

# U.S. LEADERSHIP ON ARTIFICIAL INTELLIGENCE IN AN ERA OF STRATEGIC COMPETITION

---

## HEARING

BEFORE THE

## COMMITTEE ON FOREIGN RELATIONS UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

NOVEMBER 15, 2023

Printed for the use of the Committee on Foreign Relations



Available via <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2024

COMMITTEE ON FOREIGN RELATIONS

BENJAMIN L. CARDIN, Maryland, *Chairman*

ROBERT MENENDEZ, New Jersey	JAMES E. RISCH, Idaho
JEANNE SHAHEEN, New Hampshire	MARCO RUBIO, Florida
CHRISTOPHER A. COONS, Delaware	MITT ROMNEY, Utah
CHRISTOPHER MURPHY, Connecticut	PETE RICKETTS, Nebraska
TIM KAINE, Virginia	RAND PAUL, Kentucky
JEFF MERKLEY, Oregon	TODD YOUNG, Indiana
CORY A. BOOKER, New Jersey	JOHN BARRASSO, Wyoming
BRIAN SCHATZ, Hawaii	TED CRUZ, Texas
CHRIS VAN HOLLEN, Maryland	BILL HAGERTY, Tennessee
TAMMY DUCKWORTH, Illinois	TIM SCOTT, South Carolina

DAMIAN MURPHY, *Staff Director*

CHRISTOPHER M. SOCHA, *Republican Staff Director*

JOHN DUTTON, *Chief Clerk*

# C O N T E N T S

---

	Page
Cardin, Hon. Benjamin L., U.S. Senator From Maryland .....	1
Risch, Hon. James E., U.S. Senator From Idaho .....	3
Fick, Hon. Nathaniel, Ambassador-at-Large, Bureau for Cyberspace and Digital Policy, United States Department of State, Washington, DC .....	5
Prepared Statement .....	7
Graviss, Dr. Matthew, Chief Data and Artificial Intelligence Officer, United States Department of State, Washington, DC .....	9
Prepared Statement .....	11

## ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Responses of Mr. Nathaniel Fick to Questions Submitted by Senator Benjamin L. Cardin .....	30
Responses of Dr. Matthew Graviss to Questions Submitted by Senator Benjamin L. Cardin .....	34
Responses of Mr. Nathaniel Fick to Questions Submitted by Senator Christopher A. Coons .....	36
Responses of Mr. Nathaniel Fick to Questions Submitted by Senator Brian Schatz .....	37
Letter to President Biden, Dated November 30, 2023, Concerning the Decision of the USTR To Stop Supporting Key Commitments in the E-Commerce Negotiations at the WTO .....	39



# **U.S. LEADERSHIP ON ARTIFICIAL INTELLIGENCE IN AN ERA OF STRATEGIC COMPETITION**

**WEDNESDAY, NOVEMBER 15, 2023**

U.S. SENATE,  
COMMITTEE ON FOREIGN RELATIONS,  
*Washington, DC.*

The committee met, pursuant to notice, at 10:04 a.m., in room SD-419, Dirksen Senate Office Building, Hon. Benjamin J. Cardin presiding.

Present: Senators Cardin [presiding], Menendez, Shaheen, Kaine, Merkley, Van Hollen, Risch, Romney, Ricketts, Young, and Barrasso.

## **OPENING STATEMENT OF HON. BENJAMIN L. CARDIN, U.S. SENATOR FROM MARYLAND**

The CHAIRMAN. The Senate Foreign Relations Committee will come to order.

This hearing of the Senate Foreign Relations Committee, the subject is the AI revolution and I look forward to our testimony from our witnesses.

As I think most members know, our leadership, including with Senator Young, have been busy setting up a college for us to learn AI. We appreciate it very much. We are getting continuing Senate credits for our attendance at the AI conferences, so thank you, Senator Young, for your leadership in putting that together.

This is just another opportunity for the role that the Foreign Relations Committee will play in regards to what is our appropriate policies as it relates to AI.

The AI revolution is going to change economics. It is going to change societies. It is going to change the entire world. That means it is also going to change the way we do diplomacy.

Today's advanced AI models are 5 billion times more powerful than just a decade ago—that is 5 billion times—the kind of technology growth is unlike anything humans have ever invented, and we are still just at the early stages of the AI revolution.

It has the potential to usher in unpredictable, complicated challenges like empowering digital authoritarianism or spreading bias and disinformation or locking us into a spiraling AI race against our adversaries.

At the same time, the AI revolution will bring about positive possibilities unseen in human history—predicting the outbreak of war,

improving harvests to solve food security, curing deadly diseases, unlocking green energy.

I want to thank our witnesses for appearing before us today. I know you and your team face challenges. Preparing the world to responsibly harness and deploy AI will be difficult. Preparing the Department of State for the future will not be easy either.

I want to thank you for the accomplishments you have advanced so far and for the heroic efforts that you are engaging in. Your dedication and commitment in serving our nation is appreciated.

Your teams include some of the sharpest minds in our government. That is why I want to challenge you to do even more.

Thus far much of the discussions around AI have centered around the military and private sector, but making money or making war is too narrow of an approach for the AI revolution.

We need to proceed with an AI agenda that is wrapped in American values. That is why I think the State Department is not only crucial to this effort; the State Department must be a leader in global AI governance efforts.

The State Department has valuable data. That data has not always been well-organized or used to its fullest potential. This includes real-time information from embassies and diplomats stationed around the world. It includes the U.N. voting records. It includes environmental and economic trends.

This is highly valuable information. We know how much we are trying to gather information today and how valuable that is for the private sector. State needs to unlock the insights from this novel data and you have the workforce to do just that.

The Department has concentrated public servants who have—with advanced degrees and go beyond foreign policy. Your data science experts are going to be vital in this effort.

Our diplomats also must be involved as we manage our AI competition with nations like China and Russia. Diplomats know how to take on complex and multifaceted problems.

They know how to balance competing ideas when making policy and, most importantly, American diplomats know how to drive an agenda based on American values—values that need to be part of the AI revolution, values that protect people's privacy, values that lead to democratic elections, respect for human rights, and peace and security for people around the world.

If we are going to lead on global AI governance, if we are going to avoid a dangerous AI arms race, if we are going to harness AI to improve the lives of people on this planet, the State Department must be in the lead. It cannot be left to generals without diplomats.

I believe Congress and this committee in particular must play a central role in guiding America's AI efforts. I hope you will share your thoughts on how you think Congress can accomplish that.

I now recognize our distinguished ranking member: Senator Risch.

**STATEMENT OF HON. JAMES E. RISCH,  
U.S. SENATOR FROM IDAHO**

Senator RISCH. Thank you very much, Mr. Chairman.

The ongoing wars in Europe and the Middle East are reminders of the threats and instability that define the era of strategic competition in which we live.

Amidst the images of chaos and destruction splashed across the headlines, yet another competition is arising. New advances in AI will transform the way we live, do business, and interact with the world. These advances also have significant implications for our foreign policy and, importantly, national security.

The United States and our allies must lead the world in developing the transformational technologies and the standards that govern them. That will shape the future. If harnessed appropriately, AI-driven algorithms can provide the State Department with real-time data and insights.

This includes everything from how effective policies are in different parts of the world to which IT vulnerabilities are most likely to be exploited by an adversary to which overseas staffing models are most efficient and effective in meeting the Department's needs.

We must also prepare for the ways our adversaries like Russia, Iran, and particularly China are trying to use AI. AI-powered cyber attacks could overwhelm our defenses by rapidly identifying our vulnerabilities and exploiting them. AI-driven information operations could target government officials or certain segments of the public and confuse, distract, or paralyze the decision-making process.

AI-enabled battlefield management systems could give our adversaries a decisive advantage in targeting U.S. forces and striking key weak points. Since AI and machine learning rely on accurate data to work correctly, our adversaries could also deliberately manipulate or corrupt publicly available databases to ensure predictive models or analytics used by the U.S. Government do not work properly during a crisis.

To respond to both the opportunities and the threats posed by new AI-driven technologies, the State Department should focus on two areas, and I hope our witnesses will be able to talk more about those today.

First, we need to work with our allies to set the standards that will govern how AI is used around the world. We need to collaborate on research in key areas and identify the specific national security-sensitive technologies that adversaries like China will try to steal or copy and thereafter develop tougher safeguards to answer those issues.

Ambassador Fick, Congress established the Bureau of Cyberspace and Digital Policy, which you lead, in part to spearhead this type of engagement with allies. I look forward to hearing more from you about the work you are doing in this area.

I would also like to hear your insights into how AI could transform the cyber threat landscape and what you are doing about that.

Second, we need a workforce that not only understands how data and AI and machine learning work, but also how to integrate these tools into their daily work.

I am pleased to see the Department begin to pursue a data-driven approach to diplomacy because it has the potential to improve our foreign policy. Using all the information available to make national security decisions is a crucial part in getting to the right answer.

Data-driven diplomacy also helps counteract groupthink within the Department which limits options and stifles critical thinking, but data-driven diplomacy cannot just be a talking point. The Department has to truly commit to integrating data into the policy-making process and changing course if necessary when it receives objective feedback that a policy or procedure simply is not working.

The State Department's Center for Data Analytics was established to better integrate data analysis and expertise into foreign policy decision-making and to develop a workforce that possesses the skills needed to take advantage of these technologies.

Dr. Graviss, I look forward to hearing more about the progress the Center for Analytics has made in expanding data access and utilization throughout the Department. Any insights you have into challenges and obstacles that remain would be greatly appreciated.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Risch, which is most of the cases our opening statements are very comparable and very similar. Thank you very much for your leadership here and I look forward to working with you.

Senator RISCH. You are not suggesting to plagiarize, are you?

The CHAIRMAN. No, I am suggesting we might want to combine some of our staff and save some—no, I am just—

[Laughter.]

The CHAIRMAN. It is always interesting to hear the opening statement from my colleague.

We have two very distinguished witnesses today: Ambassador Fick and Dr. Graviss. I am going to introduce both of you. Your full statements will be made part of our record.

We would ask that you proceed in about 5 minutes so we have time for the members to ask questions and to have a discussion.

First, let me introduce Ambassador Fick, who currently leads the State Department's Bureau of Cyberspace and Digital Policy. As the inaugural ambassador-at-large, Ambassador Fick has taken the reins at a critical moment for strengthening U.S. diplomatic efforts on cyber and digital issues, particularly the rapid development of AI technologies.

Prior to his leadership of the CDP bureau, Ambassador Fick had extensive career in the private sector as a technology executive and entrepreneur.

He has also served as a Marine Corps infantry reconnaissance officer including combat tours in Afghanistan and Iraq. We thank you for your service to our country in so many different ways.

Dr. Graviss has been the Department's chief data officer since December 2020. He has recently selected to serve as the Department's inaugural chief artificial intelligence officer in a dual-hatted capacity.

This also comes at a critical moment as the executive branch agencies react to the development and deployment of artificial intelligence and other data analytical tools.



Prior to his leadership of the Department's Center for Analytics, Dr. Graviss spent 13 years in leadership positions at the Department of Homeland Security as well as his time in the private sector.

He holds a master's degree in mechanical engineering from Texas A&M University and a doctorate in systems engineering from George Washington University.

We will start with Ambassador Fick.

**STATEMENT OF HON. NATHANIEL FICK, AMBASSADOR-AT-LARGE, BUREAU FOR CYBERSPACE AND DIGITAL POLICY, UNITED STATES DEPARTMENT OF STATE, WASHINGTON, DC**

Mr. FICK. Good morning, Chairman Cardin, Ranking Member Risch, distinguished members of the committee.

On behalf of the Department of State, thank you for the opportunity to speak here today and, more broadly, thank you for your support over the 14 months I have been in this new role.

I am pleased to provide you today with an update on our work in the service of the United States international technology policy priorities and will speak specifically to our efforts to strengthen U.S. global leadership to unlock the potentials of AI while also addressing its challenges.

At the State Department, I oversee the organizations that lead and coordinate the Department's work on cyberspace, digital policy, and emerging technologies, and there are two of them: the Bureau of Cyberspace and Digital Policy, known as CDP, and also the Office of the Special Envoy for Critical and Emerging Tech, S/TECH for short.

Building on years of bipartisan work, Secretary of State Blinken established these organizations in partnership with Congress as part of a comprehensive effort to modernize American diplomacy and make technology central to U.S. foreign policy.

He gave us a very clear mission: to shape the terms of the technology future, and to extend America's industrial and innovation strategy into the international realm.

Together, CDP and S/TECH with our interagency partners work to advance U.S. global leadership on topics such as: trusted technologies in digital infrastructure, advanced wireless networks, quantum computing, biotechnology and synthetic biology, cloud services and data centers, undersea communications cables, satellite communications, and, yes, AI.

We also work to build partner cybersecurity capacity, to strengthen international technical standards, to advance global cyber stability and counter adversaries in cyberspace and, finally, we use technology to promote and protect human rights.

An important distinction between my work and the work of my colleague appearing with me today, Dr. Graviss, is that my team focuses on leading U.S. diplomacy on technology topics with external international audience while Dr. Graviss' work is focused on AI deployment within the Department.

As someone who has spent a decade building and leading a software business and after a couple combat tours in the Marines, I do believe very fundamentally that responsible technology innovation is increasingly a foundational source of our geopolitical power

and over the past year I have seen firsthand how these technologies are transforming every aspect of our societies from how we work to how we learn to how we communicate, and they are transforming every aspect of our foreign policy.

Many traditional measures of national strength such as GDP or military capacity are increasingly downstream of a nation's ability to innovate in these key technology areas.

Put simply, in geopolitical competition terms, tech is increasingly the game. It is revolutionary, it is accelerating, and the United States must lead, engaging boldly on behalf of our values and our interests.

As the President recently said, we stand at an inflection point in history. Nowhere is that more evident than with AI. The decisions that we make today about how we shape the parameters around AI will define the world in so many ways for decades to come.

It is a responsibility that we must assume together with our private sector, with civil society, and with our international partners. American companies lead the world in AI innovation and the United States has increasingly strong momentum domestically to lead in AI governance.

The recent executive order on AI directs the most significant action any government anywhere in the world has ever taken on AI safety, security, and trust and it is the natural next step after having first secured the voluntary commitments that were agreed to by leading AI companies, and the President is committed to working with Congress to craft bipartisan legislation to establish an enduring domestic policy framework.

At the same time, we are working internationally with our closest partners to advance our shared views on AI policy. The G-7, with strong U.S. leadership and engagement, just released an international code of conduct for AI developers which draws heavily from the voluntary commitments.

I attended the U.K.'s AI safety summit 2 weeks ago at Bletchley Park, hallowed ground in the history of technology and national security, and we continue to work to advance shared approaches to AI with European partners through mechanisms including the U.S.-EU Trade and Technology Council.

Countries around the world realize that AI is now the foundational technology driving advances that can help solve some of our most pressing shared challenges in science, in energy, in agriculture, in education and more, and my team's role is to engage with the world in these conversations to synchronize multi-stakeholder approaches on governance, to harness the benefits of AI to mitigate its risks, and to do so while always ensuring that our innovation ecosystem remains our North Star.

We do this with three orienting principles in mind. First, it is essential for the United States to lead with an affirmative vision for the role of technology in our shared future.

We believe in tech's power to accelerate innovation, to solve major global challenges, and to support our future prosperity. Our affirmative vision is reflected in both our engagements and also in our foreign assistance through programs such as AI Connect and other recently announced programs to leverage AI to help reduce

poverty, to address energy needs, and to improve global public health.

By committing resources to these programs, we were able to secure follow-on investments from the private sector that leveraged our commitment of \$15 million—leveraged that commitment several times over to accelerate progress on the Sustainable Development Goals using AI.

The U.S. is the world's leader in innovation and if we do not champion the benefits of technology, who will? That is principle one.

Second, we know we must do this work in partnership with others. International partnerships on everything from R&D investment to standards harmonization to regulatory interoperability are the policy underpinnings that are necessary in order to seize this moment. No one can do this alone—no one country regardless of how big or powerful, no one company regardless of how advanced.

Over the past year, the State Department has been engaged constantly with our allies and with our partners, bilaterally and also in multilateral venues, like the G-7, the G-20, the OECD, the United Nations, to achieve tangible commitments on the responsible development, deployment, and use of AI, and through the Executive Order the U.S. is leading by example.

We are providing a model for the responsible use of this critical technology in our own government and we are committed to increasing participation in the AI voluntary commitments among leading companies both in the United States and around the world.

Third, we recognize that all of this is happening while a determined and well-resourced set of adversaries and competitors tirelessly advance a very different view of technology's role in our future.

They are aggressively trying to reshape the international rules-based order and are investing heavily in a worldview that prioritizes authoritarian tactics over democratic values and governance. Technology governance and specifically AI governance is one of the geopolitical imperatives of our time.

We need to lead international conversations to shape the global technology landscape in the future so that AI advances democratic values and human rights, protects our safety and our security, and supports our prosperity.

When the United States pulls back, our adversaries fill that void. Technology with global impact requires global action. The State Department is delivering on the important work of technology diplomacy for the American people.

Thank you again for the opportunity to join you today. I look forward to your questions and your input.

[The prepared statement of Mr. Fick follows:]

**Prepared Statement of Mr. Nathaniel Fick**

Chairman Cardin, Ranking Member Risch, and distinguished members of the Committee, on behalf of the Department of State, thank you for the opportunity to speak here today. More broadly, thank you for your unfailing support throughout the 14 months I have been in this new role. I am honored to provide you today with an update on our work in the service of the United States' international technology policy priorities and will speak specifically to our efforts to strengthen U.S. global leadership to unlock the potential of artificial intelligence (AI) while also addressing its challenges.

At the State Department, I oversee the organizations that lead and coordinate the Department's work on cyberspace, digital policy, and emerging technologies: the Bureau of Cyberspace and Digital Policy, known as CDP, and the Office of the Special Envoy for Critical and Emerging Technology, S/TECH for short. Building on years of bipartisan work, Secretary of State Antony Blinken established these organizations in partnership with Congress as part of a comprehensive effort to modernize American diplomacy and make technology central to U.S. foreign policy. He gave us a mission: to shape the terms of the technology future and to extend the Biden administration's modern industrial and innovation strategy into the international realm.

Together, CDP and S/TECH, with our interagency partners, work to advance U.S. leadership globally on topics such as: trusted technologies and digital infrastructure, artificial intelligence, advanced wireless networks, quantum computing, biotechnology, cloud services and data centers, undersea telecommunications cables, satellite communications; and trusted data flows across borders. We also work to build partner cybersecurity capacity; strengthen consensus-based international technical standards; advance global cyber stability and counter adversaries in cyberspace through sustained diplomatic initiatives and international partnerships; and finally, we use technology to promote and protect human rights.

An important distinction between my work and the work of my colleague appearing with me today, Dr. Matthew Graviss, is that my team focuses on leading U.S. diplomacy on technology topics with external, international audiences. So, while my team engages governments around the world, multilateral institutions, civil society, and industry, these efforts are stronger when we lead by example and responsibly and effectively use AI inside the State Department as well. That is where Dr. Graviss and his team's exciting work comes in, as he will explain shortly.

As someone who spent a decade building and leading a cybersecurity software company after a couple of combat tours in the Marines, I believe that responsible technological innovation is increasingly a foundational source of geopolitical power. Over the past year, I have seen firsthand in how technologies are transforming every aspect of our societies and our economies—how we work, how we learn, how we communicate, and how we care for ourselves. They are also transforming every aspect of our foreign policy. Many traditional measures of strength, such as GDP or military capacity, are increasingly downstream from our ability to innovate in core technology areas. In that sense, technology innovation is driving more and more of what is, and is not, possible in our foreign and national security policy. Put simply, in the realm of geopolitical competition, tech is the game. It is revolutionary and it is accelerating. The United States must lead, engaging boldly on behalf of our values and interests.

As the President recently said, “we stand at an inflection point in history” and nowhere is that more evident than with artificial intelligence. The decisions that we make collectively today about how we shape the parameters around AI will define our world for decades. It is a responsibility that we must assume together with our private sector, civil society, and our international partners. American companies lead the world in AI innovation, and the United States has increasingly strong momentum domestically to lead in AI governance. The recent Executive Order on AI directs the most significant action any government anywhere in the world has ever taken on AI safety, security, and trust. It is just the next step after securing the voluntary commitments agreed to by leading AI companies, and the President is committed to working with Congress to craft bipartisan legislation that establishes an enduring domestic policy framework.

At the same time, we are working internationally with our closest partners to advance our shared views on AI policy. The G7, with strong U.S. engagement, just released an International Code of Conduct for AI developers which draws heavily from the voluntary commitments. I attended the UK's AI Safety Summit 2 weeks ago at Bletchley Park, hallowed ground in the history of technology and national security. And we continue to work to advance shared approaches to AI with our European partners through the U.S.-EU Trade and Technology Council.

Countries around the world realize that AI is now the foundational technology driving advances that can help solve some of our most pressing shared challenges in science, health care, energy, transportation, education, and more. And AI is already ubiquitous—the choice is not whether AI will change our societies and economies, but how governments and societies use it responsibly. We must ensure that rights-respecting states sustain their competitive advantage, that the technologies benefit all our people, and that risks are mitigated.

My team's role—in partnership with the U.S. Agency for International Development, which is leading on how AI can be used to advance global development—is to engage with the world in these conversations—to synchronize multi-stakeholder

approaches on AI governance, to harness the benefits of AI, to mitigate its risks, and to do so while encouraging our innovation ecosystem. We do this with three orienting principles always in mind:

First, it is essential for the United States to lead with an affirmative vision for the role of technology in our shared future. We believe in technology's power to accelerate innovation, to solve major global challenges, and to support our future prosperity. Our affirmative vision is reflected in both our engagements and foreign assistance, through programs such as AI Connect at State and the Responsible Computing Challenge and Equitable AI Challenge at USAID, and other recently announced programs to leverage AI to help reduce poverty, address energy needs, improve global public health, access to education, and build a stronger coalition around inclusive and ethical AI governance. This affirmative vision must include a commitment to elevating the voices of those around the world who are often not included in the conversations around AI development, deployment, and the international standards governing AI. By committing resources to these programs, we were able to secure follow-on investments from the private sector that didn't just match but far exceeded our commitment of \$15 million to leverage AI to accelerate progress on the Sustainable Development Goals. The United States is the world's leader in innovation—if we don't champion the benefits of technology, who will?

Second, we know we must do this work in partnership with others. International partnerships on everything from R&D investment to standards harmonization to regulatory interoperability are the policy underpinnings necessary to seize this moment. No one can do this alone. Over the past year, the State Department has been engaged constantly with allies and partners bilaterally and in multilateral venues like the G7, the G20, the OECD, and the United Nations to achieve tangible commitments on the responsible development, deployment, and use of artificial intelligence. Through the AI Executive Order, the United States is leading by example, providing a model for the responsible use of this critical technology. We are working to increase participation in the AI Voluntary Commitments among leading companies in the United States and all around the world, to broaden adherence to the Code of Conduct, and to internationalize different elements of the E.O. as a more comprehensive policy framework. In addition to working the governments and companies, we—from the President on down—are working with civil society experts and organizations at every step on this journey to effectively manage risks related to AI technologies.

Third, we recognize that all this is happening while a determined and well-resourced set of adversaries and competitors tirelessly advance a very different view of technology's role in our future. They are aggressively trying to re-shape the international rules-based order and are investing heavily in a worldview that prioritizes authoritarian tactics over democratic values and governance. Technology governance, and specifically AI, is one of the geopolitical imperatives of our time. We need to lead international conversations to shape the global technology landscape of the future, so that AI advances democratic values and human rights, protects our safety and security, and supports consumers and workers. When the United States pulls back, our adversaries and competitors fill the void.

Technology with global impact requires global action, and the State Department is delivering on the important work of technology diplomacy for the American people.

Thank you again for the opportunity to join you today. I look forward to your questions and perspectives.

The CHAIRMAN. Thank you very much, Mr. Ambassador.  
Dr. Graviiss.

**STATEMENT OF DR. MATTHEW GRAVISS, CHIEF DATA AND ARTIFICIAL INTELLIGENCE OFFICER, UNITED STATES DEPARTMENT OF STATE, WASHINGTON, DC**

Dr. GRAVISS. Chairman Cardin, Ranking Member Risch, distinguished members of the committee, thank you for this opportunity.

I would like to echo Ambassador Fick's message that we appreciate the committee's effort to understand the role of artificial intelligence both at the Department and in our global diplomatic efforts.

Serving as the Department's first chief data and AI officer, I lead the Center for Analytics. Formally launched in 2020, the Center for

Analytics is innovating with, among other things, AI pilots while instilling a culture of responsible AI use across the Department.

To elevate our collective data and AI proficiency our stellar team of data scientists and engineers and analysts partner closely with dozens of bureaus, offices, and posts across the Department.

Our work delivers on the President's Executive Order on safe, secure, and trustworthy AI which emphasizes the transformative potential of AI in government. Just last week, the Secretary released the Department's first ever enterprise AI strategy.

This strategy will provide our world-class diplomatic corps with advanced AI governance and analytics, training and infrastructure to prepare them both for enduring and emerging policy challenges.

As Ambassador Fick noted, our technology leadership is stronger when we set a compelling example. With that, I would like to share four important insights from our journey thus far.

First, at State we see a booming demand for data and AI services across the Department. Over the past 3 years, the Center for Analytics has received over 350 project requests from all corners of the Department. Some of them promote foreign policy objectives while others bring about operational efficiencies.

Second, on the talent front we are positioning federal data science skills as close to the mission as possible. Our efforts range from hiring data scientists to offering extensive AI-related training for Department employees at all levels.

Third, we are already elevating our diplomacy and enhancing operational efficiencies. We are not starting from scratch. For example, by including a data scientist at COP-27 last year, the U.S. delegation had access to real-time modeling on other countries' proposed policy changes, which elevated our country's negotiation position.

As another example, one of our partner bureaus, the Bureau of Complex Stabilization Operations, employs computer vision to document war crimes in Ukraine using satellite imagery. In another area, the Bureau of International Organizational Affairs employs AI to better strategize our approach within the United Nations both in elections and votes resolutions.

These examples show how data and AI augment our diplomatic capabilities. We also use AI as a force multiplier to increase operational efficiencies. An example is the statutorily required declassification process.

Traditionally, a resource intensive manual task, the declassification process is now accelerated by machine learning, achieving over 97 percent accuracy and reducing human effort by 60 percent.

Last but not least, our AI advancements must rest on a firm foundation of sound and responsible policy and governance. To achieve this we formulated the Department's first AI policy, updated our AI use case inventory, and launched an AI toolkit.

We have also appointed a responsible AI official and initiated an AI steering committee to focus on upholding AI principles and federal guidance.

As AI continues to evolve, our commitment to responsible AI use remains unwavering. As we promote a vision of responsible AI globally, the Department must and will lead by example. Secretary

Blinken believes that our workforce is more equipped to lead globally when provided with timely, relevant data.

AI enhances this data's power, unlocking our workforce's utmost potential. We are committed to harnessing AI's potential and we are committed to doing it in a manner that is safe, secure, and trustworthy.

Thank you for your attention. I am eager to address your questions and collaborate on the promising future of responsible AI at the State Department.

[The prepared statement of Dr. Graviss follows:]

**Prepared Statement of Dr. Matthew Graviss**

Chairman Cardin, Ranking Member Risch, and distinguished Members of the Committee, thank you for the opportunity to speak with you today about the role of artificial intelligence (AI) in modernizing our diplomatic work around the world. I also want to recognize and thank the Committee for its interest and the work it is doing on this very important topic.

As the Department's first Chief Data & AI Officer, I lead the Office of Management Strategy & Solutions' Center for Analytics (CfA), which is spearheading efforts to use and scale responsible AI across the Department. The Center for Analytics is the Department's hub for data and applied AI, and we are leading in the implementation of the *Foundations for Evidence-Based Policymaking Act*, the new Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, and the *Advancing American AI Act*. Our stellar team of data scientists, engineers, and policy analysts provide support to bureaus, offices, and overseas posts on priority projects, while also working with partners across the Department—including the Foreign Service Institute and the Bureau of Global Talent Management—to increase our collective data and AI capacity. As Ambassador Fick mentioned, the work of my team promotes AI internally at the Department, while his work is largely externally facing and focused on the Department's engagement with the international community.

President Biden's recent Executive Order on Safe, Secure, and Trustworthy AI makes clear that "AI can help government deliver better results for the American people," and the State Department is no exception. Just last week, Secretary Blinken signed the State Department's Strategy for AI-Powered Diplomacy, an important milestone in support of the Department's Modernization Agenda. The AI Strategy is an essential step to equipping the Department's world-class diplomatic corps with the analytics, training, safe infrastructure, and effective policies to execute efficiently on enduring and emerging policy challenges. As my colleague Ambassador Fick pointed out, our leadership in technology foreign policy is stronger when we lead by example. That is why his office and my office work so closely together to share what we are learning and exchange information on future developments in AI technology at home and abroad.

It is an honor to be here today to share four key messages. First, our work responds to the high demand for data and AI needs from across all corners of the Department to meet foreign policy objectives. Second, we upskill and empower our workforce at all levels to deliver on behalf of the American people. Third, the Department has tested and proven approaches to turn data and responsible AI into insights and efficiency gains. Fourth, the Department is prioritizing the ethical and responsible deployment of AI to both seize its promise and manage its risks.

On the first, we witness every day how the demand for data and AI across the Department continues to grow. We have delivered AI and advanced analytics projects in collaboration with over 48 bureaus and offices, with the majority of projects directly supporting U.S. foreign policy objectives, and the rest focused on expanding the operational efficiency of the Department. The demand continues to grow. In the last 3 years, we've received over 350 requests for support, demonstrating the significant interest in modern data and AI solutions across the Department's components.

Second, through our workforce development initiatives, we are placing federal data science and AI expertise as close to the mission as possible. My office has led two Department-wide hiring initiatives for data scientists, hired bureau-level chief data officers, and created a standardized locally employed staff data scientist position to enable embassies and consulates worldwide to hire expertise easily and efficiently. Additionally, with a focus on broadening data analysis and AI skills, Department employees have taken 62,000 hours of related training, and our team has incorporated data modules into foreign service tradecraft courses and Chief of Mission

onboarding seminars. This success demonstrates the tremendous value of President Biden's National AI Talent Surge for increasing government AI capacity.

Third, Data and AI have already impacted American diplomacy by equipping the right people with the right insights at the right time to use information to provide advantages in international negotiations. The Special Presidential Envoy for Climate did exactly that last year at COP27, where the United States included a data scientist in its delegation. This decision allowed us to model the impact of other countries' proposed policy changes on environmental conditions in near-real time while negotiations were ongoing—helping us hold countries to account and push for ambitious commitments to achieve climate goals. Elsewhere, the Bureau of Conflict and Stabilization Operations uses computer vision and machine learning to document war crimes in Ukraine through commercial satellite imagery; and the Bureau of International Organization Affairs analyzes votes in the United Nations to better target our resolution and election priorities. In these and many other examples, data analytics and AI are strengthening the capabilities of our world-class diplomatic corps.

But we're doing more than providing a decision advantage to U.S. foreign policy practitioners; AI and data analytics are also making the Department more efficient: for decades, the statutorily required declassification process has been entirely manual, requiring thousands of staff-hours and millions of dollars to execute. We and our partners in the Bureau of Administration developed a machine learning platform to accelerate this process by predictively marking cables for declassification, continued classification, or further human review. In our testing, the model has been over 97 percent accurate and over 60 percent faster than manual review alone—even accounting for the time needed for human oversight. As we continue to put this model to use, we are seeing the error rate improve even more. In addition to saving thousands of staff-hours per year, this approach also safeguards national security information from erroneous public disclosure. With this solution, we are able to review every cable by statutory deadline, as by statute, documents that are not reviewed on time are automatically declassified.

Fourth, none of these burden reducing or foreign policy gains would be possible without good data quality and responsible and trustworthy AI policy and guidelines. In the past year, the Department has published the first AI policy, updated its AI use case inventory, and established a Responsible AI toolkit. We have also appointed a Responsible AI Official and launched an AI Steering Committee, the Department's governance body charged with advancing responsible AI principles and ensuring adherence to federal AI guidance. As we continue to take advantage of opportunities to leverage the power of AI and the technology evolves, we will actively learn from our experiences and that of our partners and outside experts to refine our policies and ensure we have appropriate protections in place for its use in the Department.

As the United States promotes a vision of responsible AI around the world, we believe the Department must lead by example in leveraging AI responsibly in our own work. As Secretary Blinken has said, our workforce is "better prepared to engage diplomatically, manage effectively, and lead globally" when it has the data it needs when it needs it. AI and advanced analytics enhance the power of data and accelerate our workforce's potential. We are absolutely committed to pursuing U.S. foreign policy and operational advantages at scale in a safe, secure, and trustworthy way.

Thank you very much for inviting me here today. I look forward to answering your questions and to working with you to realize the vast potential of responsible AI.

The CHAIRMAN. Well, thank you again, both of you, for your testimony. We will go through 5-minute rounds.

Mr. Ambassador, you pointed out that America is the leader in innovation and technology and we accept that, but I do not want to be naive about it, and Dr. Graviss, you are talking about how you are implementing it in our own use in our Department.

We have seen this before. We have led in technology development only to see the autocratic regimes that do not play by the same rules that we do, try to steal our information, and although we will proceed with—both on cyber and on AI within our values, our adversaries do not share that commitment to our values.



There are lots of tools in our toolkit—executive orders that you have already mentioned and the executive orders and treaties. I am just interested as to how you see these standards being developed.

You talked about voluntary standards by what we do. That works up to a point, but we know that the PRC is not going to be as nice as we are in the protocols and adhering to standards.

Where do we go as far as establishing international guardrails? Are we looking at just America leading through example or are we looking at more enforceable ways to establish international guardrails?

Mr. FICK. Thank you, Senator.

Let me share a perspective on that and try to highlight a handful of things.

First, we started with the voluntary commitments for two reasons. First, voluntary by definition on the part of the companies does not constrain innovation and, again, we are in a race with our geopolitical adversaries and we cannot afford to hamstring our innovative competitive advantage.

Voluntary equals innovation. Voluntary also equals speed. The voluntary commitments are not intended to be the last step in our domestic or our international governance structure.

They are a first step and they do a couple of things. They allow us to build international consensus around a fairly robust set of commitments on AI safety, security, and trust. Safety means ensuring that the models do not return the most dangerous results.

Security means ensuring the cybersecurity and other integrity of the models themselves, and trust means helping to ensure that users, the consumer, can distinguish between AI-generated content and not AI-generated content.

The CHAIRMAN. That is fine for our allies that we have a relationship with, but the autocratic competitors we have, whether it be the PRC, whether it be Russia, whether it be North Korea, they are not following those guidelines.

What protections are you negotiating that will provide either incentives or disincentives for those who want to violate international protocols?

Mr. FICK. Yes. I will give you three things.

First, when you are running a race sometimes it is important to simply run faster than your competitor so that is our innovation prioritization. Speed is one answer to your question.

A second is trying to constrain adversaries who have a wildly different view of the role of technology in our future via mechanisms like export controls on our most advanced semiconductors.

That is a small yard high fence approach in order to help keep the most capable enabling technology of AI out of the hands of our adversaries.

Then third, is a robust global engagement to shape the norms of responsible state behavior in these critical technology areas so that our adversaries can either abide by those norms or put themselves and their behavior outside the norms.

We are under no naive illusion that our adversaries are going to comply with our norms, but building a broad coalition, setting the normative example at least puts our adversaries outside that

framework so then we have the legitimacy and the moral authority to call them out on it.

The CHAIRMAN. I would just point out we have gone through a series of congressional actions encouraging administrations, sometimes requiring administrations to take affirmative action against bad players internationally.

We call them sanctions. We call them other issues. That is pretty direct when we are dealing with specific actions that are being taken—kinetic actions.

It may not be as easy to determine with the use of AI tools, but if an adversary is not identifying the source or using it for disinformation that undermines America's national security, we are going to have to have more direction on how we can assist or we may have to try to do that on our own.

Any help that you can give us as to how America can not only lead in the race—we want to be first in the race—but to prevent adversaries from taking us in the wrong direction or stealing our information.

With that, let me turn it over to Senator Risch.

Senator RISCH. Thank you, Mr. Chairman.

I am going to follow along the same lines the chairman did, and that is if you think back probably some decades ago, some congressional committee was holding a hearing just like this saying, what are we going to do about this new thing called the internets, as George Bush called it. How are we going to police it? How are we going to—because it has tremendous possibility, but there is evilness that that can arise from the use of it, et cetera.

Frankly, after listening to you I suspect probably we are in no different position here and that is whenever you talk about voluntary, anybody here think that China or Russia are going to voluntarily comply with any international norms when they think it is in their best interest to do otherwise?

You got a country like Russia that cannot even obey the simplest mandate of the United Nations; not to abuse one of your neighbors.

China, look at them as to what they do with international norms—international norms or as we call them, on technology and patent protection of those kinds of things.

It is just stunning that they have no boundaries. They are—it is just the Wild West out there.

I guess, Ambassador and Dr. Graviss, if you would comment for a minute on are we right that we are probably barking up the wrong tree? We talk in these esoteric terms about voluntariness and goodness and kindness. Are we in the same place with this as we are going to—as we have found ourself with the internet?

Why do you not start, Ambassador?

Mr. FICK. Thanks, Senator. Just one point of clarification. The voluntary commitments are voluntary on the part of the companies. These are the leading AI developers in the world subscribing to these commitments and committing their companies to the responsible development of AI.

Senator RISCH. I am assuming that you are going to want that to flow over to—

Mr. FICK. We want international—We want businesses around the world to support the commitments and then we want the com-

mitments to become the basis of codes and frameworks for governments, and we are—please understand we are not naive about whether our adversaries will voluntarily comply.

I think we need to confront an uncomfortable reality in the software era, which is that controlling access to these technologies is somewhere between very difficult and impossible.

If an isolated and impoverished North Korea under strong sanction could develop nuclear weapons, I would suggest that the development of sophisticated software capability is a lot easier than that.

Senator RISCH. Good point.

Mr. FICK. Unfortunately, I do come back to our greatest source of strength being maintaining our innovative advantage, running faster, stewarding our competitive innovation ecosystem, putting export controls and other sanctions in place on adversaries where we think it can be effective and trying to shape the global normative framework governing these technologies.

Senator RISCH. I appreciate that.

Mr. FICK. Thank you.

Senator RISCH. Dr. Graviss, maybe you could take a crack at what the AI police are going to look like.

Dr. GRAVISS. I can speak to what we are doing within the State Department. That is my remit is focusing on internal, so I will stick with that.

Senator RISCH. Fair disclaimer.

Dr. GRAVISS. Just to point out we have the ability to set policy and we have the ability to set policy quickly within the Department and that is the first element.

We have already established an AI policy. We brought on board a responsible AI official whose job is to be laser-focused on the ethical and responsible use of AI. She has brought on a test and evaluation team—a Red Teamer. She has got these kind of capabilities on her team to provide independent assessments, independent evaluations of AI that we onboard in the Department. We have that policy lens and then we also have that independent look that we are focused on and we balance that with the opportunities.

There is a lot of repetitive work that is done all over the world by our diplomats. We have to move swiftly and we have to move smartly.

Senator RISCH. Thank you. I guess it is going to be interesting to see how this develops because I suspect that when the internet started, probably people were a lot more optimistic that that there was going to be compliance and you would not have sovereigns actually and intentionally interfering with other people's elections as they do today. It will be interesting to see how this develops.

Unfortunately, like I said, where you cannot get countries to behave themselves in public, how you are going to get them to behave themselves in a laboratory with the door closed and locked and nobody looking?

It will be interesting to see how that develops and I have no doubt that you will follow it closely.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator Risch.

Let me just caution—we will be patient to wait for your recommendations as to how we can protect those that are not following guardrails, but the next person I am going to call on, if it was not for his action in regards to Iran, we may still be waiting for some executive actions.

Senator Menendez.

Senator MENENDEZ. Thank you, Mr. Chairman.

President Biden and Chinese President Xi Jinping are set to meet today during the APEC summit to discuss a number of issues including the role of artificial intelligence in nuclear weapons.

When I think about this topic, I worry that some country would give the decision as to whether or not to launch a nuclear weapon to artificial intelligence, thinking that it may be the most astute way to make a calculus.

For me, that would be alarming. There have been press reports that the United States and the PRC will pledge to limit the use of AI in nuclear weapons systems.

Ambassador Fick, can you share with us why an agreement on these issues with a country like China is significant? Is this a model that the Administration plans to expand to other willing countries?

Mr. FICK. Thank you, Senator.

I am serving at the State Department in part because of my formative experience in the Marines in my twenties, which left me with a conviction that diplomacy is and must always be the nation's tool of first resort and so I welcome the conversation between Presidents Biden and Xi.

I welcome communication between us and all countries at all times. That does not mean we agree. It does not equal collaboration, but the communication in and of itself is valuable and is better than the alternative.

With respect to the military uses of AI, I would point to the political declaration for the responsible use of AI, a military focused framework of principles that rights-respecting countries have subscribed to.

It is a good example of the kinds of behaviors that we want to become the global norm. Again, we are under no illusion that our adversaries will abide by those norms in every case, but I think that the channel of communication in itself is valuable.

Senator MENENDEZ. I have no doubt about the communications. I agree with you totally. I have been advocating for that so that we have lines of communication, particularly for nonconflict issues in China.

My question is really going to, do we want to extend an understanding and agreement as to how or whether or not even AI should be used at all particularly in terms of nuclear launches, as well as how do we ensure—because China is growing their nuclear capabilities dramatically—how do we ensure that even if a country signs on to that how is it—have we thought about the enforcement mechanisms of that?

Mr. FICK. I think one of the foundational principles of the political declaration is a belief that when we are talking about lethal systems of any kind, there needs to be a human in the loop.

We cannot have fully machine-enabled or AI-enabled lethal systems. Your question about the inspection mechanism and the enforcement mechanism is, of course, exactly the right one.

I would have to refer to colleagues elsewhere in the Department who have that piece within their remit.

Senator MENENDEZ. All right. China has introduced some of the earliest and most detailed regulations governing artificial intelligence over the last 2 years. Our own allies, including the European Union, have also begun cooperating on developing regimes to govern the proliferation of AI.

While I applaud these engagements on global AI governance, more must be done in this area of strategic competition if we are to keep up with China's efforts to regulate AI and provide an alternate vision for AI that embraces human rights, privacy, and other values we hold so dear.

What are some of the troubling implications if America and our allies fail to develop a consensus around regulating AI and we allow China to pioneer the rules of AI globally?

Mr. FICK. I would make two points there in response to your question, Senator.

First, our foreign policy in any area will rarely be any stronger than our domestic policy in that area. American foreign policy—I think the foreign policy in any transparent democratic society is a reflection of what we do at home, and so we do need to get our own house in order with respect to the regulation and governance of these emerging technologies so that we are presenting on the world stage a responsible framework for governance that has legitimacy and moral authority.

Second, there is no room here for one of the concepts that even our closest European allies advocate, which is digital sovereignty. I would argue we need to think about digital solidarity. We have to think about close collaboration with our closest allies and partners to coordinate R&D investment, to coordinate regulatory interoperability.

Companies want large harmonized markets. We need the combined integrated efforts of our best universities, of our students and workers. It points to the importance of our domestic regulatory regime. It also points to the importance of our allies and partnerships in order to both shape the international normative environment and also present the strongest unified front against the PRC model.

Senator MENENDEZ. Mr. Chairman, if I may.

I am going to just submit a question for the record since my time has expired, but I would like really a responsive answer to it. This is the 10th anniversary of the Rana Plaza factory collapse in Bangladesh. Took the lives of over 1,000 workers.

In this AI industry, workers are being exploited, paid as little as \$1 an hour, going through the repetitive process of trying to determine what is a smile, what is a frown, to inform the algorithms, and I would like to see us lead in this regard to make sure that we do not have worker exploitation globally in the development of AI. I would like to see what the Department is doing with that.

Thank you, Mr. Chairman.

The CHAIRMAN. I would be interested in that answer also. As I mentioned, we need to lead by our values.

Senator Ricketts.

Senator RICKETTS. Thank you, Mr. Chairman, and thank you to our witnesses here today.

Ambassador Fick, I want to build on what Senator Menendez was talking about with regard to the EU specifically.

Obviously, we have talked about the different sorts of regimes—regulatory regimes that different countries around the world are trying to establish. We talked about the PRC. We have talked about what we have done with regard to the Executive Order and the voluntary guidelines you talked about.

Then, of course, we got the European Union where they have been working on their own legislation. They proposed the *AI Act* a couple of years ago and it involves a risk-based approach.

As you know, the European Union will often come up with these standards and then companies will really adopt those for their worldwide products to try and standardize their products and make it easier to have access both to the market in Europe and around the world.

If you have—I understand the legislation is coming to its final phases. They have not figured out the generative AI part of it. Assuming that gets passed, companies will be forced to make a decision of either complying with what the EU does or creating completely different algorithms that do not have access to EU data and then having to deal with the difficulties of that as well.

My question really gets to if we have got these EU regulatory constraints—you talked about cooperating with our allies, but they are moving forward on this legislation. I think you have been critical of this legislation. What effect if the EU passes their *AI Act* will that have on the United States and our other allies and is this going to potentially put a damper on that innovation you have talked about that is so important among U.S. companies?

Mr. FICK. Thank you, Senator. Yes, we have been in regular dialogue with our EU counterparts, both member states and the European Commission, on the substance of the *AI Act*.

I would make three points on this. The first is speed. As you pointed out, the Act was first drafted before ChatGPT was released a year ago and so in some sense it has already been overtaken by events, which points to—

Senator RICKETTS. It is already obsolete, essentially.

Mr. FICK. —a structural challenge with that kind of regulatory approach. It also as currently drafted would hinder law enforcement cooperation between the United States and the EU, things like the use of facial recognition technology at borders or by law enforcement.

Third, we hear repeatedly from companies and innovators not only in the United States, but also in Europe that is not adequately protective of intellectual property.

It would deter entrepreneurs from building AI businesses in Europe. Back to this point on digital solidarity, the future that I think we think positions us most strongly for competition with our adversaries, is one where we have globe-spanning technology businesses being built not only in the United States, but also in our closest and rights-respecting allies and partners in Europe and in Asia.

Senator RICKETTS. For all those reasons you just talked about, how we want to be working with our allies in Europe, and yet they are pushing forward with this, frankly, it is already obsolete now or at least it is not complete legislation, what is the State Department doing to get them to maybe to slow this down, to be able to work with us more carefully, to create that regime you are talking about where we can be on the same team with regard to pushing back against the People's Republic of China and not creating an obstacle to us working together to oppose them?

Mr. FICK. We are pushing in every form on this, multilaterally and bilaterally. I will give you three examples.

Over the last 3 weeks, I met with the German communications minister who has oversight of these policies in Germany when he was here in Washington. He was at Bletchley Park. Most of our EU counterparts were there and last week I was in France with President Macron himself and the French digital minister making exactly these cases, that the continental Europe in a lot of ways regulated itself out of the cloud services era of technology.

It is no accident that the five largest global cloud services businesses are here in the United States. It would be to our mutual detriment if the EU were to regulate its way out of the AI era of technology innovation. We are pushing on this in every form.

Senator RICKETTS. Okay. Then you just said you were at Bletchley Park. How are the Brits seeing this? What is the U.K. policy going to be and where are they going? Are they more leaning toward the European model or are they leaning more toward our model?

Mr. FICK. Prime Minister Sunak and his government are leaning very strongly toward our model. I think we and our British allies are very close on this. They intend to set themselves up as an AI superpower, in their words, which we view as very much to our benefit as well.

Senator RICKETTS. Great. Thank you very much. Thank you, Ambassador.

Mr. Chairman, thanks.

The CHAIRMAN. Thank you.

Senator Shaheen.

Senator SHAHEEN. Thank you both for being here.

Ambassador Fick, in your opening statement—and you mentioned an alphabet soup of multilateral organizations that we were looking at—you did not mention NATO, and while I recognize that NATO is not technically part of the State Department or within the purview of the State Department, certainly what they do is very important.

Was there a reason and what are you looking at with respect to NATO?

Mr. FICK. Senator Shaheen, I joke with my wife sometimes that we should get an apartment in Brussels because I am at NATO so much, especially in the context of the war in Ukraine in the past year.

Our ambassador to NATO, Julianne Smith, is a dear friend and we collaborate very closely on these topics. I think that NATO is a terrific example of what Secretary Blinken talks about as vari-

able geometry and making sure that our most important alliances historically are fit for purpose in the technology age.

A really key element of our diplomacy with NATO and in Europe has been ensuring that the alliance is equipped on all of these technology topics. Cybersecurity, at the Vilnius summit in July, we saw a robust set of deliverables on the virtual cyber incident support capability, the revitalization of the NATO cyber defense pledge.

We have been working with allies across the alliance to ensure that their own architecture and infrastructure is secure and trusted so that we can share information and intelligence freely across the alliance.

That was not an error of commission in not mentioning NATO in my opening comments. I think in technology, the NATO alliance is one of our leading partners globally on all of these topics. Thank you.

Senator SHAHEEN. Good. Thank you.

As everybody has talked about so far, AI has tremendous potential in so many areas, but it can also perpetuate existing biases and inequities. How does the Department look at how we ensure that those inequities are not part of whatever is done through AI, particularly with respect to gender or with respect to the whole range of ethnic racial differences that we want to respect?

Dr. GRAVISS. Thank you, Senator, for the question. I will make a few points here.

One is it starts with training, leveling up the literacy when it comes to data, when it comes to AI, when it comes to algorithms across the Department. We understand that this is a possibility.

The second is using good data. Good AI rides on good data, at the end of the day, and so the focus of ours is to how do we bring this kind of technology into our Department in a secure infrastructure and apply this technology on data that we manage, data that we can ensure the quality of. That is the second point.

The third has to do with our partnership with industry, which is really focused on the procurement process—how do we ensure that software procurement includes the right policies and requirements to make sure that our industry partners are providing technologies that are free of those types of biases you mentioned.

Senator SHAHEEN. Great. I want to be a little more parochial now. In my office, the number-one constituent issue we hear from people about are visas, passports, challenges with our immigration system. Yes. The State Department particularly during COVID had some real issues in countries around the world in terms of processing those kinds of issues.

Tell me how AI is going to help us make sure we can process those kinds of constituent concerns faster so that we can provide service to people who need it.

Dr. GRAVISS. Passport—the passport organization within Consular Affairs is not using artificial intelligence at this time.

Senator SHAHEEN. I know they are in New Hampshire or at least one of them is. We are very aware of that.

Dr. GRAVISS. We will make that point first.

More broadly, we see this as a real opportunity to reduce the type of repetitive rote work that happens across the Department, both domestically and overseas. We are taking a very pilot-centric



approach, starting small, learning a lot, scaling where it works and we have seen some real success with that approach.

Senator SHAHEEN. Assuming that you continue to see success, what do you need in order to ramp that up? Do you need resources? Do you need more people? Do you just need the IP to share those with our embassies around the world?

Dr. GRAVISS. I am a systems engineer, so what goes in can increase the output. In my mind it is resources in terms of infrastructure and in terms of personnel.

It is the people without the actual technology, without the data to be able to employ it are not going to get very far in technology without the skilled workforce that we are currently aggressively trying to bring into the federal employment within the State Department. You got to have both.

Senator SHAHEEN. Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. I assure you Senator Shaheen has the support of every member of this committee on consular services to be streamlined and made more timely. It would make our life a lot easier. I assure you of that.

Senator BARRASSO.

Senator BARRASSO. Thanks, Mr. Chairman.

For either you who want to address this, I have with me today the principal and a number of teachers who are here from the Southside Elementary School, Powell, Wyoming. They are a Blue Ribbon school, one of only two in the state of Wyoming, and they are here for the national celebration of their achievements and this has to do with AI, TikTok. Whoever you want to—whichever wants to answer it, because reports do indicate this—the TikTok is harvesting vast amounts of data from millions of users in the United States, many of whom are students.

It is owned by a company based in Beijing. Although TikTok executives deny it, many experts believe that the Chinese Government has access to TikTok's American user data.

The question is do you believe that TikTok is using data collected from its application to feed Chinese artificial intelligence, the machine learning algorithms and what the implications are for us here at home and for students all around the country?

Mr. FICK. Thanks, Senator. A couple of couple of points on that.

I would point out, of course, that the Administration has enacted a ban on the installation of TikTok on federal devices, which should speak to, I think, our perspective on the risk involved.

The second observation, I am probably the least popular father in my daughter's middle school because of my personal views on this point and my request to you would be that we try to speak with one voice as a country, that we adopt a position via a democratic process that acknowledges what you have said.

Senator BARRASSO. Anything you would like to add on that?

Dr. GRAVISS. Thank you, Senator. I would say we are worried about our data, too, at the State Department. How do we ensure that that our employees are not putting sensitive information out on the web?

We have existing policies in place that need to be reinforced and training and literacy has to go along with that, and then we need to move aggressively to onboard this kind of technology into the in-

frastructure that we micromanage, that we have tight security controls on and that we are constantly monitoring.

Senator BARRASSO. Thank you.

Mr. Fick, China continues to infiltrate top U.S. companies, laboratories, universities to I believe steal valuable American intellectual property. The impact on the economy is massive, the Chinese Communist Party clearly attempting to surpass America in terms of our economic strength, military strength, international influence.

A senior FBI official had said earlier this year, nation-state adversaries, particularly China, pose a significant threat to American companies and national security by stealing our AI technology and data to advance their own AI programs and enable foreign influence campaigns.

How do you assess the threat of China's increasingly adversarial government to the United States?

Mr. FICK. Senator, I certainly agree with that assessment, that intellectual property theft by the PRC has stripped critical, competitive advantage out of the U.S. economy for several decades now.

Our response to that or uneven response to that has put us in a deterrent hole and there is a very real threat to the security of our most advanced AI systems, going forward.

It is why one of the pillars in the voluntary commitments is the security pillar, which is standards around cybersecurity, testing, disclosure of testing results for our most advanced frontier models and a very real shared focus by the government and these companies on safeguarding that aspect of our innovative advantage.

Senator BARRASSO. Then a final question, since Senator Risch started by talking about the leadership that we have taken in the United States when it came to the internet years and years ago, we led in this sector because we chose to take a kind of a light-handed regulatory approach.

A number of us in the Senate have met with—we have had discussions on AI with Elon Musk, Mark Zuckerberg, a number of the leaders in the technology there.

Do you believe that a light-handed regulatory structure or a heavy-handed structure, if you will, is best for promoting American leadership and innovation in artificial intelligence and machine learning technology?

Mr. FICK. Senator, I have been in this job for a year, but I spent a dozen years before that building a software business and investing in software businesses, and I believe very strongly in the power of our innovation economy as our greatest source of national strength.

I said in my opening statement that many traditional measures of strength like GDP and military capacity are increasingly downstream of our ability to innovate in these technologies.

I do think there is a role for appropriate regulation of such powerful tech and I think our North Star must be maintaining the health of that innovation economy.

Senator BARRASSO. Thank you, Mr. Chairman.

The CHAIRMAN. Senator Barrasso, thank you for bringing the students here today. I think the students should know that Senator Barrasso is one of our leaders in the United States Senate, but his

role here on the Senate Foreign Relations Committee is invaluable. He is a great member of our committee.

As Dr. Graviss has said, there is a career at the State Department in AI, so applications will be given out shortly.

Thank you for being here. We appreciate it very much.

Senator Van Hollen.

Senator VAN HOLLEN. Thank you, Mr. Chairman. Thank both of you for your testimony and for your service, and I know we have covered a lot of ground today, including some of the questions that I was going to ask.

I just want to affirm a couple of principles, Ambassador Fick, that I know you have outlined not just this morning, but earlier, which is in order—that part of our overall digital and data strategy has to be to promote American innovation, support American values including promoting human rights. Would you agree?

Mr. FICK. Yes.

Senator VAN HOLLEN. You would agree, I think, that authoritarian regimes fear the open flow of information and data and try to put up walls and barriers against it, right?

Mr. FICK. I agree.

Senator VAN HOLLEN. Would you agree that one of the mechanisms they use to do it is to try to promote data localization requirements around the world so that those governments can sometimes spy on their people and look for dissenters?

Mr. FICK. We see an increasing balkanization of the free and open internet.

Senator VAN HOLLEN. Here is my question, because we have a unified executive branch. Were you consulted when the USTR decided to back away from the e-commerce principles at the WTO? Were you consulted as part of that decision?

Mr. FICK. I read about the decision in the press, Senator.

Senator VAN HOLLEN. I know what your earlier testimony—one of the things that struck me when you were up for your nomination was that you were a straight shooter.

Would you agree that that decision undermines the principles you and I just discussed about an open internet and not allowing authoritarian regimes to more easily spy and crackdown on dissent?

Mr. FICK. We advocate in every forum for the benefits of an internet that is free and open and interoperable and reliable and secure and that includes the free flow of data.

Senator VAN HOLLEN. I appreciate that, and I understand that you are here not just as a State Department representative, but part of an administration.

I appreciate that answer because I can tell you that, in my view, that what the USTR did at the WTO was—totally undermined the principles that we just talked about—free flow of information, stepping back from our resistance to data localization, which empowers authoritarian regimes, as well as our efforts to prevent forced tech transfer.

Those were all principles that we advocated for and it is my belief that when we back away from that, we lose our credibility around the world, not just on these issues, but on the issues that you two gentlemen have to work on every day.

Mr. Chairman, I would just like to submit for the record a letter that a group of us wrote to President Biden on this issue.

The CHAIRMAN. Without objection.

[EDITOR'S NOTE.—The information referred to above can be found in the "Additional Material Submitted for the Record" section at the end of this hearing.]

Senator VAN HOLLEN. Thank you.

On the issue of AI, of course, one of the big issues is, and I think it has been discussed a little bit already this morning, the issue of international standard-setting committees, and there are many, but there are a number of key ones.

How would you evaluate the current U.S. presence, participation, influence in those committees, and I would start with Ambassador Fick and then hear from Dr. Graviss.

Mr. FICK. May I just ask for clarification on which committees, Senator? Which organizations?

Senator VAN HOLLEN. Yes, there is the international standard-setting committee being one of them. There is one on electrical standards. Those are—

Mr. FICK. Okay. Yes, I understand.

Standards harmonization is one of the foundational pieces of building an innovation ecosystem across national boundaries that can bring to bear shared R&D, shared innovation, more than the companies of any one business. We are strongly engaged in those international standard-setting bodies to help ensure that the standards are aligned with our values, that promote shared prosperity, and that they—looking ahead now to the AI era that we adopt a similarly legitimate, broadly consensus-based approach to harmonizing standards.

Senator VAN HOLLEN. I appreciate that. I think the major ones for the purposes of AI, I think, are ISO, the IEC and the ITU, but there may be others and I think—as you know, the PRC and others have been very actively engaged in trying to increase their presence and participation. It has been one of America's strengths that we have led that effort and I know you both are committed to doing that.

I do not know, Dr. Graviss, if you had anything to add to that question.

Dr. GRAVISS. Sure. Happy to. A couple of things, Senator.

First is within the Federal Government, starts with the National Institute of Standards and Technologies. That is the—who is setting the guardrails around what standards are expected to be followed across the Federal Government. Also on the cybersecurity side, Cyber Infrastructure Security Agency within DHS.

At the State Department, as I just said, AI rides on good data. We have been doing data standards for the last several years. It is not the flashiest part of the work, but it is necessary and I think it is great that you are talking about that.

Also, I will point out that the International Organizations—Organizational Affairs Bureau—IO Bureau within the State Department has their own chief data officer. It is part of a program that we have been leading to place data leaders in each bureau and she is focused on analytics related to elections try to get Americans in

the right committees who are setting these kind of standards and that is really important, too.

That is a great example of how we apply technology, how do we apply AI in the Department to impact on a global stage diplomatically.

Senator VAN HOLLEN. Thank you. Thank you, Mr. Chair.

The CHAIRMAN. I just want to comment briefly in introducing Senator Kaine—make it clear, Mr. Ambassador, we strongly support diplomacy in dealing with these issues. Our questions are really aimed to seeing how we can make sure you have the resources, the tools, and then sometimes the direction you need for diplomacy to be successful.

We are very fortunate on this committee to have our own ambassador to the Department of Defense. Let me explain that. Senator Kaine serves on this committee and the Armed Services Committee, so we have our representative with DoD to promote diplomacy.

Senator Kaine.

Senator KAINE. Mr. Chairman, you anticipated my line of questioning because what I want to talk about is something that is at the intersection of the Foreign Relations Committee jurisdiction and the Armed Services Committee jurisdiction and that is the AUKUS partnership.

President Biden announced the AUKUS partnership with the—Australia and the U.K. a couple years back. It has been fleshed out. Last summer, the Administration came to us to ask for enabling legislation to move the partnership forward.

They thought it was going to be in the Armed Services Committee, but when I told them, no, all this comes through the Foreign Relations Committee, they said, well, good—you are on both, can you help out? Senator Cardin has been key to this as well.

The partnership has two pillars. The first pillar is the construction over a period of about 25 years of nuclear subs that would be Australian-operated and eventually Australian-built to provide additional stability in the Indo-Pacific.

Just for my colleagues, I was at a Navy-funded workforce training school in Danville, Virginia, on Monday that the Navy has stood up to build out the submarine industrial base.

Their 60 students go through in five different curriculum areas for an 8-week program and students and—multiple students in each of the five programs were from Australia.

They were not only from all over the United States, but Aussies are already training to be part of the sub industrial base and Aussie sailors are now part of the Nuclear Power School that the Navy operates in South Carolina.

Even though the first subs are not going to be purchased until the 2030s or built in Australia until the 2040s, we are integrating.

The second piece of AUKUS is pillar two, which is innovative technologies, quantum undersea capabilities, but also AI, and I would like to ask your own impressions about what we can do together with Australia and the U.K. in the pillar two space to really maximize the synergies of us working together on AI capacity that can help us in the defense of the INDOPACOM.

Mr. FICK. Thank you, Senator. Happy to address that.

I think that my overarching view here is maybe reflected in the way Senator Blinken talks about alliances and partnerships that are fit for purpose, the variable geometry of our alliances and our partnerships, and pulling on the right partners in the right fora at the right time to accomplish our highest priorities.

This is a good example. Specifically, in the innovative technology pillar for AUKUS. I will point to one thing that we announced just a few weeks ago during the Australian Prime Minister's visit—I have been working closely with Ambassador Kennedy on this for months. That is a partnership on undersea cables connecting Pacific Island countries and what is interesting here—I wish Senator Shaheen was still here because one of the world's leading manufacturers of undersea cables is in New Hampshire, and so we have a national champion in the United States in this regard.

We have an opportunity now to lay trusted cable to connect Australia and the United States, but also to link together other key strategic geographies in the Pacific and do it in a way that is part of a vertically integrated technology stack. Let me just explain for a moment what I mean.

The cables as the baseline connectivity—those cables are essential for the data backhaul if we were eventually to build data centers, say, in Australia so that key countries across the Pacific could migrate their government enterprise to the cloud, could ensure continuity of communication and continuity of operations in the event of a contingency scenario, and then put top-notch, cutting-edge cybersecurity on top of those data centers.

Again, a layered approach of trusted cables, trusted data centers, and advanced cybersecurity. That is what we are in the early stages of doing in partnership with Australia and others in the region.

I think it is really exciting and it is a template that we ought to be able to replicate now in other geographies.

Senator KAINE. My colleagues asked questions earlier that you—that led you to talk about some of the different approaches that the EU is taking, for example, compared to the United States and the hope that the U.K. would be more aligned with the U.S. in terms of AI regulation, less centralized possibly.

My hope would be that as we are having those discussions with the U.K., we also keep Australia in mind because I think if we are going to make this pillar two part of AUKUS successful, the greatest alignment between the U.S. and U.K. and Australia on matters like AI regulation would be helpful.

I hope we might be able to convince the EU to come more of our way as well, but if you have any thoughts about the Australian approach to AI regulation, I would love to hear them, but at least I would like to encourage that we include Australia in the discussions that we are having with the U.K. around alignment.

Mr. FICK. I agree completely, Senator. I was at Bletchley Park for the U.K. AI safety summit a couple weeks ago. At the end of the summit, we released the Bletchley communique. Australia is a signatory there and so I think we are fully aligned.

Senator KAINE. Great. Thank you, Mr. Chair.

The CHAIRMAN. Senator Young.

Senator YOUNG. Well, thank you, Chairman, for holding this very important hearing. I thank our witnesses for your service. This is such an important topic we are all dealing with in various ways.

I will dive right in. Ambassador Fick, I have a number of questions for you. I ask that you keep your responses as tight as possible so we can get through them.

As we think about harmonizing AI policies and R&D between partners and allies, can you speak, Ambassador, to the importance of forging clear and enforceable digital trade rules that will ensure the regulated flow of data across international boundaries that may enable future AI and machine learning systems and which have to entail necessary cross border privacy protections?

There is a possibility that a failure to reach these sorts of rules and agreement on the rules may jeopardize AI collaboration and cooperation.

Ambassador, do you believe it would be to America's advantage to prioritize digital trade in our multilateral and bilateral trade negotiations? Not a trick question.

Mr. FICK. Thanks, Senator. I was at Purdue a few weeks ago in Indiana and let me let me just say that Keith Krach, who has endowed a center for tech diplomacy at Purdue, in many ways was my predecessor with his portfolio and put the markers down on some essential topics and we have tried to carry that work forward.

Yes. In a word, I think that harmonizing data flows and prioritizing digital trade in our international trade agenda is an important component of American competitiveness in the 21st century.

Senator YOUNG. How do we get there?

Mr. FICK. Through a series of bilateral/multilateral negotiations that result in outcomes like the U.S.-EU data privacy framework. There is no silver bullet here. I think it is a lot of hard-fought diplomacy bilaterally and multilaterally.

Senator YOUNG. I agree with you, and I know others in the Administration agree with that perspective as well because trade is—at once it is a vehicle for upward mobility for prosperity, but also for forging tighter relationships among countries and regions and I think it is very important that everyone in the Administration regard it as such.

We will continue to work on the Finance Committee and the Foreign Relations Committee on the topic of digital trade.

Ambassador, can you speak to how your bureau is approaching the use of artificial intelligence in converging technologies like synthetic biology, especially in gene synthesis and gene editing, as you promote the responsible adoption of artificial intelligence?

Mr. FICK. I think the simplest answer to that question, Senator, is that we have seen the PRC run what we now call the Huawei playbook in telecom. It is a series of—has a series of elements—IP theft, subsidies.

That playbook—that rough template is now being run by the PRC across a whole host of other emerging technologies including synthetic biology.

Senator YOUNG. All right. Thank you.

There is much congressional discussion, Ambassador, around the regulation of artificial intelligence. As the chairman was kind to ac-

knowledge earlier, I have been pretty involved in many of those conversations and much of what we discussed has centered on whether we can use existing statutes and regulations for specific use cases of artificial intelligence.

I think this is probably the approach our country will take on a going forward basis, but the same sort of debate about how conceptually you approach AI regulation extends to the global harmonization of policies across countries, across regions.

There have been countless forums already, and I think that is a good thing, to discuss artificial intelligence from the G-7 to the EU to a recent conclave on safety as it pertains to frontier models that was in the U.K., and making sense of how our country is going to approach harmonization can sometimes be complicated and confusing.

From your vantage point, Ambassador, how is the Department approaching this question of global harmonization? Is the intention to pursue action through existing multilateral institutions or instead to convene special multilateral conventions or pursue bilateral agreements?

Then, in any harmonization effort, what role do you envision the U.S. private sector actors are going to play?

Mr. FICK. Thanks, Senator. Yes, just in the last 10 days we have seen four strands come together. We have seen the AI code of conduct for developers at the G-7, the American executive order, the Bletchley convening and communiqué, and the *AI Act*—the EU *AI Act* in trilogue negotiation.

We have this dynamic policy landscape and our overarching next step is to try to drive these to convergence in some sort of a comprehensive policy framework that is going to be to the advantage of rights-respecting allies and partners—the U.S. the EU, the Japanese, the Australians, South Koreans—and as inclusive as possible of middle ground states that are willing to subscribe to a rights-respecting use of these technologies.

Senator YOUNG. You have not settled—just by way of follow-up, you have not settled on a particular format, you have not identified who will sit in the individual seats around a table as you try and harmonize different policies? Is that accurate? I am not asking this critically—

Mr. FICK. Sure.

Senator YOUNG. —but as an important investigative matter by this committee.

Mr. FICK. I think there are two basic approaches we could take. One approach would be to form a new group—a T-12, a T-15, a T-18—an alliance of techno democracies, if you will. That has been in the press, in the think tank world. It has been a subject of discussion.

The other general approach is to use the alliances and the partnerships that we have or to create new ones and make sure they are fit for purpose—Senator Shaheen's question about NATO, Senator Kaine's question about AUKUS.

My view and the view of the Department, the view of the Secretary, is that we should do the latter—that we should be using organizations that exist. We should not be setting up new secretar-



iat's with overhead, creating new sets of meetings for people to attend.

We should be using existing organizations. We should be ensuring that they are fit for purpose and we should be making sure the technology issues and AI governance are threaded through all of them.

Senator YOUNG. Okay. I very much hope that you will keep myself and other members of this committee informed of developments as it pertains to who you will be convening, when you will be convening them.

I hope it is not in the very distant future—that is, the first quarter or two of next year—and what you anticipate the agenda looking like.

Mr. FICK. Senator, if I may. You asked a question about the private sector I think it is important to address here.

Senator YOUNG. Yes, sir.

Mr. FICK. The private sector has been front and center in these discussions from day one, starting with the voluntary commitments of the White House. They have been involved in every multi-stakeholder consultation in the G-7 and the G-20 and other fora. They were present in force at Bletchley Park, widely consulted on the E.O.

Again, back to the point that the bulk of the innovative horsepower in our economy sits in the private sector. The bulk of our talent is in the private sector. The bulk of the attack surface we care about protecting is in the private sector.

This only works if it is truly a multi-stakeholder process involving governments, companies, and civil society and other organizations.

Senator YOUNG. Thank you, Ambassador. Thank you, Chairman, for your patience.

The CHAIRMAN. Let me again acknowledge that Senator Young has been instrumental in bringing together the top experts basically in the world on AI in a nonpartisan environment where we can really absorb and try to understand where we are today, where we are heading, and what are our options and what are our needs.

Thank you very much for that help. Appreciate it very much.

Senator Risch, anything?

Senator RISCH. I am good. Thank you.

The CHAIRMAN. Let me thank our witnesses. Let me just underscore the point. We recognize this is not just a governmental exercise. It is the private sector as well, but the private sector also needs to have guardrails and needs to be protected.

That is why the global rules are incredibly important for how the United States leads in establishing those global rules not only for state actors, but also for private companies.

This conversation will continue. We anticipate there is going to be legislative action throughout 2024 in regards to AI to try to get a handle on appropriate guardrails and to give us the tools so we can continue to lead in innovation, but also in the responsible use of AI.

Thank you both for your contributions and we look forward to the continuation.

The record will remain open through close of business on Friday for members who may have questions for the record. We would ask that you respond in a timely way.

Thank you.

Mr. FICK. Thanks for having us.

The CHAIRMAN. The hearing is adjourned.

[Whereupon, at 11:25 a.m., the hearing was adjourned.]

#### ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

##### RESPONSES OF MR. NATHANIEL FICK TO QUESTIONS SUBMITTED BY SENATOR BENJAMIN L. CARDIN

*Question.* U.S. Leadership in Global AI Governance: The world has recognized the need for international engagement and cooperation on AI, underscored by the recent rapid advancements in powerful generative AI models. The U.S. has played a leadership role in the global conversation on AI, including at the AI Safety Summit in London and through the G7 AI International Code of Conduct. As governments around the world attempt to respond to the proliferation of these advanced AI tools. What role should the United States play in shaping international AI governance and what are our highest priorities? How can we ensure that our interests and values are protected as other actors, including some of our competitors, seek to shape the global AI landscape?

*Answer.* The United States is taking a strong leadership role in shaping international AI governance. Our priorities include: leading with an affirmative, positive vision on technology; maintaining a focus on innovation; ensuring trust, transparency, and a risk-based framework; establishing guardrails around AI use; mitigating potential harms; and ensuring AI policy is grounded in established ethical frameworks.

The United States promotes the responsible use of trustworthy AI in line with democratic values and respect for human rights. We advocate for an international, multistakeholder AI ecosystem that enables innovation and fosters public confidence in AI. We can ensure that the United States' interests and values are protected by building coalitions of like-minded countries who coalesce around a set of commitments on AI that reflect these values.

*Question.* How are U.S. domestic efforts around AI impacting U.S. competitiveness and leadership internationally? Does the U.S. need domestic regulation on AI in order to remain competitive on the international stage?

*Answer.* The United States must continue our international engagement on AI even while domestic efforts take shape. The Department of State's role is to advance U.S. AI policy in the international domain. This is an iterative process as the Administration works on its lines of effort, such as the voluntary commitments and the Executive Order, while discussions in Congress on possible legislation are underway. President Biden has also called on Congress to pass bipartisan data privacy legislation which will further support the Department's AI-focused engagement internationally.

However, even as we and others work on domestic approaches, we believe international dialogue is crucial to maintain interoperability and build consensus around shared regulatory approaches. The U.S. approach domestically to AI is directly relevant to our global influence and how other governments choose to govern this technology. Our multi-stakeholder approach begins with university and industry research and innovation, includes voluntary commitments from leading AI companies for safety and security, and incorporates civil society stakeholder input. The United States seeks to be a global model of how forward-looking, rights-respecting countries can leverage AI to advance both our shared values and our shared aspirations by putting in place the requisite guardrails to ensure safety and security and mitigate harms.

*Question.* Does the Department require any additional resources or authorities to promote U.S. leadership on AI?

*Answer.* With the creation of the State Department Bureau of Cyberspace and Digital Policy (CDP) and the Office of the Special Envoy for Critical and Emerging Technology, we are well placed to promote U.S. leadership on AI. Due to the ever-increasing global interest in policymaking on AI and related digital economic issues,

and considering the growing long-term geopolitical, economic, and human rights implications, additional personnel and resources remain a necessity. The establishment and funding of a dedicated Foreign Assistance Fund for Cyber, Digital, and Related Technologies would help support U.S. leadership in this space, represent a needed step forward in the evolution of U.S. cyber diplomacy, and provide a clear return on investment for U.S. national security interests. CDP remains eager to discuss this important concept with Congress.

*Question.* AI and Strategic Competition: We are all very aware that the PRC Government has already demonstrated its willingness to use AI-enabled tools like facial recognition and social scoring to facilitate mass surveillance and repression on its own population, particularly Uyghurs and Tibetans. Given these facts, do you think it was appropriate that the PRC participated in the UK AI Safety Summit? Why? Can you help us understand the fact that the United States AND the PRC both agreed to the same set of AI principles outlined in the Bletchley Declaration at that summit?

*Answer.* The Bletchley Declaration represents an important expansion of the multilateral work on AI we accomplished this year, including through the G7 Hiroshima AI Process, with likeminded partners and allies. The decision to invite the PRC was made by our UK counterparts, who were the hosts of the conference. Many major stakeholders active in the AI space, including countries large and small, accepted the key outcomes around AI safety in Bletchley, suggesting that there are areas where norms can be adopted, even if we disagree on other important arenas of AI. Having the PRC endorse a declaration where protection of human rights and transparency around AI are explicitly stated helps align international norms with U.S. national interests.

*Question.* How is the Administration viewing the need to maintain a dialogue with the PRC on avoiding AI's most significant risks while also pushing back against the PRC's digital authoritarianism and its efforts to influence global norms on AI?

*Answer.* Channels of communication are important to protect against both expected and unexpected risks which may arise from the use or deployment of emerging technologies, such as AI. Ensuring that safe and rights-respecting AI is adopted, deployed, and used globally includes discussions on AI at the UN and other global fora, which will necessarily require interaction and conversations with the PRC. In multilateral bodies across the United Nations, we are actively working with likeminded partners at the International Telecommunications Union (ITU) and the United Nations Educational, Science and Cultural Organization (UNESCO) to stem the diffusion of critical technologies that enable authoritarian misuse, to include taking tailored actions if those governments seek to use these technologies to jeopardize our national security.

*Question.* The PRC is ahead of the rest of the world when it comes to establishing AI regulations with clear anti-compliance repercussions, including rules requiring that AI generated content by PRC companies is compliant with PRC law. How do you assess the PRC's domestic regulatory actions on AI will impact their AI competitiveness and innovation? How are other capitals struggle with similar questions, how do you assess they are responding to the PRC model?

*Answer.* The PRC's regulations reflect a desire to increase control over the outputs of AI systems to align with "core socialist values," and potentially to use these systems for state-driven purposes, such as surveillance. It is not yet clear how the PRC's regulatory actions will impact their AI competitiveness and innovation.

One manner in which the PRC appeals to other countries in this domain is to tout "access to AI technologies" for developmental purposes. While the actual technologies and use cases remain nebulous, the simple promise of development-oriented AI can attract support. We maintain active and consistent engagement with partners and allies on discussions of AI technologies and work to advance efforts, particularly with developing countries, to push back against PRC influence efforts related these technologies.

*Question.* Global AI Equity: Across the globe, leveraging AI could help advance progress in critical areas such as healthcare, education, and addressing issues related to climate. At the same time, some have voiced concerns about the risk that developing countries could be left behind from the benefits that advanced AI tools can bring to bear. India in particular has sought to highlight this issue through its Chairmanship of the Global Partnership for AI. How is the Department seeking the participation of a broader range of stakeholders and governments to work towards equitable distribution of the benefits of AI?

Answer. Engaging a broad range of stakeholders is a key component of the United States' strategy to ensure a cohesive approach to realizing our vision for the global use of AI. We are working globally, including with developing countries, to identify and promote broadly accepted norms, guardrails, and governance models for this technology. We are working in bilateral, multilateral, and multi-stakeholder venues to build international partnerships driven by shared values and a shared commitment to the responsible use of AI. The Department seeks to ensure that the developing world benefits from AI-based technologies and does so through a rights-respecting, democratic governance system.

At the "Artificial Intelligence (AI) for Accelerating Progress on the Sustainable Development Goals (SDGs)" event during the 78th UN General Assembly, Secretary Blinken announced that the State Department will work with Congress to provide \$15 million to "help more governments leverage the power of AI to drive global good, focused specifically on the Sustainable Development Goals." The Department anticipates allocating at least \$7.5 million in funds from the CDP-managed Digital Connectivity and Cybersecurity Partnership (DCCP) over the next 5 years to promote the responsible use and governance of AI globally. This allocation would include programs such as "AI Connect," which is designed to strengthen the multi-stakeholder AI ecosystem, promote trustworthy AI applications and the responsible use of AI, and empower low and middle-income countries to more effectively participate in global conversations on AI and deploy AI-based solutions to public policy challenges.

*Question.* G7 Hiroshima Process: The United States and other G7 members released an "International Code of Conduct," which provides voluntary guidance for organizations developing the most advanced AI systems. How does the Hiroshima Process play into the Administration's broader goals of leading with partners on AI governance internationally?

Answer. The development of the "International Code of Conduct for Organizations Developing Advanced AI Systems" by the G7, as a part of the G7 Hiroshima AI Process, is an important step in showing that the G7 can meet the AI moment and that democratic systems can move quickly and deliver results for our citizens. This effort has helped to internationalize our own domestic efforts such as the U.S. voluntary commitments. The Code of Conduct is a significant diplomatic achievement that advances the United States' approach to AI governance by leveraging a larger multilateral framework. The Code consists of 11 principles that are directly inspired by and reinforce the U.S. Voluntary Commitments. It represents the most substantive international effort yet on international governance, and a common approach among the world's leading democracies, released by G7 Leaders ahead of the UK AI Safety Summit, amidst renewed UN interest in AI, and before adoption of the anticipated EU AI Act. Several leading U.S. companies have already voiced their support, and companies from other G7 countries are moving toward support.

*Question.* Noting that the international code of conduct is a set of voluntary principals, does the Administration anticipate that the Hiroshima Process will lead to more enforceable actions in the future?

Answer. It is important that the United States and like-minded partners begin discussions around AI regulation and governance with voluntary principles to ensure strong alignment and coordination with the private sector and research community and to ensure regulation does not stifle innovation. The Department believes that domestic regulations, which may include enforceable actions based on a risk-based framework, can inform international discussions. The President has voiced support for bipartisan legislation along these lines.

*Question.* U.S. Trade Representative Decision on Digital Trade: USTR recently announced that it would no longer pursue digital trade rules on data flows, data localization, source code protection, and digital non-discrimination. As you conduct digital diplomacy with other nations, how does USTR's decision affect your ability to advance a free, open, and interoperable internet? How does it impact our efforts to coordinate with allies and partners on AI research and development?

Answer. The United States is committed to advancing a fair, inclusive, and innovative digital economy, and we continue the United States' long-standing support for the trusted free flow of data and an open Internet with strong and effective protections for individuals' privacy as well as measures to preserve governments' abilities to enforce laws and advance policies in the public interest.

*Question.* U.S. Federal Data Privacy Laws: One of the many risks posed by the rapid development and deployment of artificial intelligence is the impact that this technology will have on our privacy. However, this is by no means a new problem.

As you know, the United States has struggled for years with some of our closest European partners over issues related to data privacy protections for cross-border data flows. How does our lack of federal data privacy laws impact our ability to promote cooperation with allies and partners on artificial intelligence research and development?

Answer. A bipartisan and comprehensive national data protection law will add further credibility to the United States' efforts to build international partnerships around AI governance, norms, and values, and the Biden administration has strongly supported Congressional adoption of comprehensive data protection law. The United States has long-standing practices around privacy, has often been at the vanguard of such discussions in the OECD, APEC, and elsewhere, and has robust privacy safeguards in several key sectors such as health and financial data, as well as strong protections on government handling of personal data. Nevertheless, the lack of a comprehensive national data protection law remains a key challenge when the United States is asking other countries to make commitments around data and digital economy matters, seeking to cooperate on AI research and development with our allies and partners, and advocate on U.S. principles of privacy and effective data governance.

*Question.* What is your assessment of the need for federal data privacy legislation in terms of both safeguarding American's privacy while also promoting U.S. innovation and competitiveness on artificial intelligence? Is it a necessary foundation for potential subsequent regulatory actions on artificial intelligence?

Answer. Comprehensive national data privacy legislation would add further credibility to the United States' diplomatic efforts to shape the international environment around AI governance and on other, related digital policy issues. Trust and transparency in data use is an important foundation to support future risk-based regulations on AI. President Biden has called on Congress to pass bipartisan data privacy legislation to better protect Americans' privacy, including from the risks posed by AI.

*Question.* How effective has the U.S.-EU data sharing agreement been in facilitating data flows between the U.S. and Europe?

Answer. The U.S.-EU Data Privacy Framework is an important instrument to support the digital trade flows that underpin the transatlantic digital economy. The Framework underscores with the EU our shared commitment to privacy, data protection, the rule of law, and our collective security, as well as our mutual recognition of the importance of transatlantic data flows to our respective citizens, economies, and societies. Data flows are critical to the transatlantic economic relationship and for U.S. companies from all sectors of the economy. The Framework has been effective in restoring legal certainty and predictability in transatlantic data flows.

*Question.* Addressing the Spread of AI-Generated Disinformation: At the UK AI Safety Summit, Vice President Harris called on all nations to support the development and implementation of international standards to help verify authentic government-produced digital content through techniques such as watermarking and labeling. How is the State Department assisting with this initiative?

Answer. The Department of State is working to advance mechanisms to increase global resilience against deceptive or harmful synthetic AI-generated or manipulated media. We will be working closely with civil society, private sector, academia, standard-setting technical bodies, industry, international community, and others to harmonize effective authentication and identification standards through a multi-stakeholder process to inform the U.S. Government and international content authentication and provenance practices.

The Department is supporting global partners and civil society to inform and implement content authentication standards. Our affirmative vision is reflected in both our engagements and foreign assistance. We plan to provide a range of support to ensure the development and implementation of these standards is inclusive. First, we are supporting civil society organizations to engage directly with key standards setting bodies and to inform the U.S. Government about international content authentication and provenance practices. Second, we intend to sponsor capacity building and training programs to support G7 partners, journalists, and other stakeholders to implement best practices including those involved in establishing and implementing content authentication and provenance standards. Third, the Department of State convenes international Technology Challenges to identify local and regional technologies that could be applied to address issues including digital content authentication and AI-generated content detection.

*Question.* What are the most promising tools or global standards for digital content provenance?

*Answer.* The Department of State's Global Engagement Center (GEC) encourages the development of guidelines, tools, and practices for digital content authentication and synthetic content detection capabilities to enhance high-integrity information exchange. The GEC has openly encouraged the adoption of tools and safeguards to increase the integrity and transparency of the information environment abroad, to include international outreach to encourage and support the development and implementation of uniform content authentication and provenance standards. A promising strategy leverages multiple technologies for digital content authentication rather than a single best practice, such as using a combination of watermarking, labeling, authentication blockchain technologies, steganographic techniques, content modification logs, and hardware verification.

GEC is engaged in outreach efforts to the private sector and academia, to include members of the Content Authenticity Initiative, as they identify and implement technologies for content authentication and provenance of high-integrity content. These efforts include understanding the various forums and standards being enacted or deliberated and how the U.S. Government should be involved or otherwise learn from those efforts to inform our own policies and regulations.

Further, the GEC facilitates the use of a wide range of technologies and techniques to reduce the malign use of AI by sharing expertise among U.S. federal departments and agencies, and international partners. The GEC executes a technology testbed to rapidly test emerging technology applications for digital content authentication and synthetic content detection measures. The GEC has tested technology to authenticate foreign digital content and track its provenance abroad and was an early tester of processes to label digital content through watermarking.

---

RESPONSES OF DR. MATTHEW GRAVISS TO QUESTIONS  
SUBMITTED BY SENATOR BENJAMIN L. CARDIN

*Question. Department Adoption of AI Tools:* Data analytics and machine learning tools, if deployed correctly and responsibly, present an opportunity to inform and accelerate decision-making, to create efficiencies to reduce the number of person-hours required to complete complex tasks, to broaden the bandwidth to pursue other critical missions, and to identify key areas of improvement.

Could you describe specific ways in which the Department has integrated AI and machine learning tools into its work? How have they enhanced the Department's ability to pursue its mission, particularly as it relates to challenges like strategic competition and climate change?

*Answer.* AI has progressively improved the Department's ability to meet its mission. For example, the Department included a data scientist in its COP27 delegation, allowing negotiators to have a decision-advantage by modeling the impacts of proposals in real time. These same climate-focused data scientists streamlined the creation of climate negotiator briefing materials about 190 countries from 9 hours to 9 seconds; and, recently explored AI use in the robust collection of information for climate evaluations.

*Question.* How are these tools and capabilities being coordinated across the Department from bureau to bureau?

*Answer.* The Department has robust data governance policies and coordination mechanisms at all organizational levels. As the Department's Chief Data and AI Officer, I chair the Enterprise Data & AI Council (EDAC), which sets the strategic direction for data and AI utilization Department-wide. Subordinate to the EDAC is a robust Data Governance Network, which includes Bureau-level Chief Data Officers (BCDOs) and other data and AI practitioners across the Department to coordinate tools, capabilities, and cross-bureau strategic initiatives.

*Question.* In an era of strategic competition, why is it important that the Department of State embrace data analytics and machine learning tools?

*Answer.* The United States is in a race for information and decision advantage against the PRC, Russia, and other competitors. In a world of information overload, data analytics, machine learning, and AI are increasingly important tools for accelerating "speed-to-insight," finding needles in haystacks, and providing national security leadership with actionable information through analytical tools and tradecraft—quantitative and qualitative alike. For example, we intend to pursue responsible generative AI to make better, systematic use of the information in our over 60 million diplomatic cables.

*Question.* While the State Department seeks to cooperate with partners at an international level on responsible AI principles, it is all the more critical that the Department has its own house in order in terms of responsible AI use.

What oversight mechanisms does the Department have in place to ensure that these tools are deployed safely and responsibly?

*Answer.* As the chair of the Enterprise Data and AI Council, I have designated the Department's Responsible AI Official to chair the offshoot AI Steering Committee, where technical experts in data science, records management and privacy, cybersecurity, legal affairs, and procurement address tactical questions of safe and responsible AI deployment in accordance with E.O.s 14110, 13960, and 13859. These groups oversaw development of the Enterprise AI Strategy (E AIS), which articulates the responsible deployment of safe, secure, and trustworthy AI.

*Question. Department of State Enterprise AI Strategy:* The Department recently released its first ever "Enterprise AI Strategy."

Could you describe the vision that this strategy sets out for the Department's future use of AI?

*Answer.* The vision of the Enterprise AI Strategy is that the Department of State will responsibly and securely harness the full capabilities of trustworthy artificial intelligence to advance United States diplomacy and shape the future of statecraft. We will execute this vision through four goals focused on secure infrastructure, an AI-ready workforce, high-quality data assets, and responsible innovation. The successful realization of this vision will depend on Department-wide collaboration through the Enterprise Data and AI Council (EDAC) and the Data and AI Campaigns it oversees.

*Question.* How does this new strategy shape or enhance the way the Department's existing AI guidelines?

*Answer.* The Department's existing AI guidelines, outlined in 20 FAM 201.1, lay out a framework within which the Department's workforce can use AI responsibly and largely aligns with E.O. 13960. The Enterprise AI Strategy augments this existing policy framework by identifying opportunities to embed AI into existing Department operational and policy processes to improve efficiencies and reduce workload burden. Additionally, the Strategy complements this policy framework by initiating Department-wide AI maturity processes aligned to E.O. 14110.

*Question. AI Workforce:* The Administration's Executive Order has placed an emphasis on the need to boost the Federal Government's ability to hire individuals with the necessary skills to not only find ways to leverage AI, but also to ensure that the adoption of AI is safe and responsible.

What types of skillsets and backgrounds will be needed for the Department to ensure that these tools are adopted responsibly and ethically?

*Answer.* The Department has deployed data and AI modules into mandatory tradecraft and DCM onboarding, in addition to its existing slate of elective data and AI courses. Last year the Department initiated the Bureau Chief Data Officer program, places senior data/AI leaders in all bureaus alongside bureau leadership to responsibly infuse data and AI into decision making processes. Additionally, the Department has onboarded nearly five dozen job series 1560 data scientists and U.S.D.C. fellows and have created a Locally Employed Staff Data Scientist position description for all posts.

*Question.* What obstacles does the Department face in filling any hiring gaps?

*Answer.* The Department strives to be a model employer and a home to top-tier talent by positioning itself to rapidly onboard data and AI practitioners that will strengthen our policy decisions and operational processes. The Federal Government is generally at a disadvantage versus private sector counterparts in terms of hiring. We are encouraged by recent changes allowing for direct hire authority on relevant job series. We are working to improve the Department's hiring competitiveness through additional avenues such as specialized incentive pay.

*Question.* In September, the Office of Personnel Management announced a direct hire authority for federal agencies for data scientist positions.

How does this authority impact the Department's ability to meet its AI workforce needs? What else should this committee consider to ensure that the Department is able to expand the use of data and AI to meet its mission?

*Answer.* Direct hire authority will improve the Department's ability to be a competitive employer in the marketplace by expediting the hiring of data science and AI talent. The Department is seeking to ensure its workforce can be compensated at a comparable rate to private sector counterparts. Department organizational

units require specialized positions, like Bureau Chief Data Officers, who are positioned at the bureau level to manage and govern data assets so that data scientists can analyze data and leverage AI techniques to create evidence for decision-makers.

*Question. Administration EO and Digital Content Provenance:* The Administration's recent EO on artificial intelligence requires the Department of State and other federal agencies to issue guidance for authenticating the digital content they produce or publish.

What role will your office play in addressing the risks posed by AI-generated content as outlined in the executive order?

Answer. As the Chief Data and AI Officer for the Department, my office plays a central role in creating the governance framework around responsible AI and any associated risk. The Responsible AI Official (RAIO), who reports to me, is the Department's lead on AI risk and chairs the AI Steering Committee (AISC)—a group of technical experts that are charged with mitigating AI's various risks. As my office leads the implementation of the Enterprise AI Strategy, the RAIO and AISC will assemble policies and procedures for safe, secure, and ethical AI use.

*Question.* How is your office coordinating internally at the Department, including with offices like the Global Engagement Center, to identify and address foreign disinformation operations enabled by generative AI?

Answer. The Global Engagement Center leads the Department's efforts to identify and address foreign disinformation and propaganda, is an active member of the State Department's Enterprise Data and AI Council (EDAC) and has shared tactics and findings in this space at EDAC meetings. Additionally, the EDAC's current AI for Public Diplomacy (PD) Campaign is sponsored by the Under Secretary for Public Diplomacy and Public Affairs (R) and coordinates data and AI efforts across the R Family (of which GEC is a part) and with PD practitioners at post.

*Question.* Does the Department of State intend to label and authenticate the digital content posted on its public website?

Answer. E.O. 14110 outlines steps that federal departments and agencies will take to make recommendations and issue guidance related to labeling and authenticating digital content they create and share with the public. As such, the Department, led by the Responsible AI Official and the AI Steering Committee, will take steps to develop a plan for such labels and authenticating measures, consistent with any recommendations or guidance issued pursuant to the E.O. We want to make sure the public will be able to trust when they see content from a U.S. Government source.

*Question.* Are you aware of any existing tools or global standards for digital content provenance?

Answer. We are aware of both standards and techniques used by the public and private sector globally to certify digital content. It is imperative that the Department, led through the Enterprise Data and AI Council, work with digital creators in bureaus, offices, and posts and across the interagency to leverage an appropriate metadata standard that ensures content shared by the Department can continue to be trustworthy.

---

RESPONSES OF MR. NATHANIEL FICK TO QUESTIONS  
SUBMITTED BY SENATOR CHRISTOPHER A. COONS

*Question.* USTR recently announced that it would no longer seek to advance digital trade rules on data flows, data localization, source code protection, and digital non-discrimination. Does this decision reflect an interagency consensus to abandon these longstanding priorities that have been consistent across Administrations of both parties?

Answer. We continue the United States' long-standing support for the trusted free flow of data and an open Internet. We are committed to advancing a fair, inclusive, and innovative digital economy, with strong and effective protections for individuals' privacy as well as measures to preserve governments' abilities to enforce laws and advance policies in the public interest.

In the coming weeks and months, we will step up our engagement with stakeholders—including both large and small companies in the technology and other data-intensive sectors as well as privacy, safety, labor, and human rights advocates—and work with our partners to chart a path forward that appropriately balances these objectives. We will continue to engage vigorously on the WTO's Joint Statement Initiative on E-Commerce. We also look forward to working with Mem-



bers of Congress to support the legislative process on privacy, competition, and digital regulation.

*Question.* If not, will you work with partners across the interagency to arrive at a new consensus position that supports American jobs, economic growth, and global competitiveness?

*Answer.* We are committed continued engagement with stakeholders on this topic. We know these are complex issues, but we are bringing a whole-of-government effort to find solutions and stepping up our extensive engagement to chart a path forward. The Department is committed to work across the interagency on these issues to support American jobs, economic growth, and global competitiveness.

---

RESPONSES OF MR. NATHANIEL FICK TO QUESTIONS  
SUBMITTED BY SENATOR BRIAN SCHATZ

*Question.* Unregulated AI-generated content could destabilize societies around the world. Although many other countries, including the G7, the EU, even the People's Republic of China, have implemented, or are pursuing AI labeling regulations, the United States has not. Would U.S. diplomatic efforts be bolstered if the United States legally required companies to label AI-generated content?

*Answer.* Since taking office, President Biden, Vice President Harris, and the entire Biden-Harris administration have moved with urgency to seize the tremendous promise and manage the risks posed by Artificial Intelligence (AI) and to protect Americans' rights and safety. As part of this commitment, President Biden convened seven leading AI companies at the White House on July 21 to announce that the Biden-Harris administration secured voluntary commitments from these companies to help move toward safe, secure, and transparent development of AI technology. As a result, several companies have committed themselves to developing and implementing mechanisms to increase transparency, such as content authentication and provenance that will enable informing the public about the origins of their content, such as labeling. At the same time, under the Executive Order issued on October 30, the U.S. Government committed to developing such mechanisms for its own content. Creating effective mechanisms remains a significant technical challenge that governments and companies around the world must still address, but these initial efforts will bolster our ability to coordinate with allies and partners around common, technically feasible approaches to content authentication and provenance.

*Question.* How are you prioritizing AI labeling regulations in your diplomatic discussions?

*Answer.* The United States is deeply engaged in discussions around AI labeling in several fora with allies and partners, most prominently the G7 and the OECD. In these fora the Department of State is working to advance mechanisms and strategies to increase global resilience against deceptive or harmful synthetic AI-generated digital content.

*Question.* Governments around the world are cutting off internet access to suppress critical comments and remain in power. AI algorithms can make this practice even more effective. What tools do we have to discourage partners from cracking-down on internet freedom—whether by using AI or other methods?

*Answer.* We are concerned by increasing efforts from governments to control Internet access and content—including through the blunt use of Internet shutdowns to suppress freedom of expression online—to stifle dissent, quell protests, curb criticisms of the government, or limit information leading up to and during elections. The U.S. Government has made Internet freedom a major foreign policy priority for more than a decade. The Department uses several tools to protect human rights online, including raising our concerns bilaterally, building and participating in multi-lateral and multi-stakeholder coalitions, messaging our concerns through public diplomacy efforts, and providing venture-capital-like grants to leading technologists and NGOs for capacity building.

Regarding algorithms, we recognize that while AI can be immensely helpful to technology companies in flagging content that may violate their terms of use, it can also be used to suppress critical discourse. We strongly discourage government intervention on content regulation and instead encourage all governments to respect the independence of technology platforms in developing and implementing content moderation policies as per their terms of service.

*Question.* Can you provide examples of where those tools have been successful and assess where the biggest challenges remain?

*Answer.* The Department works together with our country desk officers, relevant bureaus, and U.S. embassies to monitor and respond to laws, policies, and activities that impact human rights online, and works to elevate concerns through appropriate channels, both publicly and bilaterally. We also engage through international organizations and UN bodies, such as the OECD and the G7, where we strive to develop consensus around Internet freedom issues that we hope will establish strong foundational norms. We continue to play a leadership role in the Freedom Online Coalition (FOC), a group of 38 like-minded governments committed to advancing human rights online. The FOC has been instrumental in building cross-regional coalitions to support Internet freedom, addressing related challenges in multilateral venues, and creating a space for collaboration with civil society and business around related emerging and critical issues, including AI.

*Question.* Besides U.S.-led efforts, which multilateral and international organizations should we be prioritizing to help promote internet freedom in the face of AI?

*Answer.* In multilateral bodies across the United Nations, such as in the International Telecommunications Union (ITU) and the United Nations Educational, Science and Cultural Organization (UNESCO), we are actively working with like-minded partners to stem the diffusion of critical technologies that enable authoritarian misuse, to include taking narrowly-focused actions if those governments seek to use these technologies to jeopardize our national security. The United States will continue to lead and support global norm setting for the use of AI to ensure the adoption and deployment of safe and values-based standards.

*Question.* What guardrails must be put in place to set AI development on a path that bolsters democracy, not undermines it?

*Answer.* All actors developing, deploying, and using AI can and should be implementing measures throughout the lifecycle of AI systems to manage the risks this technology can pose to democracy as well as support civil and human rights. Such measures include conducting impact assessments, sufficiently testing AI systems in appropriate real-world contexts, identifying and mitigating factors contributing to algorithmic discrimination or other disparate impacts on specific populations, and conducting ongoing monitoring of deployed AI systems. Other measures include creating options for ongoing feedback, repeal, and recourse by users and other impacted stakeholders; training AI operators on risk identification, assessment, prevention, and mitigation; prioritizing cybersecurity by design in AI systems; as well as implementing transparency measures such as watermarking synthetic content or disclosing when decisions are made by AI systems.

*Question.* How do you weigh the tradeoffs of including the PRC, which staunchly opposes freedom of expression, in international negotiations over AI?

*Answer.* AI will impact nearly all facets of government and society around the world, and a multistakeholder and international approach is necessary to mitigate potential risks to people's rights and safety. We also recognize that international cooperation is essential to building a safe, secure, and trustworthy AI future. A multistakeholder approach is critical to build international consensus around safe, secure, responsible, ethical, trusted, and transparent use of AI technology that protects, among other principles, the freedom of expression.

Through this approach, the United States engages with many countries on AI issues, including those active in the development of AI technologies, such as the PRC. As part of these conversations, the United States and the international community deploys strategic, long-term, and persistent diplomacy to continue to protect and promote freedom of expression and human rights. Overall, ensuring that safe and rights-respecting AI is adopted, deployed, and used globally, includes discussions on AI at the UN and other global fora that will necessarily require interaction and conversations with the PRC.

**Letter to President Biden, Dated November 30, 2023,  
Concerning the Decision of the USTR To Stop Supporting  
Key Commitments in the E-Commerce Negotiations at the  
WTO**

*Submitted by Senator Chris Van Hollen*

United States Senate

WASHINGTON, DC 20510

November 30, 2023

The Honorable Joseph R. Biden, Jr.  
President of the United States  
The White House  
1600 Pennsylvania Avenue NW  
Washington, D.C. 20500

Dear President Biden:

We write to express our concerns with the decision of the United States Trade Representative (USTR) to stop supporting key commitments in the e-commerce negotiations at the World Trade Organization (WTO)—and potentially in other negotiations. These commitments reflect bipartisan principles that, until now, the United States has strongly supported across political parties, administrations, and the federal government: an open internet that promotes the flow of information across borders to support American exports and American values. USTR's decision to abandon these commitments at the WTO creates a policy vacuum that China and Russia will fill. Accordingly, before changing the longstanding U.S. position, we request that you work with Congress and run a comprehensive consultation process—with other federal agencies, with the public, and with us—to reach a consensus U.S. position on these issues that promotes U.S. competitiveness, innovation, and jobs.

For decades, the United States has been at the helm of global leadership on protecting, promoting, and expanding the open internet as both a means of worldwide connectivity and an engine of U.S. economic growth and opportunity. This effort has long been a feature of U.S. trade policy: the United States advocated for commitments to ensure the free flow of information in WTO rules agreed to almost 30 years ago, and our trade agreements with Korea, Mexico, Canada, and Japan include strong digital trade rules guaranteeing the right to move data across borders. In this vein, the United States joined negotiations on e-commerce at the WTO, working with like-minded democratic allies to create rules for a digital economy that is open, fair, and competitive for all. The United States has supported proposals to spur economic growth, encourage free expression and access to information, and promote consumer protections online, while also allowing countries to address concerns regarding security, privacy, surveillance, and competition. These negotiations are crucial to our strategic approach to outcompeting our adversaries: both China and Russia are at the negotiating table, actively pushing their cyber-agenda of censorship, repression, and surveillance that not only hurts their own citizens but also undercuts U.S. competitiveness. Indeed, China is actively seeking to weaken the very principles at issue so it can promote its own version of internet governance.

In spite of this, on October 25, 2023, USTR reversed course and announced that it was walking away from the negotiating table on several core commitments in the e-commerce negotiations. These commitments, which again have broad bipartisan support, are fundamental to the modern economy, supporting U.S. businesses of all sizes across all sectors. Specifically, USTR abandoned the following commitments:

- *Promoting the free flow of data.* Almost every sector of the U.S. economy requires cross-border data flows, from manufacturers sharing product specifications, to airlines diagnosing problems mid-flight, to farmers leveraging precision agriculture to maximize crop yield. Arbitrary and trade-distorting restrictions on cross-border data flows that serve no legitimate public policy purpose can prevent American firms from doing business abroad, stifle economic growth here at home, and trample on human rights in authoritarian countries. Russia, for example, has weaponized data-restrictive laws to crack down on dissent, control information, and expel civil society organizations amidst its ongoing invasion of Ukraine.<sup>1</sup> Recognizing the importance of data flows to U.S. economic and foreign policy goals, the United States' original proposal at the WTO sought to ensure that consumers, companies, and non-governmental organizations could move data across international borders, while recognizing that countries must be able to act in the public interest, such as to protect personal data from abuse and foreign surveillance.
- *Combating forced data localization.* China and Russia, as well as other countries emboldened by their actions, have increasingly pursued data localization measures that require certain domestic data to be stored or processed within their borders. These policies require companies to build or maintain capital- and energy-intensive infrastructure in every market they enter, a major expense for large businesses, but an insurmountable hurdle for small and medium-sized enterprises. Small and medium-sized businesses are then left with an impossible choice: enter a risky joint venture with a foreign enterprise or get shut out of the market entirely. In this way, authoritarian governments leverage data localization measures to discourage competition and facilitate governmental access to data within their borders, helping them access trade secrets, censor and surveil their citizens, and hide human rights abuses, including forced labor.<sup>2</sup> The United States' proposal sought to limit data localization, while acknowledging that in certain circumstances, data localization may be appropriate to address national security, law enforcement, and privacy concerns.
- *Preventing forced tech transfer.* The U.S. government opposes the Chinese government's practice of conditioning market access on the sharing of proprietary information belonging to U.S. innovators, creators, and start-ups—a threat to both our economic and national security.<sup>3</sup> The United States' proposal sought to ensure that countries could not

<sup>1</sup> Justin Sherman, The Brookings Institution, *Russia is Weaponizing Its Data Laws Against Foreign Organizations* (Sept. 27, 2022), <https://www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/>.

<sup>2</sup> Freedom House, *User Privacy or Cyber Sovereignty?* (2020), <https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty>.

<sup>3</sup> Daniel Wagner, *The Global Implications of China's National and Cyber Security Laws*, International Policy Digest (Aug. 10, 2020), <https://intpolicydigest.org/the-global-implications-of-china-s-national-and-cyber-security->

force businesses to surrender their source code or share it with domestic competitors as a condition of doing business, while preserving the ability of governments to access source code to achieve legitimate public policy objectives, such as conducting investigations and examinations and promoting consumer health and safety.

- *Open, competitive markets for digital goods and services.* The principle of non-discrimination has been a central component of U.S. trade policy for decades and underlies the international trading system that the United States helped create. It has opened markets for American exporters across industries, from farmers to filmmakers. At its core, non-discrimination ensures that foreign governments treat U.S. companies fairly. It ensures that countries cannot gain a competitive edge by targeting their regulations on imports from one or multiple countries without regulating similarly situated domestic businesses. China, in particular, has leveraged discriminatory policies to handicap international competitors and nurture its domestic companies, many of which are state-owned enterprises that operate at the behest of the Chinese government.<sup>4</sup> Not only do these homegrown giants facilitate human and worker rights abuses, particularly in the Uyghur community in Xinjiang, but they have the ability to grow without competition and then undercut American competitors in international markets. Recognizing this, the U.S. WTO proposal sought to ensure that protections against discrimination would apply to digital products (e.g., apps, music, games, and movies), ensuring that American creators, innovators, and businesses could operate on a level playing field around the world.

As indicated above, each of these commitments maintained flexibility to regulate for legitimate public policy reasons.

USTR provided no policy alternatives to these longstanding and bipartisan U.S. positions, nor a timeline for providing them. We are concerned that USTR's retreat will hurt workers and employers across all sectors of the U.S. economy, with disproportionate effects on small and medium-sized businesses in creative industries like film, music, and book publishing; innovative industries like software, medical devices, and precision agriculture; travel, tourism, and transportation; logistics, shipping, and supply chain management; and manufacturing, including the critical automotive and semiconductor sectors. Moreover, with this abrupt change in policy, USTR has not only turned its back on our democratic allies and undermined U.S. credibility in other negotiations and fora around the world, but it has also empowered authoritarian regimes like China and Russia, who are eager to fill the void and regulate U.S. jobs out of existence.

We recognize that there is much interest in the digital regulation space, particularly with the rapid adoption of artificial intelligence technology. We welcome discussions and debate on the best way to protect consumers, promote privacy, and ensure a competitive marketplace. However, these efforts do not require the United States to walk away from negotiating strong rules at the WTO that support U.S. businesses and workers—nor would these rules constrain the

---

<sup>4</sup> [laws.](https://www.uscc.gov/annual-report/2021-annual-report-congress)

<sup>4</sup> U.S.-China Economic and Security Review Commission, *2021 Annual Report to Congress* at p. 165, <https://www.uscc.gov/annual-report/2021-annual-report-congress> ("The Chinese Communist Party (CCP) views achieving technological self-sufficiency as essential for both economic growth and political survival.").

ability of the United States to regulate. In fact, the commitments under discussion have built-in exceptions that ensure countries can legislate in the public interest. Retreating from our longstanding principles without offering a viable alternative does not help U.S. workers, it does not help U.S. consumers, it does not help U.S. businesses, and it does not help U.S. allies; it only helps our adversaries.

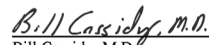
We continue to support the core commitments that USTR has distanced itself from in the WTO e-commerce negotiations. We request that you run a consultation process before changing the historical, consensus U.S. position on these important issues. We look forward to working with you to address this and other bipartisan Member concerns.


Sincerely,


  
Ron Wyden  
United States Senator

  
Mike Crapo  
United States Senator

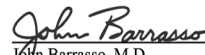
  
Thomas R. Carper  
United States Senator


  
Bill Cassidy, M.D.  
United States Senator

  
Chris Van Hollen  
United States Senator

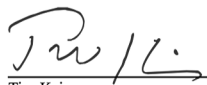
  
Thom Tillis  
United States Senator


  
Christopher A. Coons  
United States Senator

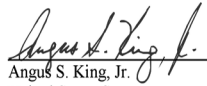
  
John Barrasso, M.D.  
United States Senator

  
Catherine Cortez Masto  
United States Senator

  
Charles E. Grassley  
United States Senator


  
Tim Kaine  
United States Senator

  
Ted Budd  
United States Senator


  
Angus S. King, Jr.  
United States Senator

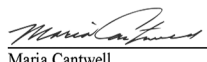
  
Todd Young  
United States Senator


  
Patty Murray  
United States Senator

  
Shelley Moore Capito  
United States Senator

  
Kirsten Gillibrand  
United States Senator

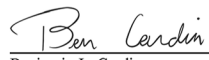
  
Steve Daines  
United States Senator

  
Maria Cantwell  
United States Senator

  
Kevin Cramer  
United States Senator

  
Kirsten Sinema  
United States Senator

  
Cynthia M. Lummis  
United States Senator


  
Benjamin L. Cardin  
United States Senator


  
John Cornyn  
United States Senator

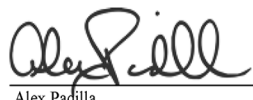
  
Mark Kelly  
United States Senator


  
James E. Risch  
United States Senator

  
Ted Cruz  
United States Senator

  
Ron Johnson  
United States Senator

  
Jacky Rosen  
United States Senator

  
Alex Padilla  
United States Senator

  
Tim Scott  
United States Senator

  
James Lankford  
United States Senator