Hearing on

Safeguarding Data and Innovation: Building the Foundation for the Use of Artificial Intelligence

House Committee on Energy and Commerce
Subcommittee on Innovation, Data, and Commerce

October 18, 2023, at 10:00 a.m.
Rayburn House Office Building
Washington, D.C.

Testimony of Victoria Espinel
CEO
BSA | The Software Alliance

Testimony of Victoria Espinel
CEO of BSA | The Software Alliance

Hearing on Safeguarding Data and Innovation: Building the Foundation for the Use of Artificial Intelligence

Before the House Committee on Energy and Commerce
Subcommittee on Innovation, Data, and Commerce

October 18, 2023

Good morning Chairman Bilirakis, Ranking Member Schakowsky, and members of the Subcommittee. My name is Victoria Espinel, and I am the CEO of BSA | The Software Alliance.[1]

BSA is the leading advocate for the global enterprise software industry.[2] Our members are at the forefront of developing cutting-edge services — including AI — and their products are used by businesses across every sector of the economy. I commend the Subcommittee for convening today's hearing and thank you for the opportunity to testify.

I appreciate this Committee's bipartisan focus and success in moving forward comprehensive consumer privacy legislation last year. I encourage the Committee to further refine its work in this Congress, to advance legislation that protects consumers and establishes nationwide rules for companies to act responsibly when they collect and use consumers' personal data.

This hearing implicates one of the most critical questions for our future: how do we protect consumers and enable the digital transformation of our economy?

Our nation's privacy laws will impact our development of AI, and our use of AI will impact Americans' privacy. The United States needs a strong, comprehensive federal privacy law that creates important limits around how companies collect and use consumers' information. We also need strong, effective laws addressing high-risk uses of AI. This Committee passed legislation last year that addressed both of these issues, and it is well-positioned to do so again.

Today's hearing comes at a particularly important time. Companies of all sizes and in all industries are undergoing a digital transformation, leveraging tools including AI to improve safety and competitiveness in every sector of our economy.

The United States needs to maintain its leadership on AI and digital transformation, not just in the development of these tools, but also in shaping the policy environment. Other governments worldwide have already enacted consumer privacy laws, as have 13 US states. The European Union and other countries are now poised to enact rules that will govern AI's future. The United States will have a stronger voice in the development of global AI rules with federal legislation that creates clear requirements on companies that develop and deploy AI for high-risk uses.

[1] I am a member of the National AI Advisory Committee, but I am testifying in my capacity as CEO of BSA.

[2] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Okta, Oracle, Palo Alto Networks, Prokon, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

I. Privacy and AI Are Critical to the Digital Transformation of the US Economy.

The promise that software and other digital tools may one day impact every industry has become a commercial reality. Over the past 20 years, consumers, businesses, and governments have moved online to conduct business and to share information, driving a digital transformation across every sector of the economy. Farmers can use AI to analyze vast amounts of weather information to use less water and maximize their harvest; manufacturers can adopt digital design and manufacturing processes; suppliers and distributors can retool how goods are ordered and delivered, and construction companies can build AI-generated "digital twins" of real-life cities to understand the impacts of a proposed design, to reduce costs and increase sustainability.

BSA members are the enterprise software companies leading this digital transformation, by creating the innovative products and services used by other companies.[3] BSA members prioritize creating privacy-protective products and services, and they understand that robust data protection is a key part of building consumer trust and promoting full participation in the digital economy. I have included an annex to this testimony with an extensive list of examples showing how companies in all industries are using AI-powered enterprise software. I want to focus on a few examples:

- In healthcare, a large pharmacy chain uses an advanced platform to forecast demand and redistribute medications across thousands of store locations and to deliver near real-time insights and recommendations for pharmacists to provide more personalized advice to patients. This helps managers understand the supply chain, store labor and productivity, patient vaccine scheduling, and prescription pickup processes.

- In manufacturing, a car maker used generative AI technology to redesign a seat bracket, which secures seat belt fasteners to seats and seats to floors, that is 40% lighter and 20% stronger than the previous iteration. Changes like these can help reduce the amount of material needed to build a car and make vehicles more fuel efficient.

- In agriculture, the research division of an enterprise software provider partnered with a climate risk company to develop software capable of providing more accurate long-range weather predictions. Traditional weather forecasting methods can provide accurate predictions for a seven-day window. By leveraging AI, the researchers are developing new forecasting models to provide accurate predictions of weather trends two- to six-weeks out from a given date. By providing reliable extended forecasts, these tools will help water managers predict snowpack and water availability for irrigation, hydropower, and other critical agricultural and environmental uses.

Companies are increasingly investing in digital transformation. By 2026, global digital transformation spending is forecast to reach $3.4 trillion.[4] The Digital Transformation Network, a cross-sector initiative of BSA, has highlighted digital transformation across the healthcare,

[3] BSA's policy and educational resources on AI are available at https://ai.bsa.org. For additional information about AI's adoption across industry sectors *see* BSA, Artificial Intelligence in Every Sector, *available at* https://www.bsa.org/files/policy-filings/06132022bsaaieverysector.pdf.

[4] *See* Statista, Spending on Digital Transformation Technologies and Services Worldwide from 2017 to 2026, *available at* https://www.statista.com/statistics/870924/worldwide-digital-transformation-market-size/#statisticContainer.

financial, and construction sectors, among others. Software-enabled digital transformation is significantly improving healthcare, particularly with respect to patient experience, innovations in treatment, and public health research.[5] Digital transformation also enables banks, insurers, and payment providers to support online services and identify potential fraud across global transactions.[6] Digital transformation also enables architects, engineers, and contractors to design, construct, and maintain buildings, including using digital twins to fix problems before a single brick is laid.[7]

Companies across industries are benefitting from digital transformation, including through the increased use of AI. By 2025, investment in AI is expected to approach $100 billion in the United States and $200 billion globally.[8] Generative AI alone could add up to $4.4 trillion of value to the global economy every year.[9]

To realize these benefits, however, consumers and businesses must trust that these technologies are developed and deployed responsibly. Countries that adopt clear privacy safeguards and rules that promote the responsible and broad-based adoption of AI will see the greatest economic and job growth in the coming years.

II. Congress Should Enact a Strong, Comprehensive Federal Consumer Privacy Law.

BSA companies recognize that protecting consumers' personal data is a key part of building customer trust. As a result, privacy and security protections are fundamental parts of BSA members' operations. Technologies like artificial intelligence, cloud computing, and data analytics rely on data and, in some cases personal data, to function, and consumers deserve to know their personal information is being used responsibly.

We commend the House Energy & Commerce Committee for its leadership on consumer privacy legislation. The Committee made great progress in advancing consumer privacy legislation last year, and we urge you to continue the important work of enacting a strong and comprehensive federal consumer privacy law.

For too long, consumers and businesses in the United States have lived in an increasingly data-driven and connected world without a clear set of national rules that limit how companies can collect and use personal information. Enacting a federal privacy law would meaningfully advance US leadership on privacy and bring consistency to existing protections. More

[5] *See* Digital Transformation Network, AI and Digital Tools for Better Health, *available at* https://dxnetwork.org/downloads/09062023healthcare.pdf.

[6] *See* Digital Transformation Network, Digital Tools Transform How We Save, Spend, and Invest, *available at* https://dxnetwork.org/downloads/04202023dtnfinancialservices.pdf.

[7] *See* Digital Transformation Network, Digital Tools Help Build a Better Future, *available at* https://dxnetwork.org/downloads/02232023dtnconstruction.pdf.

[8] Goldman Sachs, AI Investment Forecast to Approach $200 Billion Globally By 2025 (Aug. 1, 2023), *available at* https://www.goldmansachs.com/intelligence/pages/ai-investment-forecast-to-approach-200-billion-globally-by-2025.html.

[9] McKinsey & Company, The Economic Potential of Generative AI (June 2023), *available at* https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier?gclid=Cj0KCQjwl8anBhCFARIsAKbbpyTeLnz0c6i4X2UTnmWdO1KGQnE1mUR8ErJSrM0eMnWDxgfaZukt_L0aAqP7EALw_wcB#/.

importantly, it would create broad and long-lasting protections for consumers across the United States. Today, there are comprehensive consumer privacy laws in 13 states, but all consumers — nationwide — should be protected.

We believe federal privacy legislation should achieve three goals: (1) establish strong privacy rights for consumers, including the rights to access, correct, and delete their personal data; (2) impose strong obligations on companies to safeguard consumers' personal data and prevent misuse; and (3) provide strong, consistent enforcement. In each of these areas, a federal privacy law can — and should — build on the protections and obligations that states have advanced and enacted.

A. Establish Strong Privacy Rights for Consumers, Including the Right to Access, Correct, and Delete

A federal privacy law should give consumers important new rights over their personal data. Specifically, consumers should have the right to access their personal data, the right to correct personal data that is inaccurate, and the right to delete their personal data.

There is widespread agreement that these rights are core components of effective privacy legislation. At the state level, all 13 states to enact comprehensive privacy legislation have created rights to access and delete consumer information.[10] Eleven of the 13 states also create a right to correct inaccurate information.

Of course, these rights must be created in a manner that works in practice and be subject to appropriate limitations. For example, a federal privacy law should not give an individual the right to delete data that a company is legally required to retain. A federal privacy law should also recognize other appropriate limits on consumers' rights, to ensure those rights are exercised in a manner that strengthens privacy protections and does not undermine other important interests, such as protecting the security of a company's services or safeguarding the privacy of other consumers. In addition, a federal privacy law should assign the primary obligation to respond to rights requests to the company that decides how and why to collect and process that information. This approach will also ensure consumers know which organization to contact to exercise their rights.

B. Impose Strong Obligations on Companies to Safeguard Consumers' Data and Prevent Misuse

A federal privacy law should place meaningful limits on businesses that handle consumers' personal data and require them to handle that data responsibly.

These limits should also reflect the company's role in handling consumers' data, including whether the company decides why and how to collect a consumer's personal data, or instead acts as a service provider that processes a consumer's data on behalf of another company and pursuant to that company's instructions. The distinction between these two types of companies — often referred to as the controller and processor, or covered entities and service providers —

[10] BSA | The Software Alliance, 2023 Models of State Privacy Legislation, *available at* https://www.bsa.org/policy-filings/us-2023-models-of-state-privacy-legislation.

is critical to privacy laws worldwide[11] and is incorporated in all comprehensive state privacy laws.[12] Both types of businesses have important responsibilities, and the obligations placed on each type of company must reflect its role in handling consumers' data. If legislation does not reflect these different roles, it can end up undermining the goal of improving consumer privacy by creating obligations that inadvertently pose new privacy and security risks for consumers.

C. Provide Strong, Consistent Enforcement

Effective enforcement is important to protecting consumers' privacy, ensuring that organizations meet their commitments and legal obligations, and deterring potential violations.

BSA supports empowering both state attorneys general and the Federal Trade Commission (FTC) to enforce a strong, comprehensive privacy law. The FTC has demonstrated that it is capable of overseeing and enforcing those commitments and obligations, as is evident from the more than 150 privacy and data security enforcement actions the agency has brought under Section 5 of the FTC Act.[13] Given this strong record, the FTC should maintain its leadership role as the primary federal enforcer of consumer privacy protections. BSA also supports giving the FTC new authorities to enforce a comprehensive privacy law, including targeted rulemaking authority and the ability to fine first-time violators. Moreover, empowering state attorneys general to enforce a federal privacy law will maintain an important pathway for states to continue to promote and protect privacy.

D. The ADPPA Created an Important Baseline That Can Be Refined to Create Federal Privacy Legislation.

BSA commends the Committee for its dedication to moving bipartisan privacy legislation. We were pleased that the Committee-passed version of the American Data Privacy and Protection Act (ADPPA) made significant improvements to the legislation. As you continue to refine the Committee's approach to these issues, BSA looks forward to working with you to ensure the Committee advances legislation that achieves its objective of promoting consumer privacy. We urge you to focus on making the legislation more effective and workable, including: (1) creating flexibility in the list of permissible purposes for which companies can process covered data; (2) further clarifying the roles and responsibilities of service providers; and (3) defining key terms and refining provisions to increase clarity and workability.

1. Creating Flexibility in the List of Permissible Purposes

A strong and comprehensive federal privacy law must create important safeguards around how companies collect and process consumers' personal data. ADPPA creates a list of 17 "permissible purposes"[14] for which companies can process covered data. These purposes are

[11] BSA | The Software Alliance, Controllers and Processors: A Longstanding Distinction in Privacy, *available at* https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy.

[12] BSA | The Software Alliance, The Global Standard: Distinguishing Between Controllers and Processors in State Privacy Legislation, *available at* https://www.bsa.org/policy-filings/the-global-standard-distinguishing-between-controllers-and-processors-in-state-privacy-legislation.

[13] *See* FTC, Privacy and Data Security Update 2020, at 2–3, *available at* https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-2020-privacy-data-security-update/20210524_privacy_and_data_security_annual_update.pdf.

[14] *See* American Data Privacy and Protection Act (ADPPA), H.R. 8152 (Sec. 101(b)).

critical to how the bill functions in practice, because a company cannot process personal data unless it does so for one of these permissible purposes. We encourage the Committee to revisit this set of permissible purposes, to both add additional purposes to the current list and to create flexibility to accommodate future purposes. For example, the bill's list of permissible purposes is incomplete, since it does not clearly permit processing for purposes including research projects that consumers opted into, or specifically permitting companies to conduct disparate impact testing across their products and services. In addition, the list is not sufficiently flexible to accommodate future purposes that could arise and should be permitted. We strongly urge the Committee to work with stakeholders to create this flexibility, without creating an exception that undermines the bill's safeguards.

2. Further Clarifying the Roles and Responsibilities of Service Providers

A federal privacy law must reflect the different roles of covered entities and service providers. We commend this Committee for the significant progress it made in addressing the role of service providers in the ADPPA. However, further improvements are needed to better reflect the role of service providers, including recognizing that both service providers and covered entities can process data for the set of permissible purposes recognized in the bill. In addition, several provisions in the bill incorrectly assume that service providers review all personal data they process on behalf of their business customers. In practice, service providers are often subject to strict contractual and technical safeguards that limit when and why they access personal data they process on behalf of a business customer; these safeguards are designed to protect the privacy of that data. Legislation that assumes service providers review all data on their services can ultimately undermine consumer privacy, by creating incentives for service providers to start looking at data they otherwise would not.

Finally, while BSA strongly supports the objective of ADPPA's civil rights provision,[15] applying that provision to service providers creates significant concerns — since it could result in holding service providers responsible for discriminatory decisions by their business customers, even if the service provider had no way of knowing what data was used to make what decision. We encourage the Committee not to apply this provision to service providers in future legislation.

3. Defining Key Terms and Refining Provisions to Increase Clarity and Workability

A federal privacy law must also have clear and workable definitions. ADPPA contains several definitions that are overly broad or that could lead to unexpected outcomes, including the definition of "high impact social media company"[16] which could sweep in a range of companies well beyond social media. Additionally, the definition of "large data holder"[17] identifies certain covered entities and service providers subject to additional obligations. However, this definition is based on thresholds including whether the covered entity or service provider processes sensitive covered data. In practice, service providers may be unable to apply that threshold — because they are frequently prohibited from looking at data they process on behalf of business customers so are unlikely to know if that data is sensitive or not. We therefore urge you to focus on clarity and workability as you consider advancing privacy legislation, so that its key terms and provisions work as intended.

[15] *Id.* Sec. 207.

[16] *Id.* Sec. 2(20)(b).

[17] *Id.* Sec. 2(21).

III. Congress Should Also Act Now to Adopt Meaningful AI Legislation.

This Committee's work on provisions in the ADPPA to address AI creates a baseline to build on and refine to establish rules for the development and use of high-risk AI systems.

AI is a foundational technology that drives products and services that people use every day. It also raises important policy issues, which are core to the digital transformation of businesses of all sizes, across all industry sectors. At BSA, we undertook a year-long project to work with member companies to develop the BSA Framework to Build Trust in AI,[18] which was released in 2021 and is designed to help organizations mitigate the potential for unintended bias in AI systems. Built on a vast body of research, the BSA Framework sets out a lifecycle-based approach for performing impact assessments to identify risks and highlights best practices for mitigating those risks. Best practice documents, like BSA's Framework, have helped move the AI policy debate forward. But they are not enough, and new guardrails are needed.

We encourage Congress to adopt legislation that creates clear, nationwide rules for companies that develop and deploy high-risk AI systems. Thoughtful AI legislation will benefit the US economy by creating new rules that build trust in the use of AI technologies. It will protect consumers by ensuring AI developers and deployers take required steps to mitigate risks for high-risk uses of AI; and it will set the United States as a leader in the global debate about the right way to regulate AI. The window to lead conversations about AI regulation is rapidly closing, as other governments are moving to shape the rules that will govern AI's future. By enacting legislation, Congress will ensure the United States is not just a leader in developing AI technology but is a leading voice in the global efforts to regulate AI.

AI legislation can build upon the considerable work already undertaken by this Committee in the ADPPA, and by the efforts of governmental organizations, civil society advocates, and industry groups to identify the risks of using AI in different contexts and concrete steps that organizations can take to mitigate those risks. Indeed, while there are important differences in approach, there are also fundamental objectives on which everyone should agree: AI, in any form, should not be used to commit illegal acts. It should not be used to compromise privacy, facilitate cyberattacks, exacerbate discrimination, or create physical harm. At the same time, AI that is developed and deployed responsibly, that improves our lives and makes us safer, should flourish.

I urge you not to wait. You can adopt AI legislation now that creates meaningful rules for companies that develop and use high-risk AI systems, to reduce risks and promote innovation. We encourage you to do so.

A. Congress Should Enact Legislation That Builds Trust in AI.

There will continue to be a range of significant and evolving policy debates around AI. But there's no need to wait to pass legislation that creates meaningful guardrails against the AI risks that exist today. You can — and should — build on existing regulatory efforts by setting rules across the economy to address concerns about the development and deployment of AI systems used in high-risk ways.

We urge you to advance legislation that requires companies to:

[18] *See* Confronting Bias: BSA's Framework to Build Trust in AI (June 2021), *available at* https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai. BSA has testified before the United States Congress and the European Parliament on the Framework.

(1) establish risk management programs to identify and mitigate risks across AI systems;
(2) conduct annual impact assessments for high-risk uses of AI; and
(3) publicly certify that they have met these requirements.

1. Risk Management Programs

Risk management programs establish repeatable processes for companies to identify and mitigate potential risks that can arise throughout the lifecycle of an AI system. Risk management is particularly important in contexts like AI, privacy, and cybersecurity, where the combination of quickly evolving technologies and highly dynamic threat landscapes can render traditional approaches to compliance ineffective. Risk management programs have two key components: (1) a governance framework of policies, procedures, and personnel that support the company's risk management function, and (2) a scalable process for performing impact assessments that identify and mitigate risks of an AI system.

One way for companies to establish risk management programs is by using the AI Risk Management Framework (AI RMF), which was released earlier this year by the National Institute of Standards and Technology (NIST).[19] The AI RMF builds on NIST's work creating frameworks for managing cybersecurity and privacy risks.[20] The AI RMF helps companies incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products. Ultimately, effective AI risk management programs should support coordination across the company, to promote the identification and mitigation of risks throughout the lifecycle of an AI system.

2. Impact Assessments

Performing impact assessments is a key part of creating a meaningful risk management program. Impact assessments have three purposes: (1) identifying potential risks that an AI system may pose, (2) quantifying the degree of potential harms the system could generate, and (3) documenting steps taken to mitigate those risks.[21]

Impact assessments are already widely used in a range of other fields, including privacy, as an accountability mechanism that demonstrates a product or system has been designed in a manner that accounts for the potential risks it may pose to the public. Because impact assessments already exist today, they can be readily adapted to help companies identify and mitigate AI-related risks.[22] In our view, when AI is used in ways that could adversely impact civil

[19] NIST AI Risk Management Framework, *available at* https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[20] *See* NIST, Cybersecurity Framework, Questions and Answers, (discussing federal agency use of the NIST CSF), *available at* https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#agency.

[21] *See* BSA, Impact Assessments: A Key Part of AI Accountability, *available at* https://www.bsa.org/files/policy-filings/08012023impactassess.pdf.

[22] For example, three state privacy laws already require companies to conduct impact assessment for specific activities, including processing sensitive personal data, engaging in targeted advertising, or selling personal data; seven more state privacy laws will soon do so. Colorado, Connecticut, and Virginia already impose these requirements. See Colorado Privacy Act, Colo. Rev. Stat. Tit. 6, Art. 1, Pt. 13 §§ 6-1-1301–6-1-1313; Connecticut Data Privacy Act Conn. Gen. Stat. Tit. 42, Ch. 743jj, Sec. 42-515-525; Virginia Consumer Data Protection Act; Va. Code Tit. 59.1, Ch. 53, § 59.1-575-585. Recently passed state privacy laws in Florida, Indiana, Montana, Oregon, Tennessee, and Texas will also require impact assessments for certain activities. Globally, privacy and data protection laws worldwide use impact assessments as a tool for improving accountability.

rights or access to important life opportunities, the public should be assured that such systems have been thoroughly vetted and will be continuously monitored to account for the risks associated with unintended bias. Requiring impact assessments for companies that develop and deploy these high-risk systems is an important way to do that.

3. AI Legislation Should Focus on High-Risk Uses and Create Role-Appropriate Requirements.

Legislation that requires risk management programs and impact assessments will create new safeguards for high-risk AI systems. Any legislation incorporating these requirements should:

- *Focus on high-risk AI uses.* Legislation should create rules on high-risk uses of AI, namely AI systems that determine an individual's eligibility for housing, employment, credit, education, access to physical places of public accommodation, healthcare, or insurance. These systems have the potential to affect important life opportunities — and are a key area for policymakers to address. In contrast, many everyday uses of AI present few risks to individuals and create significant benefits, like helping organize digital files or auto-populate common forms for later human review.[23] Legislation should address high-risk uses.

- *Recognize the different roles of companies that develop AI systems and companies that deploy AI systems*. Legislation should recognize the different roles of companies that create and use AI systems. Developers are the companies that design, code, or produce an AI system, such as a software company that develops an AI system for speech recognition. In contrast, deployers are the companies that use an AI system, such as a bank that uses an AI system to make loan determinations. Legislation should recognize these different roles, because developers and deployers will each have access to different types of information and will be able to take different actions to mitigate risks.

  For example, the developer of an AI system is well positioned to describe features of the data used to train that system, the system's known limitations, and its intended use cases, but it generally will not have insight into how the system is used after it is purchased by another company and deployed. A company that deploys an AI system is well positioned to understand how the system is actually being used, what type of human oversight is in place, and whether there are complaints about how the system works in practice. Legislation should recognize these different roles, in order to assign obligations that reflect a company's role in developing or deploying an AI system.[24] This approach is not unique to AI, and the promotion of role-based responsibilities is considered best practice in privacy and security legislation worldwide.

B. Congress Can Enact AI Legislation That Builds on and Refines the ADPPA.

We appreciate this Committee's efforts to create rules on important uses of AI technologies in the ADPPA. We encourage you to further improve the legislation's approach to these issues, to

[23] For more examples of everyday uses of AI, *see* BSA, Everyday AI for Consumers, *available at* https://www.bsa.org/files/policy-filings/08012023aiconsumers.pdf, and BSA, Everyday AI for Businesses, *available at* https://www.bsa.org/files/policy-filings/08012023aibusiness.pdf.

[24] *See* BSA, AI Developers and Deployers: An Important Distinction, *available at* https://www.bsa.org/files/policy-filings/03162023aidevdep.pdf.

set new rules on the development and use of high-risk AI systems. Specifically, we recommend the Committee:

- *Continue to leverage impact assessment requirements to promote the responsible development and deployment of high-risk AI.* We appreciate the Committee's focus on requiring impact assessments, which we believe are an important tool for companies to identify and mitigate risks. We recommend improving the legislation by expanding the substance of impact assessments to be conducted by deployers and design evaluations to be conducted by developers. These obligations should be tailored to the types of actions each company can take and the information available to each type of entity.

- *Create clear thresholds that focus the legislation's requirements on AI systems that make consequential decisions*. Legislation should require AI impact assessments (for deployers) and AI design evaluations (for developers) when a system is specifically designed to make consequential decisions, or if a company is using the system to make consequential decisions. "Consequential decisions" should be defined as determinations for housing, employment, credit, education, access to physical places of public accommodation, healthcare, or insurance.

- *Require risk management programs*. It is important for companies to establish the policies, processes, and personnel that will be used to identify and mitigate risks of AI systems. We encourage the Committee to add a new requirement for companies to adopt risk management programs for AI systems.

- *Require companies to certify they are compliant*. We encourage the Committee to include a system of enforcement that requires companies to certify that they are in compliance with their obligations and enables the FTC to review impact assessments and design evaluations as part of an appropriate investigation.

Congress should act now to protect consumers and create meaningful rules that reduce AI risks and promote innovation.

* * *

We appreciate this Committee's leadership on the important policy issues raised by privacy and AI. We are ready to help as you craft and pass legislation. Thank you and I look forward to your questions.

Annex: AI In Every Sector

Improving Healthcare and Quality of Life

The rapid digitalization of health information has created tremendous opportunities for AI to transform how clinicians care for patients, how consumers manage their health, and how researchers discover breakthroughs in the treatment and prevention of diseases.

Helping Pharmacies Redistribute Medication and Provide Personalized Advice to Patients

Walgreens uses the Databricks Lakehouse platform to run an intelligent data platform incorporating AI to forecast demand and redistribute medications across Walgreens' network of nearly 9,000 pharmacies, while delivering near real-time insights and recommendations for pharmacists to help provide more personalized advice to patients. This integrated AI-driven platform allows Walgreens' different data teams to work better together, create smarter algorithms and generate new types of reporting to help managers understand the supply chain, store labor and productivity, patient vaccine scheduling, and prescription pickup processes.

Advancing Accessibility

For people with visual impairments, AI is turning the visual world into an audible experience. Microsoft's Seeing AI app helps people who are blind or visually impaired recognize objects, people, and text via a phone or tablet's camera and describes what it recognizes to the user. With this new layer of information, users can navigate the world more independently.

Strengthening Security

Although data security is core to the management of most organizations, cyber threats continue to evolve at a breakneck pace. AI helps organizations stay a step ahead of hackers by predicting potential attacks, mitigating attacks in real-time, managing access to resources, and encrypting sensitive data.

Enabling Fast Action Against Security Threats

Palo Alto Networks' AI-driven Security Operations Center automation engine, XSIAM, is delivering never-before-seen cybersecurity outcomes. The company's own instance of this tool ingests 36 billion events every day from across all network layers and attack surfaces and triages just 8 of those for human analysis. This empowers their most precious resources — people — to focus on the most sophisticated attacks that uniquely require human analysis. Importantly, this AI-driven tool has reduced overall Mean Time to Detection (MTTD) to 10 seconds and Mean Time to Response (MTTR) to one minute for high priority incidents. This more resilient and automated cyber future would not be possible without AI.

Protecting Business Transactions

Splunk is helping financial institutions to leverage AI and data analytics to strengthen their cybersecurity and their ability to serve customers. For example, consumer report and risk scoring provider TransUnion uses data analytics and machine learning capabilities provided by Splunk to monitor customer traffic and transactions. TransUnion monitors and manages customer traffic to its website and detects when unusual activity takes place so it can alert customers about security concerns and ensure seamless customer experiences.

Building 21st Century Infrastructure

Whether it's creating smarter and safer cities by integrating sensors in bridges and highways to monitor their safety or increasing efficiency by cutting travel time and fuel expenses, AI plays an instrumental role in creating an infrastructure designed for the 21st century.

Optimizing Manufacturing

Generative design tools can optimize the manufacturing process to reduce waste and improve products. Autodesk teamed up with Michigan-based foundry Aristo Cast to develop an ultralightweight aircraft seat frame. The team used generative design, 3D printing, lattice optimization, and investment casting to ultimately create a seat frame that weighs 56% less than typical current models. For a 615-seat Airbus A380 plane, that would mean saving $100,000 in fuel per year, as well as more than 140,000 fewer tons of carbon in the atmosphere.

Streamlining Building Projects

Companies are using AI to streamline the building design and construction processes. Bentley Systems has teamed with Hyundai engineering on an AI system that automates design processes for steel and concrete structures, reducing the time needed to create designs and the cost of building a structure.

Monitoring Vehicle Fleets

Oracle's anomaly detection software uses AI to monitor the operation of complex systems and detect potentially concerning incidents. Transportation and logistics company SS Global LLC uses Oracle's software to monitor their fleet of vehicles and get alerts when there are early signs of potential safety issues. By detecting the early onset of tire baldness and air leaks, the system helps SS Global perform predictive maintenance that keeps its fleet safer and more efficient.

Creating New Ways to Learn

AI applications are enabling personalized learning resources for every stage of life, including adaptive learning programs, digital tutoring, curriculum recommendations, and more. There are more digital resources available to instructors and students than ever before, and AI is affording them the ability to access relevant tools quickly and easily.

Enriching Math Education

Educators are using IBM's Teacher Advisor With Watson AI to access the math resources they need in seconds, including proven lesson plans, activities, standards information, and teaching strategies for students with varying degrees of preparation and ability. This can save valuable time for teachers throughout the school year.

Tailoring Workplace Learning

Employers are using Workday Learning, an application that uses machine learning to personalize workplace learning for individuals, to recommend professional development content and courses based on employee position, tenure at the company, interactions with the content, and other factors. This helps companies adjust learning strategies and programming to ensure employees learn new skills, continue to grow in their roles, and prepare for what's ahead.

Enhancing the Customer Experience

For businesses with large customer bases that are processing a high volume of purchases — such as banks, restaurant chains, and large retailers — analyzing the massive amount of data collected every day is impossible without the computing and predictive power of AI. By using machine learning tools, businesses across a wide range of industries can analyze customer preferences and their own business performance to improve end-user experiences and increase efficiencies. Software also helps businesses generate optimal product designs by using data to produce and analyze far more iterations than humans alone could create.

Customizing Care Experiences

Powered by Salesforce AI technology, Eli Lilly has reimagined patient care with its Patient Connect Platform app. The app helps customers learn to use products, access information about their medications, and record how well they are feeling. The desktop and mobile apps also allow patients to consult with a healthcare concierge — a specialist who provides one-on-one support to guide patients toward beneficial health outcomes.

Improving Customer Service Experience

Zendesk is using AI to improve the customer service experience for both customers and the agents that interact with them. Using Zendesk's intelligent triage functionality, a company can automatically detect a customer's intent (for example, whether a customer is making a return or checking on shipping status), the language the customer is using, and the customer's overall sentiment so that the inquiry can be quickly routed to the best agent for the job. Several of Zendesk's business-to-consumer customers are using this Zendesk AI feature to automatically classify and route incoming tickets to the right agents at the right time, which has resulted in higher customer satisfaction and more one-touch tickets.

Scaling Community Impact

Twilio provides AI chatbot services to help businesses interact with customers. The United Way Worldwide worked with Twilio to help scale and route inbound calls and texts to more than 200 agencies nationwide that use their 211 system to help people locate essential needs like housing, financial assistance, food, childcare, transportation, and more. Using the AI-assisted interactive voice response menu built with Twilio Autopilot, the United Way and Twilio built a system that enables a caller to access a single 1-800 number or be transferred by their local 211 to access assistance. The result is a centralized system that efficiently reduces the call volume nationwide but increases the time staffers are able to devote to mission critical calls.

Improving Business Operations

AI is helping to streamline business operations and increase productivity.

Enhancing Business Functions
SAP provides chatbot solutions that are seamlessly integrated into other business functions, giving customers, partners, and employees a bird's-eye view of business operations. For example, SAP provides software services to Hewlett Packard Enterprise Company, including an

AI-based chatbot system that can reference serial numbers, packing slips, and shipment dates drawn from cloud services, thereby getting the right information to the right people at the right time.

Improving Contract Analysis

DocuSign has been helping organizations use AI-based technologies including natural language processing and rules-based logic to manage and analyze agreements for several years now. Using AI-powered contract analysis can increase productivity in the contract process by helping to speed up contract reviews, increase contract visibility, and identify opportunities and risks.

Empowering Creativity

AI and machine learning within Adobe's Creative Cloud tools help artists, photographers, designers, and content creators around the world handle the time-consuming aspects of their work that can easily be automated, so they have more time to be creative. From removing unwanted objects like mics and logos from videos in Adobe After Effects, to colorizing black-and-white photos in just a few clicks in Adobe Photoshop, to painting with digital brushes that look, feel, and act like the real thing in Adobe Fresco, Adobe's AI and machine learning features empower creators to focus their energy on what they love — ideating, experimenting, and creating.

Helping in Times of Crisis

In times of humanitarian crises, fast response is essential. Researchers are developing ways to use AI to help first responders in the critical hours and days after a natural disaster, and to track pathogens that could lead to outbreaks of disease and mitigate the spread.

Navigating the COVID-19 Pandemic

Siemens' Dynamic VAV Optimization (DVO) is a software solution for building management systems that uses machine learning and AI to configure HVAC controls according to a building's priorities, whether that's minimizing virus transmission or minimizing energy consumption. In direct response to the challenges of the pandemic, DVO was launched with a new operating Defense Mode in late 2020 to reduce the risk of viral spread in indoor spaces. DVO adjusts ventilation, temperature, and humidity conditions to minimize risk of viral spread indoors while also maximizing energy efficiency.

Enriching Our Lives

Leveling Up Gaming and Entertainment

AI can be used to create sophisticated 3-D environments and train autonomous characters in our favorite games and movies. Unity's AI products are used to develop video games, animations, and other detailed virtual environments. By training computer-based characters in Unity's software, game designers can create more realistic environments that capture a player's imagination and enhance the gaming experience.