for individuals with disabilities (as defined in section 3 of the Americans with Disabilities Act of 1990 (42 U.S.C. 12102)), including non-visual access

for individuals who are blind or visually impaired; and

"(II) either—

"(aa) a safety level at least equal to the safety level of the standard from which the exemption is sought; or

"(bb) an overall safety level at least equal to the overall safety level of non-exempt vehicles.".

☒

June 28, 2021

The Honorable Jim McGovern
Chair
United States House Committee on Rules
370 Cannon House Office Building
Washington, DC 20515

The Honorable Tom Cole
Ranking Member
United States House Committee on Rules
2207 Rayburn House Office Building
Washington, DC 20515

Dear Chair McGovern and Ranking Member Cole:

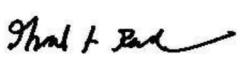
The National Federation of the Blind, the nation's transformative civil rights organization of the blind, supports and endorses the amendment to the INVEST in America Act filed by Representative Bilirakis that will prohibit discriminatory licensing practices for highly automated vehicles and create an exemption classification for manufacturers who provide transportation access for people with disabilities.

Subsection (a) of the amendment would mandate that a state "may not issue a motor vehicle operator's license for the operation or use of a highly automated vehicle in a manner that discriminates on the basis of disability." This will ensure that current requirements necessary to obtain a driver's license, like a vision test, will not be required to operate or use a highly automated vehicle. We are pleased to see this subsection included in the amendment because highly automated vehicles will pilot themselves (SAE Level 4 and Level 5), making a vision requirement arbitrary and discriminatory.

Subsection (b) of the amendment would create an exemption category under the federal motor vehicle safety standards located in Section 30113 of title 49 United States Code that would "provide transportation access for individuals with disabilities, including non-visual access for individuals who are blind or visually impaired." This addition to the law will provide the incentive needed for automobile manufacturers to ensure that the unique requirements for Americans with disabilities to be able to operate automated vehicles are considered in the early stages of development.

Highly automated vehicles have the potential to revolutionize the transportation landscape, especially for individuals with disabilities. However, individuals with disabilities who stand to gain the most from the creation and proliferation of highly automated vehicles could be left out of this new frontier if specific actions are not taken. Representative Bilirakis's amendment to the INVEST in America Act is an important step to ensure that America's journey toward automotive automation is fully inclusive of those who will benefit most.

Sincerely,



Mark A. Riccobono, President
National Federation of the Blind

National Federation of the Blind
Mark Riccobono, *President* | 200 East Wells Street *at Jernigan Place* Baltimore, MD 21230 | 410 659 9314 | www.nfb.org

JTA, Beep & NAVYA AVs Help Transport COVID-19 Tests Collected at Mayo Clinic Drive-Thru

jtafla.com/media-center/news-stories/jta-beep-navya-avs-help-transport-covid-19-tests-collected-at-mayo-clinic-drive-thru

News StoriesThursday, April 2, 2020 at 12:00 AM

The Jacksonville Transportation Authority (JTA), Beep Inc. and NAVYA partner with Mayo Clinic to safely transport COVID-19 samples on their Jacksonville Campus

JACKSONVILLE, (APRIL 2, 2020) – For the first time in the United States, autonomous vehicles are being used to transport medical supplies and COVID-19 tests at Mayo Clinic in Florida.

At a time when healthcare resources and personnel are stretched thin, the Jacksonville Transportation Authority (JTA) has partnered with Beep and NAVYA to use autonomous vehicles to facilitate the safe transport of COVID-19 tests collected at a drive-thru testing location at Mayo Clinic in Florida.

"This deployment is a historic moment for the Jacksonville Transportation Authority," said JTA Chief Executive Officer Nathaniel P. Ford Sr. "Along with our partners Beep, NAVYA and Mayo Clinic, we are leveraging our learnings from three years of testing autonomous vehicles through our Ultimate Urban Circulator program. Our innovative team saw this as an opportunity to use technology to respond to this crisis in Northeast Florida and increase the safety of COVID-19 testing."

On Monday, March 30, 2020, up to four autonomous vehicles began operating along an initial route, in full autonomous mode without attendants or other people onboard, to transport COVID-19 tests from a drive-thru testing site to a processing laboratory on Mayo Clinic's campus. The COVID-19 test samples are placed in secure containers prior to Mayo Clinic healthcare professionals loading the samples onto the shuttle.

"During a time of rapid change and uncertainty, the ability to think innovatively alongside the Jacksonville Transportation Authority, NAVYA, and Beep during the pandemic has strengthened all of our teams through community collaboration," said Kent Thielen, M.D., CEO, Mayo Clinic in Florida. "Using artificial intelligence enables us to protect staff from exposure to this contagious virus by using cutting edge autonomous vehicle technology, and frees up staff time that can be dedicated to direct treatment and care for patients. We are grateful to JTA, Beep, and NAVYA for their partnership in these challenging times."

The JTA, Beep, NAVYA and Bestmile teams partnered to create, test and deploy the routes for the autonomous vehicles at Mayo Clinic in Florida to address the fluid developments of the COVID-19 pandemic. The routes are isolated from pedestrians, traffic and staff. Beep, Mayo Clinic and the JTA will closely monitor the service from a mobile command center to maintain safe operation.

"Mayo Clinic is known as a leader in innovation and technology for providing world-class healthcare services to their patients in so many important areas of medicine," said Joe Moye, CEO, Beep, Inc. "It is both humbling and exciting to partner with them in bringing this innovative solution to support such a critical challenge facing our country. We are equally as proud to work with our partners at the JTA, NAVYA and Bestmile, a fleet orchestration and optimization software company, in making this happen and doing our part to support this important cause."

Beep, an autonomous shuttle fleet service provider, transported the shuttles through Eagle Express Inc. from Lake Nona, Florida, an innovation hub 150 miles away where the company is headquartered in Orlando, Florida. An additional shuttle is being utilized from the JTA's Ultimate Urban Circulator (U2C) program. The JTA has actively tested AV technology since 2017 to prepare for a conversion and expansion of its Skyway automated people mover in Downtown Jacksonville into a network powered by autonomous vehicles.

"The opportunity to work together with these organizations in an effort to provide a dedicated COVID-19 testing solution represents our goal as a company, and that's to create a more accessible solution in the moments that matter, whether that be crisis, shortage in manpower and resources, or other areas we can provide aid in," said Étienne Hermite, CEO of NAVYA.

The use of the autonomous vehicles to safely transport and handle the COVID-19 samples is another example of how these vehicles can be repurposed in times of need.

CONTACT INFORMATION

David Cawton II
Jacksonville Transportation Authority (JTA)
(904) 239-7989, dcawton@jtafla.com

Tia R. Ford
Mayo Clinic Jacksonville
(904) 953-1419, ford.tia@mayo.edu

Erica Olson
Beep Inc./Merit Mile
(763) 458-4435, eolson@meritmile.com

Travis Ockerman
NAVYA North America
(734) 787-0047, travis.ockerman@navya.tech

MEDIA KIT

DOWNLOAD THE MEDIA KIT (B-ROLL) DOWNLOAD PHOTOS

Photos courtesy of Mayo Clinic

ABOUT MAYO CLINIC

Mayo Clinic is a nonprofit organization committed to innovation in clinical practice, education and research, and providing compassion, expertise and answers to everyone who needs healing. Visit the Mayo Clinic News Network for additional Mayo Clinic news and An Inside Look at Mayo Clinic for more information about Mayo.

ABOUT BEEP

Beep, Inc. ("Beep") founded by experienced fleet managers and technology entrepreneurs, offers the next generation of transportation services for autonomous passenger mobility to fleet owners and operators in low speed environments across the public and private sector, including transportation hubs, medical and university campuses, residential communities, town centers, and more. Beep's operations are headquartered in Lake Nona, Orlando. Learn more about Beep on their website.

ABOUT THE JACKSONVILLE TRANSPORTATION AUTHORITY (JTA)

The Jacksonville Transportation Authority (JTA) is an independent agency of the state of Florida, serving Duval County, with multi-modal responsibilities. The JTA designs and constructs bridges and highways and provides varied mass transit services. These include express and regular bus service, monorail, ferry and on-demand services. The JTA serves the largest city in the continental U.S. in terms of landmass. An integrated transportation network is a critical element in any community to properly manage growth, provide mobility and offer a good quality of life. Learn more at their website.

ABOUT NAVYA

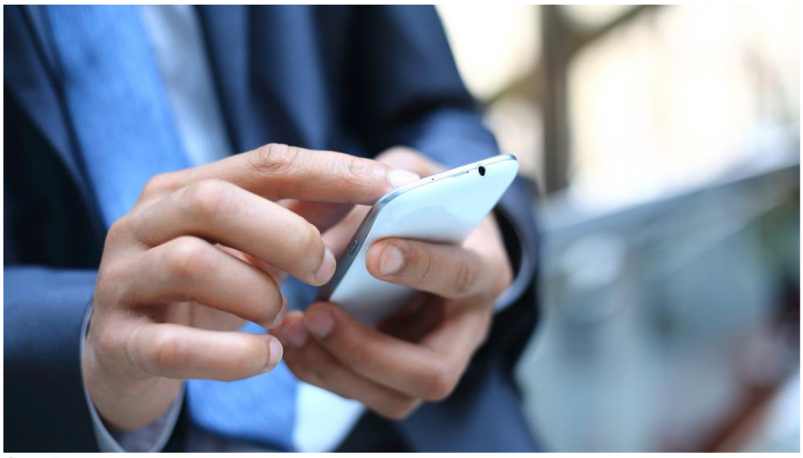
NAVYA is a top French name in autonomous driving systems. With over 280 employees in France (Paris and Lyon) and in the United States (Saline, Michigan), NAVYA is a leading specialist in the supply of autonomous driving systems for passenger and goods transport. Since 2015, NAVYA has been the first to market and put into service autonomous mobility solutions in cities and private sites across the globe. For more information, visit their website.

OPINION > CYBERSECURITY

THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

Tuya may be the China threat that beats Russia's ransomware attacks

BY HAL BRANDS AND KLON KITCHEN, OPINION CONTRIBUTORS - 07/30/21 12:00 PM ET



Getty Images

In May, Americans lined up at gas stations for days because of a Russian ransomware attack. Recently, a similar Russia-sourced attack struck a large group of companies via software used by IT departments to manage remote computers. But those attacks are about money, not about power or information, and a little-known Chinese technology company, Tuya, is on the verge of being able to blow Russian hackers away.

Tuya, a nominally private Chinese company backed by Beijing-government crony Tencent, takes "things" and makes them "smart" by connecting them to the internet, a function known as "platform as a service," or PaaS. Tuya dominates the global "internet of things" (IoT)/PaaS market. It operates from Hangzhou City, China, and its hardware, software, cloud services and applications power more than 100 million "smart" devices in 1,100 product categories in 220 countries — including consumer products, surveillance equipment, and manufacturing and supply chain applications.

More than 600 of the world's leading brands use the company to power their own IoT devices sold at Walmart, Nordstrom, Amazon, Target and elsewhere. Tuya's market domination translated into a March 2021 listing on the New York Stock Exchange and more than $900 million in new investment. Strangely,

however, that access has brought little scrutiny — even in light of new focus on Chinese efforts to corner the market in next-gen tech.

Over the past few years, the United States and at least 20 other countries have either banned or significantly restricted China's Huawei telecommunications company from building or managing 5th Generation (5G) networks. Their motive? Fear that the company could siphon the masses of data — including classified government data — created and shared on its networks, and make it available to the Chinese government.

Remember, China's Data Security Law dictates that both private and state or partially state-owned or controlled corporations must cede control over user data to the Beijing government.

The alarm that has spread from Washington to Europe and Asia over 5G makes sense. The technology means an unprecedented 20-fold increase in data flow. And it is just that expansion that is enabling the rapidly exploding internet of things, and a world where the internet is omnipresent. Enter Tuya. This one Chinese company alone soon may control hundreds of millions more "smart" devices enabled by 5G — even non-Huawei 5G — essentially rolling back any progress made in defending proprietary personal or government data from China's ruling Communist Party.

A recent investigation by cybersecurity firm Dark Cubed found that Tuya-powered devices "had at least one network connection to servers based in China … failed basic security checks … provided complete visibility into private images to anyone in the network … [and] are woefully insecure and sending data to China." In other words, Tuya may well be funneling the information picked up on home security cameras and connected health devices — just to name two examples — back to Beijing.

U.S. law makes it illegal for companies to provide this data to the Chinese government, but enforcing that law is difficult — especially when Beijing assists companies in hiding their actions. Meanwhile, naysayers insist all such arguments are little more than alarmism or xenophobia. But consider the precedents.

In 2009, the Dutch telecommunications company KPN used technology provided by Huawei in its networks. An internal risk assessment, which only came to light years later, reportedly concluded that this access allowed Huawei to monitor all conversations on KPN networks, including those by the Dutch prime minister. And the internet of things only adds vulnerability: In 2016, the so-called Mirai botnet attack took over more than 600,000 smart devices and used them to temporarily shut down much of the internet on the East Coast. That attack was the work of criminals, but it foreshadows the sort of trouble a determined state actor — with access to a far larger number of devices — could cause.

Fortunately, the United States has options. The Biden administration has extended a 2019 Executive Order on Securing the Information and Communications Technology and Services (ICTS) Supply Chain, which gives the Secretary of Commerce the authority to review — and deny — "any acquisition, importation, transfer, installation, dealing in, or use of any [ICTS products] that has been designed, developed, manufactured, or supplied" by persons owned, controlled, subject to, or at the direction of foreign adversaries, which "poses certain undue or unacceptable risks."

Tuya appears to meet that definition and Congress should consider barring it from operating in the United States and from doing business with U.S. companies. There are alternative IoT/PaaS offerings

from companies in the U.S. and other trusted nations. It's time for better U.S. leadership, before it's too late.

Hal Brands is a senior fellow at the American Enterprise Institute, where he studies U.S. foreign policy and defense strategy, and a professor at the Johns Hopkins University School of Advanced International Studies.

Klon Kitchen is a senior fellow at the American Enterprise Institute, where he studies emerging technologies and national security. He is an adviser to Afero, an American IoT/PaaS company.

Editor's note: In response to this article, Tuya states that, since March 2021, it has been a publicly traded Chinese company whose investors include Tencent, operating internationally with local headquarters in the U.S., India, Germany, Colombia, China and Japan. Regarding the potential for sharing data with the Beijing government, Tuya states that all user data on its platform is assigned to specific regional data centers, according to the users' locations, and that servers operate independently with no connection to China. Regarding IoT devices and 5G technology, Tuya states that the consumer IoT devices it supports do not use 5G technology related to base station infrastructure and have no cooperation or association with Huawei or other 5G technology service providers. And regarding the investigation by Dark Cubed, Tuya says the IPC products mentioned in the report are not devices developed by Tuya and the specific domain requested by those products belongs to the IPC manufacturer. Tuya says it welcomes fair-market competitions around the globe, to facilitate healthy and orderly IoT development.

February 1, 2023

The Honorable Gus Bilirakis
Chairman
Committee on Energy & Commerce
Subcommittee on Innovation, Data, and Commerce
U.S. House of Representatives
2322 Rayburn House Office Building
Washington, DC 20515

The Honorable Janice Schakowsky
Ranking Member
Committee on Energy & Commerce
Subcommittee on Innovation, Data, and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Tim Walberg
Vice Chair
Committee on Energy & Commerce
Subcommittee on Innovation, Data, and Commerce
U.S. House of Representatives
2322 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Bilirakis, Ranking Member Schakowsky, and Vice Chair Walberg:

On behalf of the undersigned organizations representing the United States' information and communications industry, we respectfully submit this Letter for the Record for today's Energy and Commerce Committee's Subcommittee on Innovation, Data, and Commerce hearing, "Economic Danger Zone: How America Competes to Win the Future Versus China." The Subcommittee's focus on enhancing America's technology leadership to counter competition from China is critical and commendable. In addition to the issues in focus for this hearing, such as the important need for additional licensed spectrum to enhance global competitiveness with China, a key element in securing America's leadership and independence from influence or interference from China remains outstanding – a fully funded Secure and Trusted Communications Networks Reimbursement Program (Program) at the Federal Communications Commission (FCC).

In 2020, Congress created the Program to fund the removal of Chinese equipment and services deemed to pose a national security risk from U.S. telecommunications networks and replacement with equipment and services from trusted vendors. The Program, however, is significantly underfunded, and recent bipartisan Congressional efforts to fully fund the Program have languished. This creates significant economic burdens on many smaller rural wireless carriers and allows a national security risk to continue unabated. Affected carriers have already begun the "rip and replace" process at the

direction of both Congress and the FCC, committing and expending significant resources in good faith reliance that the Program would be fully funded, and many are now stranded mid-effort. In July 2022, the FCC identified a funding shortfall of $3.08 billion to fully fund the Program's approved application cost estimates. The shortfall means that carriers could only be reimbursed for approximately 40% of their costs, which would preclude them from completing the removal and replacement process, placing their networks in jeopardy of failure and, in some cases, causing them to discontinue service in traditionally underserved areas of the country.

The success of this Congressionally mandated national security imperative depends on fully and immediately funding the Program. Carriers cannot complete the job without full funding. Failure to fully fund the Program means that untrusted equipment is still in service today, including some near military bases, airports, and other areas of strategic importance. Furthermore, because the FCC's timeline to complete this work began in July 2022, the window is closing on this high-priority and accelerated Program.

All carriers participating in the Program urgently want to complete the transition to secure and trusted networks. They have been largely prohibited from servicing or upgrading their networks for years, increasing chances for network degradation or even failure, and leaving their communities behind as technology evolves to 5G and beyond. While the United States has taken a leadership position internationally about the risks of untrusted communications networks, particularly those under Chinese influence, work remains to eliminate that risk in our own heartland.

The FCC cannot provide additional resources for this Program – only Congress can provide funding to resolve the shortfall. Every day that passes without addressing this national security threat is another day that American networks remain at risk. Congress must immediately prioritize this national security emergency and fully fund the Program.

Sincerely,

Competitive Carriers Association
CTIA
Information Technology Industry Council (ITI)
NATE: The Communications Infrastructure Contractors Association
NTCA – The Rural Broadband Association
Rural Wireless Association
Telecommunications Industry Association
Wireless Infrastructure Association
WTA — Advocates for Rural Broadband

cc:
The Honorable Cathy McMorris Rodgers, Chair, House Committee on Energy & Commerce
The Honorable Frank Pallone, Jr., Ranking Member, House Committee on Energy & Commerce

January 31, 2023

The Honorable Gus Bilirakis
Chair
Subcommittee Innovation, Data, and Commerce
House Committee, Energy and Commerce
2354 Rayburn House Office Building
Washington D.C. 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee Innovation, Data, and Commerce
House Committee, Energy and Commerce
2376 Rayburn House Office Building
Washington D.C. 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

As members of Congress consider measures that could bolster America's competitiveness globally and especially with countries like China, it is critical to advance policies that will strengthen supply chain resiliency, support domestic manufacturing, and lay the groundwork for optimizing supply chain performance for decades to come.

Pandemic disruptions, port congestion and challenges like last year's thankfully averted freight rail strike are no longer front-page news, but America's supply chains are as vulnerable now as they were before March 2020. Bipartisan legislation to strengthen supply chains and enhance U.S. economic competitiveness should be a priority for the Committee in 2023. More than 130 organizations strongly supported past legislative efforts as outlined in the attached letter ("Association Supply Chain Letter 5.10.22"), which is included as an appendix to this document. We believe that Congress should build on lessons learned to bolster economic and national security.

Specifically, we encourage Congress to support businesses working to develop, diversify, preserve, and improve critical supply chains and the manufacturing of critical goods. This is critical to ensuring the availability, affordability and accessibility of goods and services, especially amid current and future disruptions. We urge robust consideration of programs that would invest in domestic manufacturing and strengthen resilience in sectors essential to national security, economic growth and consumer health and wellbeing. We also believe that government must fill key knowledge and expertise gaps on supply chain issues, both through the development of new tools to map and monitor supply chains, as well as greater levels of senior inter-agency policy coordination to drive greater levels of supply chain performance.

Absent investment in and prioritization of supply chains, we are concerned that America will continue to cede geopolitical ground and that supply chain vulnerabilities will imperil national and economic security. Thank you for convening today's discussion on competitiveness, and we look forward to working with the Committee to strengthen supply chains and to advance bipartisan solutions.

Sincerely,

Consumer Brands Association
Information Technology Industry Council

May 10, 2022

The Honorable Nancy Pelosi
Speaker
U.S. House of Representatives
H-232, U.S. Capitol
Washington, DC 20515

The Honorable Chuck Schumer
Majority Leader
U.S. Senate
Room S-221, U.S. Capitol
Washington, DC 20510

The Honorable Kevin McCarthy
Republican Leader
U.S. House of Representatives
H-204, U.S. Capitol
Washington, DC 20515

The Honorable Mitch McConnell
Republican Leader
U.S. Senate
S-230, U.S. Capitol
Washington, DC 20510

Dear Speaker Pelosi and Leaders Schumer, McCarthy, and McConnell:

As members of Congress come together to advance bipartisan legislation strengthening supply chains and enhancing U.S. economic competitiveness, the undersigned organizations write to express our strong support for the Manufacturing Security and Resilience Program and other critical provisions included in the supply chain resilience subtitle of the House-passed America COMPETES Act (Sec. 20201 through 20211 of H.R. 4521).

The pandemic laid bare what many of us have known for years: American workers and consumers—and thus the American economy—depend on a robust supply chain bolstered by American manufacturers. The federal government needs dedicated funding to help manufacturers meet these challenges in times of crisis, as well as supply chain expertise and the ability to nimbly coordinate across agencies and policy silos to strengthen U.S. competitiveness, drive manufacturing growth, and ensure the continued availability, accessibility, and affordability of critical products.

The America COMPETES Act contains provisions that would establish a Manufacturing Security and Resilience Program ("Program") to support businesses working to develop, diversify, preserve, and improve critical supply chains and the manufacturing of critical goods. The Program would be administered within the Department of Commerce ("Department"), which would be responsible for leading a government-wide effort to invest in manufacturing and address supply chain risk. Through grants, loans, and loan guarantees, the Program would support the development of new technologies, growth in the U.S. manufacturing base, re-tooling of industrial equipment, and production of critical goods. We believe that such a Program will play an essential role in strengthening supply chains crucial for consumers and ensuring Americans' quality of life and economic prosperity for decades to come.

Additionally, we appreciate that the America COMPETES Act empowers the Department to conduct comprehensive supply chain mapping and monitoring, provide $45 billion of financial assistance to strengthen supply chains and manufacturing, and equip the private sector with the tools and best practices needed to address supply chain weaknesses before they become full blown crises. Critically, the subtitle outlines a clarified vision for the Department on its implementation of the Program, benefiting from the lessons learned from the supply chain disruptions experienced in the timeframe since Senate passage of the United States Innovation and Competition Act of 2021 ("USICA").

As you discuss the path forward for provisions subject to the conference process in both chambers, we encourage you to support enactment of this Program and the other critical measures in the supply chain resilience subtitle. Adopting these provisions of the House-passed COMPETES Act as part of bipartisan legislation to support American competitiveness will empower unprecedented

expertise at the Department and the ability to invest in sectors critical to the health, economic well-being, and security of our country.

Sincerely,

AICC, The Independent Packaging Association
Air-Conditioning, Heating & Refrigeration Institute
American Automotive Policy Council
American Chemistry Council
American Cleaning Institute
American Coatings Association
American Composites Manufacturers Association
American Feed Industry Association
American Foundry Society
American Frozen Foods Institute
American Mold Builders Association
American Wood Council
Ames Chamber of Commerce
Associated Equipment Distributors
Associated Industries of Florida
Associated Industries of Massachusetts
Associated Industries of Missouri
Associated Industries of Vermont
Association of Equipment Manufacturers
Association of Home Appliance Manufacturers
Auto Care Association
Barrow County Chamber of Commerce
Battery Materials & Technology Coalition
Beer Institute
Berkeley Chamber of Commerce
Brick Industry Association
Buffalo Niagara Manufacturers Alliance
Business and Industry Association of New Hampshire
California Manufacturers & Technology Association
Can Manufacturers Institute
Cedar Rapids Metro Economic Alliance
Central Fairfax Chamber of Commerce
Charleston Metro Chamber of Commerce
Chillicothe Ross Chamber of Commerce
Cobb Chamber of Commerce
Colorado Advanced Manufacturing Association
Composite Can and Tube Institute
Consumer Brands Association
Consumer Healthcare Products Association
Corn Refiners Association
Council Bluffs Area Chamber of Commerce
Dental Trade Alliance
Effingham County Chamber of Commerce
Electronic Components Industry Association
Employ America Action Fund
Flexible Packaging Association
Forging Industry Association
Glass Packaging Institute

Global Cold Chain Alliance
Greater Des Moines Partnership
Greater Mount Airy Chamber of Commerce
Gwinnett Chamber of Commerce
Hampton Roads Chamber of Commerce
Illinois Manufacturers' Association
INDA, The Association of the Nonwoven Fabrics Industry
Independent Lubricant Manufacturers Association
Industrial Fasteners Institute
Industrial Packaging Alliance of North America
Industrial Truck Association
Information Technology Industry Council
International Bottled Water Association
International Food Additives Council
Iowa Association of Business and Industry
Iowa Business Council
IPC - Build Electronics Better
Juniata River Valley Chamber of Commerce
Kansas Chamber and the Kansas Manufacturing Council
Lansing Regional Chamber of Commerce
Maine State Chamber of Commerce
Manufacturing Alliance of Philadelphia
Metal Powder Industries Federation
Midwest Manufacturers Association
Minnesota Chamber of Commerce
Mississippi Manufacturers Association
Montana Chamber of Commerce
Motor & Equipment Manufacturers Association
Murray County Chamber of Commerce
National Association of Manufacturers
National Association of Trailer Manufacturers
National Automatic Merchandising Association
National Confectioners Association
National Electrical Manufacturers Association
National Foreign Trade Council
National Glass Association
National Marine Manufacturers Association
National Seasoning Manufacturers Association, Inc.
National Tooling and Machining Association
National Waste & Recycling Association
Nebraska Chamber of Commerce & Industry
Non-Ferrous Founders' Society
North American Association of Food Equipment Manufacturers
North American Die Casting Association
North Carolina Chamber
Northeast Pennsylvania Manufacturers & Employers Association
Norwin Chamber of Commerce
Outdoor Power Equipment Institute, Inc.
Pennsylvania Manufacturers' Association
Pet Advocacy Network
Plastics Pipe Institute
Plumbing Manufacturers International
Power Tool Institute

Precision Machined Products Association
Precision Metalforming Association
PRINTING United Alliance
Railway Supply Institute
Reshoring Initiative
Rhode Island Manufacturers Association
Roanoke Regional Chamber of Commerce
Rowan Chamber of Commerce
Salem-Roanoke County Chamber of Commerce
San Antonio Manufacturers Association
Schuylkill Chamber of Commerce
SNAC International
Society of Chemical Manufacturers & Affiliates
Society of Glass & Ceramic Decorators Products
Software & Information Industry Association
Somerset County Chamber of Commerce
South Carolina Chamber of Commerce
Specialty Tools & Fasteners Distributors Association
St. Paul Area Chamber
SynBio Coalition
Texas Association of Manufacturers
Texas International Produce Association
The Aluminum Association
The Association For Manufacturing Technology
The Carpet and Rug Institute
The Hardwood Federation
The Ohio Manufacturers' Association
The Toy Association
Utah Manufacturers Association
Valve Manufacturers Association
Virginia Chamber of Commerce
Window & Door Manufacturers Association
York County Economic Alliance

cc: The Honorable Frank Pallone, Jr.
Chair, U.S. House Committee on Energy and Commerce

The Honorable Maria Cantwell
Chair, U.S. Senate Committee on Commerce, Science, and Transportation

The Honorable Cathy McMorris Rodgers
Ranking Member, U.S. House Committee on Energy and Commerce

The Honorable Roger Wicker
Ranking Member, U.S. Senate Committee on Commerce, Science, and Transportation

ADVOCATES FOR HIGHWAY & AUTO SAFETY

January 31, 2023

The Honorable Gus M. Bilirakis, Chair
The Honorable Jan Schakowsky, Ranking Member
Committee on Energy and Commerce
Innovation, Data, and Commerce Subcommittee
United States House of Representatives
Washington, D.C. 20510

Dear Chairman Bilirakis and Ranking Member Schakowsky:

As you prepare for tomorrow's hearing, "Economic Danger Zone: How America Competes to Win the Future Versus China," Advocates for Highway and Auto Safety (Advocates) would like to address the issue of new and emerging vehicle technologies and autonomous vehicles (AVs).

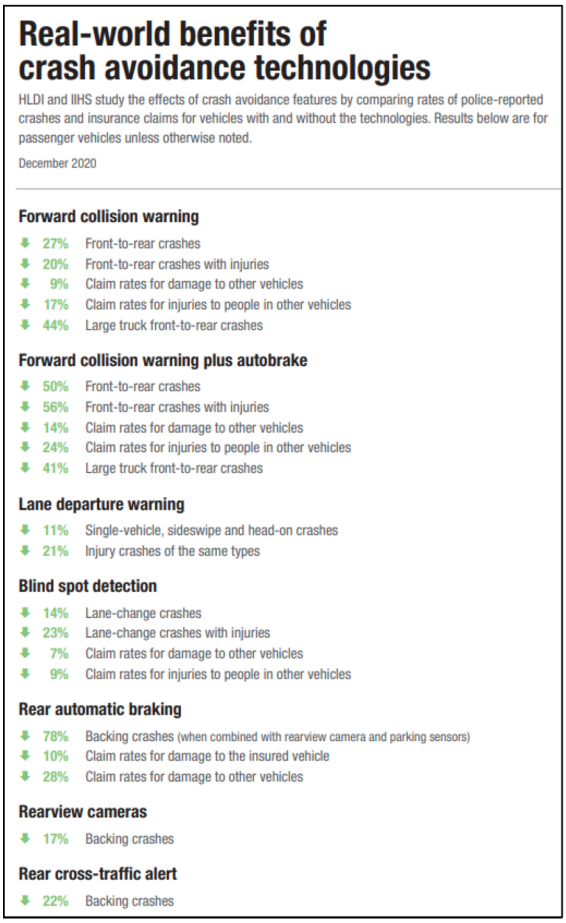
Advocates is an alliance of consumer, medical, public health, law enforcement, and safety groups and insurance companies and agents working together to improve road safety in the United States (U.S.). Advocates' mission is the adoption of federal and state laws, policies and programs that prevent motor vehicle crashes, save lives, reduce injuries, and contain costs. We respectfully request this letter be included in the hearing record.

The "Danger Zone" on Our Nation's Roads: Death and Injury Toll is Skyrocketing While Requirements for Proven Safety Technology Stagnate

According to the National Highway Traffic Safety Administration (NHTSA), 38,824 people were killed and an estimated 2.28 million more were injured in traffic crashes in 2020.[1] In 2021, the NHTSA estimates that 42,915 people were killed in traffic crashes and that these numbers remained relatively static in the first nine months of 2022.[2] The NHTSA currently values each life lost in a crash at $11.8 million.[3] In 2019, crashes, injuries, and fatalities imposed a financial burden of nearly $1.4 trillion in total costs to society -- $340 billion of which are direct economic costs, equivalent to a "crash tax" of $1,035 on every American.[4] In 2018, crashes alone cost employers $72.2 billion.[5]

While some have touted AVs as a panacea to address this significant and costly public health emergency, requiring proven and available safety technologies with minimum performance standards would address the issue now. The NHTSA has estimated that between 1960 and 2012, over 600,000 lives have been saved by motor vehicle safety technologies.[6] Advocates always has enthusiastically championed this approach. In 1991, Advocates led the coalition that supported enactment of the bipartisan Intermodal Surface Transportation Efficiency Act (ISTEA) of 1991[7] which included a mandate for front seat airbags as standard equipment. As a result, by 1997, every new car sold in the United States was equipped with this technology and the lives saved have been significant. Airbags have saved an estimated 50,457 lives from 1987 to 2017, according to NHTSA.[8] Advocates continued to support proven lifesaving technologies as

standard equipment in all vehicles in other federal legislation and regulatory proposals. These efforts include: tire pressure monitoring systems;[9] rear outboard 3-point safety belts;[10] electronic stability control;[11] rear safety belt reminder systems;[12] brake transmission interlocks;[13] safety belts on motorcoaches;[14] electronic logging devices for commercial motor vehicles (CMVs);[15] and, rear-view cameras.[16]



Real-world benefits of crash avoidance technologies

HLDI and IIHS study the effects of crash avoidance features by comparing rates of police-reported crashes and insurance claims for vehicles with and without the technologies. Results below are for passenger vehicles unless otherwise noted.

December 2020

Forward collision warning

- ↓ 27% Front-to-rear crashes
- ↓ 20% Front-to-rear crashes with injuries
- ↓ 9% Claim rates for damage to other vehicles
- ↓ 17% Claim rates for injuries to people in other vehicles
- ↓ 44% Large truck front-to-rear crashes

Forward collision warning plus autobrake

- ↓ 50% Front-to-rear crashes
- ↓ 56% Front-to-rear crashes with injuries
- ↓ 14% Claim rates for damage to other vehicles
- ↓ 24% Claim rates for injuries to people in other vehicles
- ↓ 41% Large truck front-to-rear crashes

Lane departure warning

- ↓ 11% Single-vehicle, sideswipe and head-on crashes
- ↓ 21% Injury crashes of the same types

Blind spot detection

- ↓ 14% Lane-change crashes
- ↓ 23% Lane-change crashes with injuries
- ↓ 7% Claim rates for damage to other vehicles
- ↓ 9% Claim rates for injuries to people in other vehicles

Rear automatic braking

- ↓ 78% Backing crashes (when combined with rearview camera and parking sensors)
- ↓ 10% Claim rates for damage to the insured vehicle
- ↓ 28% Claim rates for damage to other vehicles

Rearview cameras

- ↓ 17% Backing crashes

Rear cross-traffic alert

- ↓ 22% Backing crashes

Advanced Driver Assistance Systems (ADAS)

According to the Insurance Institute for Highway Safety (IIHS), advanced driver assistance systems (ADAS) can prevent or mitigate crashes and protect occupants and road users. The National Transportation Safety Board (NTSB) has included increasing implementation of collision avoidance technologies in its Most Wanted Lists of Transportation Safety Improvements since 2016.[17]

However, lifesaving capabilities of ADAS are limited because they are not required as standard equipment in new vehicles. Rather, their sale as part of an additional, expensive trim package along with other non-safety features, or including them as standard equipment in high end models or vehicles reduces mass dissemination and inequitably provides access only to those who can afford an upcharge of thousands of dollars. Moreover, there are currently no minimum performance standards to ensure the technologies execute as expected and needed. Research performed by IIHS indicates that AEB with pedestrian detection can reduce pedestrian crash risk by as much as 33 percent.[18] However, over a third of pedestrian deaths occur in dark/unlighted conditions, and research also indicates that today's pedestrian AEB systems do not reduce pedestrian crash risk in the dark without street lighting.[19] Further, testing performed by IIHS and NHTSA indicates that pedestrian AEB systems have the ability to properly perform in the dark now.[20] Therefore, requiring that these systems function in all light conditions will lead to a greater reduction in the grim statistics noted above. Considering the

historic increases in fatalities involving vulnerable road users (VRUs) including pedestrians, bicyclists, people who use wheelchairs and other assistive devices, roadside first responders and others, it is imperative that this technology detects and responds to all people in the roadway. Pedestrian fatalities have increase by 79 percent since the historic low in 2009. Pedalcyclist fatalities have increased by 58 percent since the historic low in 2010.[21] When consumers walk into auto showrooms to purchase a vehicle, which is often one of the most considerable expenditures for families, they expect the assurances of minimum safety standards to protect them, as has been the case since the first regulation in 1966.[22]

Since enactment of the Infrastructure Investment and Jobs Act (IIJA, Pub. L.117-58), Advocates has been urging the U.S. Department of Transportation (DOT) to meet and exceed its directives for ADAS. The current void of regulations for ADAS renders all road users, including VRUs, at risk to dangers. Furthermore, these technologies are some of the essential building blocks for the potential of AVs in the future.

Connected Vehicles

Connected vehicle technologies allow a vehicle to send and receive communications with other vehicles (vehicle-to-vehicle (V2V)), the infrastructure (vehicle-to-infrastructure (V2I), and "everything" (vehicle-to-everything (V2X)). These messages can relay information ranging from the relative location and direction of motion of other vehicles (and the potential for all road users) to warning messages that traffic lights are about to change, or inclement weather conditions are soon to be encountered. Further, digital alert technologies could allow emergency and first response vehicles to communicate their location in an effort to prevent collisions with personnel and vehicles on the roadside. The NHTSA estimated that two potential applications of V2V alone could yield a 50 percent reduction in crashes, injuries and fatalities, on average. NHTSA notes, "this could potentially prevent 400,000 to 600,000 crashes, 190,000 to 270,000 injuries, and save 780 to 1,080 lives each year."[23] This Subcommittee should direct NHTSA to update and complete the 2017 Notice of Proposed Rulemaking (NPRM) to require vehicle-to-vehicle (V2V) technology. Congress should also direct NHTSA to partner with the Federal Highway Administration (FHWA) to study the needs and benefits of vehicle-to-infrastructure (V2I) with the goal of mandating vehicle-to-everything (V2X) communications for safety.

On the path to AVs, requiring minimum performance standards for these foundational technologies will ensure the safety of all road users while also building consumer confidence in the capabilities of these newer crash avoidance technologies.

Autonomous Vehicles: The Need to Avoid "What's Past is Prologue"

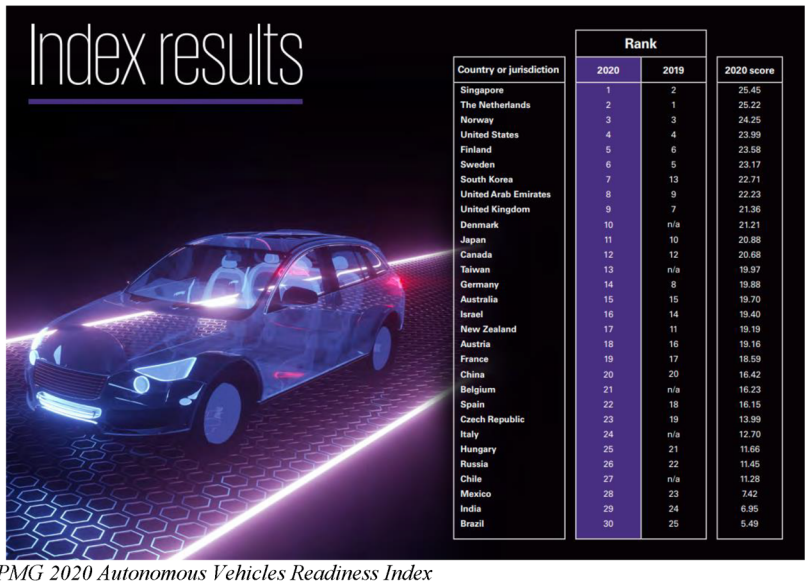
Data obtained through the Standing General Order (SGO) from July 2021 to December 2022 have revealed 227 crashes involving Automated Driving Systems (ADS) and 731 with ADAS (including 18 resulting in a fatality).[24] These disturbing statistics demonstrate that is imperative that NHTSA continue to collect and refine this data and provide it to Congress and the public, and that sensible federal safety standards be developed to prevent crashes and save lives.

Development and Deployment in the U.S. Compared to Other Countries

Other countries are taking a more calculated, careful and cautious approach to AVs.[25] Despite often-repeated claims about "falling behind" other countries in the "race" for AVs, the U.S. remains a leader in the field. For example:

- China continues to require permits or restricts operations of AVs on its roads to only those areas approved by the authorities.[26]

- Germany continues to require permits, approvals, and limits areas of operation for AVs.[27]
- In Japan, the introduction of Level 4 vehicles will be controlled and limited to specific, lightly populated areas.[28]
- Even the latest United Nations Economic Commission for Europe (UNECE) regulations will limit operations to restrict risks and oversee approval through testing and other requirements.[29]



Country or jurisdiction	Rank 2020	Rank 2019	2020 score
Singapore	1	2	25.45
The Netherlands	2	1	25.22
Norway	3	3	24.25
United States	4	4	23.99
Finland	5	6	23.58
Sweden	6	5	23.17
South Korea	7	13	22.71
United Arab Emirates	8	9	22.23
United Kingdom	9	7	21.36
Denmark	10	n/a	21.21
Japan	11	10	20.88
Canada	12	12	20.68
Taiwan	13	n/a	19.97
Germany	14	8	19.88
Australia	15	15	19.70
Israel	16	14	19.40
New Zealand	17	11	19.19
Austria	18	16	19.16
France	19	17	18.59
China	20	20	16.42
Belgium	21	n/a	16.23
Spain	22	18	16.15
Czech Republic	23	19	13.99
Italy	24	n/a	12.70
Hungary	25	21	11.66
Russia	26	22	11.45
Chile	27	n/a	11.28
Mexico	28	23	7.42
India	29	24	6.95
Brazil	30	25	5.49

KPMG 2020 Autonomous Vehicles Readiness Index

In sum, no country is selling fully automated vehicles for unfettered use to the public and by many accounts, none will be for a significant amount of time.[30] According to the most recent KPMG analysis, the U.S. ranks fourth in the world for AV readiness, while China is at number twenty. While the U.S. is not behind other countries in allowing AVs to go to market, we are behind in establishing comprehensive safeguards to ensure that this progress happens without jeopardizing or diminishing public safety.

Advocates and numerous stakeholders developed the "AV Tenets," policy positions which should be a foundational part of any AV policy.[31] It has four main, commonsense categories including: 1) prioritizing safety of all road users; 2) guaranteeing accessibility and equity; 3) preserving consumer and worker rights; and, 4) ensuring local control and sustainable transportation. Many promises have been made about AVs bringing reductions in motor vehicle crashes and resultant deaths and injuries, lowering traffic congestion and vehicle emissions, expanding mobility and accessibility, improving efficiency, and creating more equitable transportation options and opportunities. The commonsense safeguards in the AV Tenets will help accomplish these goals. The AV Tenets are supported by a coalition of more than 60 groups and are based on expert analysis, real-world experience and public opinion. Requiring that AVs meet minimum standards, including for cyber security, and that operations are subject to adequate oversight, including a comprehensive database accessible by vehicle identification

number (VIN) with basic safety information, will save lives and boost consumer confidence in this burgeoning technology.

Moreover, no demonstrable evidence has been presented to show that the development of AVs requires larger volumes of exemptions from federal safety standards which are essential to public safety. Current law already permits manufacturers to test an unlimited number of vehicles on public roads and to apply for an unlimited number of exemptions. For each exemption granted, manufacturers can sell up to 2,500 exempt vehicles. In fact, since the first AV bill was introduced in 2017, AV development has not come to a grinding halt. For example, in March 2022 Waymo announced it was offering autonomous rides in its taxi in San Francisco expanding its previous testing zone that was limited to Arizona.[32] In addition, it has recently been reported that Microsoft is investing millions of dollars in an autonomous trucking company.[33] Allowing huge numbers vehicles on the road (potentially millions) exempt from current safety standards and in the absence of new standards for the ADS and related issues, de facto turn everyone -- in and around these vehicles -- into unknowing and unwilling human subjects in a risky experiment. A massive influx of new vehicles exempt from FMVSS will have serious, costly and potentially deadly ramifications, both those that can be predicted or some that cause unintended consequences.

Lastly, we commend Congress for the safety advances included in the bipartisan IIJA and have been urging the U.S. DOT to implement the directives with urgency to address the motor vehicle crash fatality and injury toll. With 115 people being killed on our roadways every day, time is certainly of the essence.

Thank you for your consideration of these critically important safety issues. As always, we are ready and willing to be of assistance to you in furtherance of improving safety for all road users.

Sincerely,

Catherine Chase, President

cc: Members of the Subcommittee on Innovation, Data, and Commerce

---

[1] Traffic Safety Facts 2020, A Compilation of Motor Vehicle Crash Data, DOT HS 813 375, NHTSA (Oct. 2022).
[2] Early Estimates of Motor Vehicle Traffic Fatalities And Fatality Rate by Sub-Categories in 2021, NHTSA, May 2022, DOT HS 813 298; and Early Estimates of motor Vehicle Traffic Fatalities and Fatality Rate by Sub-Categories Through June 2022, NHTSA, Dec. 2022, DOT HS 813 405
[3] Departmental Guidance on Valuation of a Statistical Life in Economic Analysis, NHTSA, available at https://www.transportation.gov/office-policy/transportation-policy/revised-departmental-guidance-on-valuation-of-a-statistical-life-in-economic-analysis, last accessed Jan. 31, 2023.
[4] The Economic and Societal Impact of Motor Vehicle Crashes, 2019, NHTSA, Dec. 2022, DOT HS 813 403.
[5] Cost of Motor Vehicle Crashes to Employers 2019, Network of Employers for Traffic Safety, March 2021.
[6] Lives Saved by Vehicle Safety Technologies and Associated Federal Motor Vehicle Safety Standards, 1960 to 2012, DOT HS 812 069 (NHTSA, 2015); See also, NHTSA AV Policy, Executive Summary, p. 5 endnote 1.
[7] Pub. L. 102-240 (Dec. 18, 1991). Statistics are from the U.S. Department of Transportation unless otherwise noted.
[8] Traffic Safety Facts 2020, A Compilation of Motor Vehicle Crash Data, DOT HS 813 375, NHTSA (Oct. 2022).

[9] Transportation Recall Enhancement, Accountability, and Documentation (TREAD) Act, Pub. L. 106-414 (Nov. 1, 2000).
[10] Anton's Law, Pub. L. 107-318 (Dec. 4, 2002).
[11] Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU), Pub. L. 109-59 (Aug. 10, 2005).
[12] SAFETEA-LU), Pub. L. 109-59 (Aug. 10, 2005)
[13] SAFETEA-LU), Pub. L. 109-59 (Aug. 10, 2005)
[14] Moving Ahead for Progress in the 21st Century (MAP-21) Act, Pub. L. 112-141 (Jan. 3, 2012).
[15] (MAP-21) Act, Pub. L. 112-141 (Jan. 3, 2012).
[16] Cameron Gulbransen Kids Transportation Safety Act of 2007, Pub. L. 110-189 (Feb. 28, 2008).
[17] NTSB Most Wanted List Archives, https://ntsb.gov/safety/mwl/Pages/mwl_archive.aspx
[18] IIHS, Petition for Rulemaking (Mar. 22, 2022); available at: https://www.iihs.org/media/4619ab07-fc36-4a62-8a92-da401206e03b/4ZqPbA/Petitions/petition_2022-03-22.pdf
[19] IIHS, Petition for Rulemaking (Mar. 22, 2022)
[20] IIHS, Petition for Rulemaking (Mar. 22, 2022)
[21] Traffic Safety Facts 2020, A Compilation of Motor Vehicle Crash Data, DOT HS 813 375, NHTSA (Oct. 2022); and Early Estimates of Motor Vehicle Traffic Fatalities And Fatality Rate by Sub-Categories in 2021, NHTSA, May 2022, DOT HS 813 298
[22] National Traffic and Motor Vehicle Safety Act of 1966, Pub. L. 89-563 (Sep. 1966).
[23] NHTSA, *Fact Sheet: Improving Safety and Mobility Through Vehicle-to-Vehicle Communication Technology,* available here: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/v2v_fact_sheet_101414_v2a.pdf.
[24] Standing General Order on Crash Reporting: For incidents involving ADS and Level 2 ADAS; NHTSA, available at https://www.nhtsa.gov/laws-regulations/standing-general-order-crash-reporting, last accessed Jan. 31, 2023
[25] Autonomous vehicles: cross jurisdictional regulatory perspectives update, Oct. 7, 2022,
[26] China drafts rules on use of self-driving vehicles for public transport; Aug. 8, 2022, Reuters; and Baidue bags China's first fully driverless robotaxi licenses, Aug. 7, Reuters. Real driverless cars are now legal in Shenzhen, China's tech hub, Jul. 25, 2022, TechCrunch+.
[27] Germany completes legal framework for autonomous driving | Federal Cabinet approves new ordinance, Apr. 2022, Malterer, M.
[28] Japan to open roads to autonomous vehicles in 2023, Nov. 28, 2022, Wessling, B., The RobotReport.
[29] New rules to improve road safety and enable fully driverless vehicles in the EU, Jul. 6, 2022, UNECE.
[30] Lawrence Ulrich, Driverless Still a Long Way From Humanless, N.Y. Times (Jun. 20, 2019); Level 5 possible but "way in the future", says VW-Ford AV boss, Motoring (Jun. 29, 2019).
[31] The AV Tenets are attached as Appendix B.
[32] Alan Ohnsman, Waymo Starts Fully Autonomous Rides In San Francisco, Expanding Arizona Robotaxi Zone, Forbes (Mar. 30, 2022).
[33] Krystal Hu and Joseph White, Microsoft to invest in autonomous trucking startup Gatik -sources, Reuters (Jan. 4, 2023).

NATIONAL ASSOCIATION OF Manufacturers

Aric Newhouse

Senior Vice President,
Policy and Government Relations

February 1, 2023

The Honorable Gus Bilirakis
Chairman
Committee on Energy and Commerce
Subcommittee on Innovation,
Data and Commerce
U.S. House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Committee on Energy and Commerce
Subcommittee on Innovation,
Data and Commerce
U.S. House of Representatives
Washington, DC 20515

Dear Chairman Bilirakis and Ranking Member Schakowsky:

Thank you for holding today's hearing, *Economic Danger Zone: How America Competes To Win The Future Versus China*, and for your focus on maintaining America's global leadership in innovation. The National Association of Manufacturers is the largest manufacturing association in the United States, representing small and large manufacturers in every industrial sector and in all 50 states. Manufacturing employs nearly 13 million Americans, contributes $2.81 trillion to the U.S. economy annually, pays workers over 18% more than the average for all businesses and has one of the largest sectoral multipliers in the economy. Taken alone, manufacturing in the United States would be the eighth-largest economy in the world.

Manufacturers perform more research than any other industry, accounting for 55.2% of private-sector R&D, investing $347.4 billion in 2021. As a result of this research, manufacturers create new technologies, cutting-edge materials, life-saving treatments and vaccines and develop more sustainable processes that improve the lives of every American.

Enhancing the manufacturing industry's ability to compete – particularly against state-funded entities that are focused on displacing the United States from its position as the world's largest and most innovative economy – is vital to our national interest. The National Association of Manufacturers has produced a blueprint of the most critical actions policymakers can take to support the industry: *Competing to Win*, which is attached to this submission.[1]

The challenges faced by manufacturers are complex, varied and will require a concerted effort that is strategic and intentional to advance our interests. The range of actions the NAM recommends that Congress take are designed to achieve critical economic and strategic goals. The NAM respectfully encourages you to consider the following items, among others in *Competing to Win*, in order to immediately support manufacturers' competitiveness.

Reform the federal permitting system

Too often, manufacturers seeking to make significant investments in the United States face years-long delays in obtaining the permits needed to break ground on a project. Speeding the permitting process and establishing permit certainty will support industrial growth. Efforts to

[1] National Association of Manufacturers, *Competing to Win* (Sept. 2022) *available at* https://documents.nam.org/COMM/Competing_to_Win_2022.pdf.

expand domestic energy production, upgrade our nation's infrastructure, increase critical mineral extraction and processing and expand facilities are all dependent upon the success of advancing permitting reform. To that end, ensuring the Administration is following congressional intent regarding One Federal Decision from the bipartisan Infrastructure Investment and Jobs Act is key, as that mandate establishes strict permit review timelines and eliminates duplicitous efforts across various federal agencies. Moreover, key permitting authorities are rife with ambiguity and inconsistent terminology, and need Congressional intervention in order to facilitate manufacturing expansion while achieving environmental stewardship.

Grow the manufacturing workforce

Manufacturers are facing a workforce crisis. Over the next decade, 4 million manufacturing jobs will likely be needed, and 2.1 million are expected to go unfilled because we there are not enough potential workers with the skills needed in today's modern manufacturing sector. The effects of this shortfall will be felt throughout the country. According to a recent report by the NAM's workforce and education partner, the Manufacturing Institute, and Deloitte the U.S. economy will be $1 trillion smaller in 2030 if those positions are not filled.[2]

In order to fully address this challenge, the perception of manufacturing careers must be changed and there must be an effort to broaden recruitment pipelines to engage under-represented populations and – with only 58 people actively looking for work for every 100 job openings – the potential workforce must grow. Reforming our nation's broken immigration system is a critical step to address some workforce needs. Manufacturers support securing our borders and reforming the immigration system to reflect the needs of the modern workforce, including addressing the existing backlog of immigration cases, providing certainty for individuals who are already in this country and updating our nation's approach to asylum seekers and refugees.

Support investment in America

Manufacturing is a capital-intensive industry. Facilities, equipment and machinery have long productive lives but require significant up-front capital investments. Reducing barriers to these investments will help grow the manufacturing base. In this regard, manufacturers urge lawmakers to take two actions.

First, funds that have been authorized to support the manufacturing economy should be disbursed quickly and equitably. Portions of the CHIPS and Science Act, the Infrastructure Investment and Jobs Act and the Inflation Reduction Act authorize investments in key parts of the manufacturing economy. Congress should work with the Administration to ensure that these funds reach manufacturers expeditiously. Second, lawmakers must ensure that the tax code supports private investment in manufacturing activities. Specifically, making the 2017 Tax Cuts and Jobs Act permanent would support small businesses, and reversing harmful changes to the tax treatment of research expenses, business loans and equipment purchases would benefit all manufacturers in America.

---

[2] The Manufacturing Institute and Deloitte, *Creating Pathways for Tomorrow's Workforce Today: Beyond Reskilling in Manufacturing* (2022) *available at* https://www.themanufacturinginstitute.org/wp-content/uploads/2021/05/DI_ER-I-Beyond-reskilling-in-manufacturing-1.pdf.

Protect Manufacturers' IP and Combat Counterfeits

It is vital that the United States advance policies that defend American innovation and technology leadership in the U.S. and abroad, including through efforts to advance strong rules and robust protection of IP and innovation. Notably, manufacturers appreciate the work of members of this subcommittee on policies that will work towards stopping the flow of counterfeit goods into the United States. Counterfeit goods, particularly those sold online, remain a top concern and competitive advantage for manufacturers of all sizes. The enactment of the INFORM Consumers Act in December 2022 was a significant step in combatting the scourge of counterfeit goods. The NAM respectfully urges the subcommittee to monitor and ensure the full implementation of this act by all parties and continue its focus on the issue in this Congress through both legislative and oversight activities.

****

Thank you again for your focus on enhancing manufacturers' ability to compete. The NAM looks forward to working with members of the subcommittee on this important issue.

Respectfully,

Aric Newhouse
Senior Vice President,
Policy and Government Relations
National Association of Manufacturers

TECH

Intel's horrible quarter revealed an inventory glut and underused factories

PUBLISHED THU, JAN 26 20236:58 PM EST | UPDATED THU, JAN 26 2023 8:13 PM EST

Kif Leswing
@KIFLESWING

KEY POINTS

- **Intel's December earnings showed significant declines in the company's sales, profit, gross margin, and outlook, both for the quarter and the full year.**
- **In short: Intel had a difficult 2022, and 2023 is shaping up to be tough as well.**

Intel CEO Pat Gelsinger, with U.S. President Joe Biden (not pictured), announces the tech firm's plan to build a $20 billion plant in Ohio, from the South Court Auditorium on the White House campus in Washington, January 21, 2022.
Jonathan Ernst | Reuters

Intel's December earnings showed significant declines in the company's sales, profit, gross margin, and outlook, both for the quarter and the full year.

Investors hated it, sending the stock over 9% lower in extended trading, despite the fact that Intel did not cut its dividend.

The earnings report, which was the eighth under CEO Pat Gelsinger's leadership, shows a legendary technology company struggling with many factors outside of its control, including a deeply slumping PC market. It also highlights some of Intel's current issues with weak demand for its current products and inefficient internal performance, and underscores how precarious the company's financial health has become.

"Clearly, the financials aren't what we would hoped," Gelsinger told analysts.

In short: Intel had a difficult 2022, and 2023 is shaping up to be tough as well.

Here are some of the most concerning bits from Intel's earnings report and analyst call:

Weak and uncertain guidance

Intel didn't give full-year guidance for 2023, citing economic uncertainty.

But the data points for the current quarter suggest tough times. Intel guided for about $11 billion in sales in the March quarter, which would be a 40% year-over-year decline. Gross margin will be 34.1%, a huge decrease from the 55.2% in the same quarter in 2021, Gelsinger's first at the helm.

But the biggest issue for investors is that Intel guided to a 15 cent non-GAAP loss per share, a big decline for a company that a year ago was reporting $1.13 in profit per share. It would be the first loss per share since last summer, which was the first loss for the company in decades.

An inventory glut

Management gave several reasons for the tough upcoming quarter, but one theme that came through was that its customers simply have too many chips and need to work through inventory, so they won't be buying many new chips.

Both the PC and server markets have slowed after a two-year boom spurred by remote work and school during the pandemic. Now, PC sales have slowed and the computer makers have too many chips. Gelsinger is predicting PC sales during the year to be around 270 million to 295 million — a far cry from the "million units-a-day" he predicted in 2021.

Now, Intel's customers have to "digest" the chips they already have, or "correct" their inventories, and the company doesn't know when this dynamic will shift back.

"While we know this dynamic will reverse, predicting when is difficult," Gelsinger told analysts.

Dropoff in gross margin

Underpinning all of this is that Intel's gross margin continues to decline, hurting the company's profitability. One issue is "factory load," or how efficiently factories run around the clock. Intel said that its gross margin would be hit by 400 basis points, or 4 percentage points, because of factories running under load because of soft demand.

Ultimately, Intel forecasts a 34.1% gross margin in the current quarter — a far cry from the 51% to 53% goal the company set at last year's investor day. The company says it's working on it, and the margin could get back to Intel's goal "in the medium-term" if demand recovers.

"We have a number of initiatives under way to improve gross margins and we're well under way. When you look at the $3 billion reduction [in costs] that we talked about for 2023, 1 billion of that is in cost of sales and we're well on our way to getting that billion dollars," Gelsinger said.

The not-so-bad news: Dividend and self-driving

Long-term investors have always closely watched how the company balances the near-term need to placate shareholders with the massive capital spending needed to stay competitive in the semiconductor manufacturing business.

If Intel is cutting costs and still needing to invest in chip factories to power its turnaround, analysts say it may want to reconsider its dividend. Intel spent $6 billion on dividends in 2022, but did not cut its dividend on Thursday.

Meanwhile, the company said it wants to cut $3 billion in costs for 2023 and analysts believe it wants to spend around $20 billion in capital expenditures to build out its factories.

Gelsinger was asked about this dynamic on Thursday.

"I'd just say the board, management, we take a very disciplined approach to the capital allocation strategy and we're going to remain committed to being very prudent around how we allocate capital for the owners and we are committed to maintaining a competitive dividend," Gelsinger replied.

There was at least one bright spot for Intel on Thursday.

Mobileye, its self-driving subsidiary that went public during the December quarter, reported earlier in the day, showing adjusted earnings per share of 27 cents and revenue growth of 59%, to $656 million. It also forecast strong 2023 revenue of between $2.19 billion and $2.28 billion. Shares rose nearly 6% during regular trading hours Thursday.

Jeff Farrah QFR Responses – Innovation, Data, and Commerce Subcommittee Hearing

Chair Bilirakis: I understand prior to your role with AVIA you worked at the National Venture Capital Association. I assume this expertise had a lot to do with you being asked to lead this organization.

Can you offer a broad perspective on how venture capital moves when there is an attractive market with clear regulatory frameworks? Can you provide some examples to where you have seen the US lose market leadership?

Response: Innovative companies need capital to grow and develop new products and services. In many cases, investors focused on forward leaning companies will cease to invest in a sector due to uncertainty over government policy. For example, venture capital investment into medical device companies has been significantly reduced in recent years due to uncertainty over reimbursement rules for these companies. As a result, the United States no longer has the necessary pipeline of inventive medical device companies. This lesson illustrates why the U.S. government establishing a federal policy framework for autonomous vehicles is critical. By clarifying rules of the road and demonstrating strong support for AVs, policymakers can encourage capital investment in this space that is essential to a thriving American AV ecosystem. Only then will the United States be able to maintain its global leadership role with respect to autonomous vehicles.

Rep. Buschon: To date, AV testing and deployment in the US has largely been confined to urban and suburban areas. But much of our country, including the district I represent, is rural. I think these communities would immensely benefit from AV deployment in their areas, as rural roads have some of the worst crash incidence rates in the nation. What are some things Congress can do to encourage testing and deployment of non-trucking and passenger AV s in rural areas?

Response: I share your concern with the alarming trend of crash fatality rates on rural roads. AVs are positioned to combat the crisis of roadway injuries and fatalities by eliminating the unsafe driving that is the cause of most of these incidents. As I stated at the hearing, AVs do not speed, they do not drive drunk, and they do not get distracted. The continued deployment of AVs will benefit rural communities by making roads safer and bringing more transportation options, like shuttle services, to these communities. However, regulatory uncertainty for AV developers is a significant hurdle for moving beyond deployment in high population density areas. A federal framework for AV deployment could help expand the geographical reach of the benefits of AV technology by spurring additional investment and allowing companies to plan long term. Although autonomous passenger vehicles are not currently deployed at scale in rural areas, autonomous trucks are currently running freight in a variety of locations in rural America. Autonomous trucks will help farmers, ranchers, and manufacturers get their products to market in an effective and efficient manner. Autonomous trucking can will have tremendous benefits for rural communities, such as reducing food spoilage by running more efficient routes without hours limitations.

Rep. Dunn:

1. A July 2019 Inspector General's report found that the Department of Defense continues to buy tens of millions of dollars in Commercial off the Shelf (COTS) technologies with known cybersecurity risks such as Lenovo computers, Lexmark printers, and GoPro cameras. What is the U.S. government doing to close loopholes that Lenovo and other IT firms in which the Chinese government has an ownership stake can exploit to sell its equipment to the U.S. military and other federal government departments and agencies?

Response: I share your concern with U.S. government cybersecurity vulnerabilities. However, this is not an area where I have expertise and therefore am unable to provide answers to these questions. I would be happy to schedule a follow up discussion to address any concerns that you may have.

2. Although the State Department, Department of Defense, and several intelligence agencies have banned the purchase of computers and printers from companies in which the Chinese government has an ownership stake, these procurement guidelines are not standard. What steps in the Administration taking to close these widespread critical cybersecurity vulnerabilities across the federal government?

Response: I share your concern with U.S. government cybersecurity vulnerabilities. However, this is not an area where I have expertise and therefore am unable to provide answers to these questions. I would be happy to schedule a follow up discussion to address any concerns that you may have.

3. The computing division of the Chinese Academy of Sciences (CAS) was added to the U.S. government's Entity List in December 2022. Why does the U.S. government continue to allow federal departments and agencies to purchase computers from other firms that CAS owns? Why should a known security threat like Lenovo, in which CAS has a significant ownership stake that it tries to hide through subsidiary entities, be allowed to sell equipment to the U.S. federal government?

Response: I share your concern with U.S. government cybersecurity vulnerabilities. However, this is not an area where I have expertise and therefore am unable to provide answers to these questions. I would be happy to schedule a follow up discussion to address any concerns that you may have.

Question 4: Which allies and partners should the US be working with to help diversify supply chains away from China?

Response: It is imperative that policymakers create a federal policy framework to support the development of autonomous vehicles. This includes passing federal legislation that addresses matters like vehicle exemption caps and directs the National Highway Traffic Safety Administration (NHTSA) to complete rulemakings that encourage deployment of AVs. At the

same time, the United States should work with its strategic allies to ensure market access for U.S. AV developers. These critical measures will help solidify American leadership on autonomous vehicles in the future.

Rep. Fulcher: China is also trying to be the leader in key technologies and other industries per its Made in China 2025 by setting industry standards. If they take our technology and develop it, then they can use their government power to spend their way into foreign markets, setting the standards for a particular industry. I am thinking about Autonomous Vehicle (AV) technology.

This would give it not only preference in foreign ventures, but force U.S. companies to meet potentially a dual set of standards, making it more costly for them to compete and potentially turning over sensitive information in the process.

What can Congress do to strengthen rules when it comes to U.S. and foreign companies participating in certain standards-setting bodies? What tools can we use, what sharpening of our authorities can we employ to strengthen the U.S. role in countering China's efforts to drive these standards?

Response: I share your concern about the risks posed by China setting industry standards in the AV sector, and the risks posed to U.S. based companies if China were to lead on standard setting. Standard setting organizations provide an important channel for industry-government collaboration by ensuring companies are operating from consensus terminology and practices. A comprehensive federal framework for autonomous vehicle deployment would put the U.S. in a leadership position globally and could empower U.S. companies to work with standards setting bodies to develop leading industry standards. The AV industry has a track record of working with standard setting organizations such as the Society of Automotive Engineers ("SAE") and the Commercial Vehicle Safety Alliance ("CVSA"). Many of our member companies sit on SAE committees tasked with developing automation industry standards. AVIA also has worked extensively with CVSA to develop inspection standards for commercial vehicles equipped with automated driving systems.

Attachment 1—Additional Questions for the Record

The Honorable Neal Dunn

1. A July 2019 Inspector General's report found that the Department of Defense continues to buy tens of millions of dollars in Commercial off the Shelf (COTS) technologies with known cybersecurity risks such as Lenovo computers, Lexmark printers, and GoPro cameras. What is the U.S. government doing to close loopholes that Lenovo and other IT firms in which the Chinese government has an ownership stake can exploit to sell its equipment to the U.S. military and other federal government departments and agencies?

2. Although the State Department, Department of Defense, and several intelligence agencies have banned the purchase of computers and printers from companies in which the Chinese government has an ownership stake, these procurement guidelines are not standard. What steps in the Administration taking to close these widespread critical cybersecurity vulnerabilities across the federal government?

3. The computing division of the Chinese Academy of Sciences (CAS) was added to the U.S. government's Entity List in December 2022. Why does the U.S. government continue to allow federal departments and agencies to purchase computers from other firms that CAS owns? Why should a known security threat like Lenovo, in which CAS has a significant ownership stake that it tries to hide through subsidiary entities, be allowed to sell equipment to the U.S. federal government?

4. Which allies and partners should the US be working with to help diversify supply chains away from China?

5. You have commented in the past about the potential for creating a network of trusted trading partners. You propose that to do so, we must lower trade barriers to help create a resilient and reliable allied supply chain. Can you discuss this issue and why it has merit?

Responses from Marc Jarsulic

Responses to these five questions, in the order presented:

1. This question could best be answered by appropriate U.S. government agencies.

2. This question could best be answered by appropriate U.S. government agencies.

3. This question could best be answered by appropriate U.S. government agencies.

4. This question could best be answered by appropriate U.S. government agencies.

5. Trade policies should put the interests of U.S. workers front and center. An outline of this approach can be found in "Trump's Trade Deal and the Road Not Taken", available

at https://www.americanprogress.org/article/trumps-trade-deal-road-not-taken/. That paper explains that a worker-centered trade policy would include several elements, among them strong, detailed standards and meaningful enforcement for meaningful labor and the environment rules; trade-related tools to address the threat of climate change; and greater ability for U.S. businesses and farmers to distinguish their products, whether for consumer right-to-know, climate-labeling, or other purposes, from import competition. In addition, such a trade regime would avoid the inclusion of harmful elements, such as allowing companies to override needed domestic regulation through investor-state dispute mechanisms, or the inclusion of limitations to effective competition policy.

House Energy & Commerce Subcommittee on Innovation, Data, and Commerce
Additional Questions Submitted for the Record
Samm Sacks

Honorable Larry Bucshon

1. A July 2019 Inspector General's report found that the Department of Defense has purchased tens of millions of dollars of Commercial off the Shelf (COTS) technologies with known cybersecurity risks from IT firms in which the Chinese government has an ownership stake. What is the U.S. government doing to protect the U.S. military and other government departments and agencies against the risks associated with this behavior?

Answer: My understanding is that there are range of mandated requirements for ICT products used by the U.S. government and military when it comes to supply chain security, but answering what the DOD is doing specifically on IT purchases of COTS is beyond my area of expertise and focus of my research. I also encourage the Administration to further examine and review areas of the supply chain that present vulnerabilities that may not be covered and merit additional scrutiny and restrictions.

2. Although the State Department, Department of Defense, and several intelligence agencies have individually banned the purchase of computers and printers from companies in which the Chinese government has an ownership stake, these procurement guidelines are not standard across federal agencies. What steps is the Administration taking to close these widespread critical cybersecurity vulnerabilities?

Answer: I do not know the answer to this question. Please see response above.

3. The computing division of the Chinese Academy of Sciences (CAS) was added to the U.S. government's Entity List in December 2022. Do you believe the U.S. government should continue to allow federal departments and agencies to purchase computers from other firms that CAS owns, or firms in which CAS has a significant ownership stake? Why or why not?

Answer: The Chinese Academy of Science holds the status of a government Ministry in China. It is a powerful and influential research institute connected with senior government leadership and involved with directing science and technology policy. I am not familiar with the specific division or subsidiary firm that sells computers, but my understanding is that any firm listed on the U.S. government's Entity List has been identified for restrictions on sales or transfer of U.S. technology due to a preponderance of evidence that the entity has connections to actors in the government or military in China that pose U.S. national security risks. While the Entity List would not itself restrict purchasing technology from any identified firm, the fact that any firm is listed there reflects there are factors of concern related to U.S. national security that should be factored into any sensitive commercial or U.S. government procurement decisions.

Honorable Neal Dunn

1. A July 2019 Inspector General's report found that the Department of Defense continues to buy tens of millions of dollars in Commercial off the Shelf (COTS) technologies with known cybersecurity risks such as Lenovo computers, Lexmark printers, and GoPro cameras. What is the U.S. government doing to close loopholes that Lenovo and other IT firms in which the Chinese government has an ownership stake can exploit to sell its equipment to the U.S. military and other federal government departments and agencies?

Answer: I do not know what specific steps the U.S. government is taking regarding purchases from Lenovo, Lexmark, and GoPro cameras. I have not researched these specific companies and their associated cybersecurity risks.

2. Although the State Department, Department of Defense, and several intelligence agencies have banned the purchase of computers and printers from companies in which the Chinese
government has an ownership stake, these procurement guidelines are not standard. What steps in the Administration taking to close these widespread critical cybersecurity vulnerabilities across the federal government?

Answer: The question of U.S. government procurement of computers and printers in relation to China is not something I have looked at in depth. I applaud the Administration for its recently released National Cybersecurity Strategy and its efforts to close critical cybersecurity vulnerabilities across several areas, including mandated cybersecurity requirements (beyond recommended standards), security by design, and examining loopholes and unaddressed vulnerabilities tied to market incentives.

3. The computing division of the Chinese Academy of Sciences (CAS) was added to the U.S. government's Entity List in December 2022. Why does the U.S. government continue to allow federal departments and agencies to purchase computers from other firms that CAS owns? Why should a known security threat like Lenovo, in which CAS has a significant ownership stake that it tries to hide through subsidiary entities, be allowed to sell equipment
to the U.S. federal government?

Answer: The Chinese Academy of Science holds the status of a government Ministry in China. It is a powerful and influential research institute connected with senior government leadership and involved with directing science and technology policy. I am not familiar with the specific division or subsidiary firm that sells computers, but my understanding is that any firm listed on the U.S. government's Entity List has been identified for restrictions on sales or transfer of U.S. technology due to a preponderance of evidence that the entity has connections to actors in the government or military in China that pose U.S. national security risks. While the Entity List would not itself restrict purchasing technology from any identified firm, the fact that any firm is listed there reflects there are factors of concern related to U.S.

national security that should be factored into any sensitive commercial or U.S. government procurement decisions.

4. Which allies and partners should the US be working with to help diversify supply chains away from China?

Answer: Democracies with systems based on rule of law as well as non-democracies considered to be like-minded governments.

Honorable Russ Fulcher

Much of the danger of using Chinese infrastructure and companies when research, development,
and subsequent data from testing, comes from the potential for Chinese vendors to access information from the back end.

1. Would there be benefits to creating a data reciprocity community, like a "Transparency Defensive Alliance" for corporate data sharing, for countries allied with western standards of corporate conduct and accountability and western values?

Answer: A Data Allies approach involves a coalition of partners (democracies with systems based on rule of law as well as non-democracies considered like-minded governments) working together within a framework to develop principles for transferring data among themselves. Allies use a principled basis to facilitate more data sharing within each other, while also using a more strict standard for "adversary" countries like Russia and China to access Americans' data. The OECD "Declaration on Government Access to Personal Data held by Private Sector Entities" announced on December 14 represents an example of this kind of approach for facilitating data flows among OECD nations. The Commerce Department's Global Cross Border Privacy Rules (CBPR) Declaration also fits into this model by promoting data flows among certain countries based on an international certification system.
This model could also take the form of an adequacy determination approach to allies, drawing on the European and UK systems.

Creating a coalition of data-sharing allies would help the United States more seamlessly import data with economic and national security benefits. Despite the emphasis in recent U.S. policy proposals on restricting outbound U.S. data transfers, the reality is that the United States primarily imports, not exports, data from the rest of the world. Since the United States is a data importing country (both from an economic and national security perspective), we benefit from policies that help create a durable coalition of countries allowing their data to be sent to the United States. 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.

This model sets up a framework for countries to share their data—even if those countries lack identical data protection laws—by setting achievable, similar standards for data to flow. It allows more companies both large and small to operate globally, in contrast to a situation

where only a few of the largest firms can afford to comply with different data protection laws in many countries.

Being part of a large data sharing coalition, the United States could create more economic incentives for other parts of the world to join, from Latin America to parts of the Southeast Asia. The economic pull of such a coalition offers an appealing to alternative to other countries that may be considering modeling their own system based on China's model.

2. Would it be beneficial to extend this sort of an agreement to encompass cloud storage and other services that may be shared with a host company or nation?

Answer: It is also important to recognize that country or geography is not synonymous with security. There are existing NIST and other internationally recognized standards for the safe and secure cloud storage practices regardless of where that data is stored.

WRITTEN RESPONSES – QUESTIONS FOR THE RECORD

BRANDON J. PUGH, ESQ.
POLICY DIRECTOR & RESIDENT SENIOR FELLOW,
CYBERSECURITY & EMERGING THREATS
R STREET INSTITUTE

FOR THE

SUBCOMMITTEE ON INNOVATION, DATA, AND COMMERCE
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON

ECONOMIC DANGER ZONE:
HOW AMERICA COMPETES TO WIN THE FUTURE VERSUS CHINA
FEBRUARY 1, 2023

Attachment 1—Additional Questions for the Record

The Honorable Larry Bucshon

1. *A July 2019 Inspector General's report found that the Department of Defense has purchased tens of millions of dollars of Commercial off the Shelf (COTS) technologies with known cybersecurity risks from IT firms in which the Chinese government has an ownership stake. What is the U.S. government doing to protect the U.S. military and other government departments and agencies against the risks associated with this behavior?*

   The 2019 Inspector General's report was alarming and highlighted what many suspected about Commercial off the Shelf (COTS) technologies, including that adversaries could exploit known cybersecurity vulnerabilities in COTS items purchased by the Department of Defense and other federal agencies. The 2023 National Cybersecurity Strategy notes that the federal government will continue to focus on software supply chain risk mitigation in federal civilian executive branch (FCEB) agencies and replace or update systems that are not defensible against sophisticated cyber threats. Executive Order 14028, "Improving the Nation's Cybersecurity," expressed similar themes.

   While COTS are not specifically named in either, I am hoping they are one aspect of the administration's implementation plan. Unfortunately, the issue is not isolated at the federal level because local and state entities often use these devices, including in K-12 schools.

2. *Although the State Department, Department of Defense, and several intelligence agencies have individually banned the purchase of computers and printers from companies in which the Chinese government has an ownership stake, these procurement guidelines are not standard across federal agencies. What steps is the Administration taking to close these widespread critical cybersecurity vulnerabilities?*

   A consistent approach is critical in addressing cybersecurity concerns that are present with both software and hardware made partially or fully by Chinese-backed or Chinese-owned companies. The 2023 National Cybersecurity Strategy furthers the call for technology modernization and eliminating legacy systems that are difficult to defend. I am hopeful that will entail removing concerning technology that already exists. Looking ahead, part of the strategy entails furthering EO 14028 to ensure "contract requirements for cybersecurity are strengthened and standardized across Federal agencies," along with enforcement when companies do not follow best practices. Specifics are not clear, but I am hopeful this will entail products with links to countries of concern like China.

3. *The computing division of the Chinese Academy of Sciences (CAS) was added to the U.S. government's Entity List in December 2022. Do you believe the U.S. government should continue to allow federal departments and agencies to purchase computers from other firms that CAS owns, or firms in which CAS has a significant ownership stake? Why or why not?*

   The Chinese Academy of Sciences Institute of Computing Technology was one of 36 entities added to the Entity List for "acting contrary to the national security or foreign policy interests of the United States." If an entity is on this list, we must be concerned and skeptical of other transactions by firms that are fully or partially owned by the entity so they cannot use a subsidiary as a workaround to exploit or create vulnerabilities. Availability, convenience and

cost are factors for purchasing these products, but those factors should not outweigh security risks. I recommend that the Department of Commerce conduct a review of all of these entities for potential additions to the Entity List.

The Honorable Neal Dunn

1. *A July 2019 Inspector General's report found that the Department of Defense continues to buy tens of millions of dollars in Commercial off the Shelf (COTS) technologies with known cybersecurity risks such as Lenovo computers, Lexmark printers, and GoPro cameras. What is the U.S. government doing to close loopholes that Lenovo and other IT firms in which the Chinese government has an ownership stake can exploit to sell its equipment to the U.S. military and other federal government departments and agencies?*

   The 2019 Inspector General's report was alarming and highlighted what many suspected about Commercial off the Shelf (COTS) technologies, including that adversaries could exploit known cybersecurity vulnerabilities in COTS items purchased by the Department of Defense and other federal agencies. The 2023 National Cybersecurity Strategy notes that the federal government will continue to focus on software supply chain risk mitigation in federal civilian executive branch (FCEB) agencies and replace or update systems that are not defensible against sophisticated cyber threats. Executive Order 14028, "Improving the Nation's Cybersecurity," expressed similar themes.

   While COTS are not specifically named in either, I am hoping they are one aspect of the administration's implementation plan. Unfortunately, the issue is not isolated at the federal level because local and state entities often use these devices, including in K-12 schools.

2. *Although the State Department, Department of Defense, and several intelligence agencies have banned the purchase of computers and printers from companies in which the Chinese government has an ownership stake, these procurement guidelines are not standard. What steps is the Administration taking to close these widespread critical cybersecurity vulnerabilities across the federal government?*

   A consistent approach is critical in addressing cybersecurity concerns that are present with both software and hardware made partially or fully by Chinese-backed or Chinese-owned companies. The 2023 National Cybersecurity Strategy furthers the call for technology modernization and eliminating legacy systems that are difficult to defend. I am hopeful that will entail removing concerning technology that already exists. Looking ahead, part of the strategy entails furthering EO 14028 to ensure "contract requirements for cybersecurity are strengthened and standardized across Federal agencies," along with enforcement when companies do not follow best practices. Specifics are not clear, but I am hopeful this will entail products with links to countries of concern like China.

3. *The computing division of the Chinese Academy of Sciences (CAS) was added to the U.S. government's Entity List in December 2022. Why does the U.S. government continue to allow federal departments and agencies to purchase computers from other firms that CAS owns? Why should a known security threat like Lenovo, in which CAS has a significant ownership stake that it tries to hide through subsidiary entities, be allowed to sell equipment to the U.S. federal government?*

The Chinese Academy of Sciences Institute of Computing Technology was one of 36 entities added to the Entity List for "acting contrary to the national security or foreign policy interests of the United States." If an entity is on this list, we must be concerned and skeptical of other transactions by firms that are fully or partially owned by the entity so they cannot use a subsidiary as a workaround to exploit or create vulnerabilities. Availability, convenience and cost are factors for purchasing these products, but those factors should not outweigh security risks. I recommend that the Department of Commerce conduct a review of all of these entities for potential additions to the Entity List.

4. *Which allies and partners should the US be working with to help diversify supply chains away from China?*

   Supply chain risks only continue to expand, especially considering we rely on countries like China for essential products and components. Bringing back more manufacturing to the United States is a key way to help mitigate cybersecurity risks, to make American companies more competitive and to reduce our reliance on countries of concerns. Relatedly, "friend-shoring" is a way to diversify and secure our nation's supply chain. This can empower countries that the United States has positive relations with, like our military allies, to produce products that we need without relying on concerning countries like China. This can also entail working with countries closer to the United States to help minimize supply chain risks like we have already done with Mexico.

The Honorable Greg Pence

I share your concerns of anti-competitive practices of the Chinese Communist Party and their efforts to undermine innovation here in the U.S. Rightfully so, companies across the world are re-thinking their partnerships with the CCP, who have spent decades cornering critical supply chains by stealing intellectual property and manipulating free markets.

As the U.S. continues re-building our domestic manufacturing base, foreign direct investment will be a critical tool to work alongside allied nations against the illegal subterfuge of China and bring good-paying jobs to communities in Indiana and across the country. Indiana is a national leader in attracting foreign direct investment from allied countries. Over 200,000 Hoosiers are employed by international companies, of which 56 percent are in the manufacturing sector. To continue fostering strong growth in these sectors, I introduced the Global Investment in American Jobs Act last Congress, which seeks to identify barriers to innovation and promote investment from our friends abroad to open new markets.

I am concerned, however, that China could be circumventing national security laws to gain footholds in domestic industries, particularly in next generation technologies. These efforts could threaten the security of our nation as well as the privacy of our citizens.

1. *In your view, how can foreign direct investment from allied nations be used as a tool to combat anti-competitive practices of the Chinese Communist Party?*

   Foreign direct investment (FDI) from allied nations can be helpful in combating anti-competitive practices of the Chinese Communist Party in two main ways. First, we see China being a large recipient of FDI and that strengthens China and its companies. It is important for the United States to foster an environment favorable for FDI to ensure we

outpace China on receiving FDI. Second, Chinese firms are eager to invest in the United States, which presents risks and strengthens a main rival. It is important to ensure our allies are empowered to push back against China.

2. *How can Congress secure the landscape of foreign direct investment from allied countries and prevent China from subverting national security laws to gain strongholds in domestic industries?*

   There are risks with FDI from firms that are directed, controlled or funded by select foreign governments like the Chinese Communist Party. FDI can be leveraged to make China stronger or even exploit security vulnerabilities. Congress should ensure a climate is created that fosters innovation from our allies, while ensuring that risky investments are properly vetted or avoided.

The Honorable Russ Fulcher

As a former Micron tech executive, I get the foreign subsidy challenge. I dealt with it against Japan in the 1980s, and others since. That is a part of dealing with various governments. What is different in this case is the level and systematic theft, and then subsidizing the technology from these ill-gotten gains.

As the Congressional Research Service (CRS) noted, China's strategy involves the "process of introducing, absorbing, and adapting" foreign technology and then "rebranding" that technology as its own.

The "One Belt, One Road" initiative is one way they do this. We know it includes requiring some industry sensitive information to be shared by the foreign company in a joint venture with a Chinese-backed company in China. But it also includes various types of collaboration centers, open technology grabs, and overseas academic and non-academic research centers.

1. *When it comes to basic research, what are things we can do to protect open source technology platforms, and are there areas in U.S. export control laws that need to be strengthened?*

   Open source software and related technologies offer benefits like fostering collaboration and access, but there can be cybersecurity risks. For example, a known vulnerability can be exploited to compromise data or an entire system, or software might be outdated. Also, we see Chinese developers contributing to open source projects. To combat this, it is important that entities are aware of known vulnerabilities, that United States' software manufacturers implement strong security and that we do not allow China to dominate open source efforts.

2. *When it comes to online research, I support the committee's efforts to move on legislation from the last Congress that would alert users who go to a website that is owned by the Chinese Communist Party. What next steps to secure online collaboration among researchers, or allow the U.S. to take actions against CCP-backed efforts to steal our IP? Emerging patent courts and laws in China?*

   Unfortunately, China's quest to steal United States' data is not new and it is an ongoing concern. This ranges from data on Americans to our intellectual property. Awareness of the threat is one key step. For example, a comprehensive data privacy and security law like the American Data Privacy and Protection Act (ADPPA) would alert individuals if their data is being transferred to select countries like China, which puts the individual on notice and allows them the option to proceed or not. Actions by law enforcement, federal agencies, and even the private sector must continue to help stop bad actors from stealing our data and property. This also entails making sure public and private sector entities are prepared and resourced, especially our smallest entities.

Much of the danger of using Chinese infrastructure and companies when research, development, and subsequent data from testing, comes from the potential for Chinese vendors to access information from the back end.

3. *Would there be benefits to creating a data reciprocity community, like a "Transparency Defensive Alliance" for corporate data sharing, for countries allied with western standards of corporate conduct and accountability and western values?*

   Creating a system or process for corporate data sharing could be a helpful tool for countries allied with western standards of corporate conduct, but there are many questions to answer first. A key threshold point is that there is always the risk for a bad actor to access and exploit data so this community would not be foolproof. This would require clarity on the type of data to be shared, security protections, how international laws would be implicated like those on data privacy, and access and monitoring rules, among other areas.

4. *Would it be beneficial to extend this sort of an agreement to encompass cloud storage and other services that may be shared with a host company or nation?*

   As the foundation and structure for a data reciprocity community are explored, I think encompassing cloud storage and other services that might be shared with a host country and/or nation is worth exploring.

Attachment 2—Member Requests for the Record

The Honorable Debbie Lesko

When a security camera that was made in China is connected to wireless internet in the United States, have there been instances where this information has been transmitted back to China?

There are many software and hardware products that pose risks like connected devices. For example, there are reports of baby cameras spying on children, electronic locks being remotely opened and robot vacuum cleaners recording people in the bathroom. Some manufacturers implement strong privacy and security measures, but that is not the case for all and many devices lack even basic security measures.

Even more troubling, there is a lack of clarity about what is and is not accessible in China. With so many Internet of Things (IoT) devices made fully or partially in China, it is possible for the data to be collected and harvested in China. We have seen cases where Chinese-made cameras with security vulnerabilities have permitted remote access and eavesdropping. Options to help address these concerns include acting on a comprehensive data privacy and security law, advancing an IoT label for consumers and furthering IoT security baselines.

The Honorable Kat Cammack

How can we protect our kids and data while simultaneously respecting free market economics?

Acting on a comprehensive data privacy and security law, like the American Data Privacy and Protection Act (ADPPA) from the last Congress, is the best way to protect our kids and data. While there are bills specifically aimed at protecting kids, a comprehensive approach would simultaneously protect kids and all Americans. Threats to our data continue to increase so it is critical that the threat be dealt with for all.

A comprehensive bill would also better assist companies of varying sizes so they would have one law to follow, rather than the growing patchwork of state laws that is becoming a compliance nightmare and resource drain. When legislation is contemplated, it should consider businesses of all sizes, include strong preemption language, and be based on achieving compliance rather than being enforcement-heavy.

○