U.S. Chamber of Commerce Artificial Intelligence Commission
On Competitiveness, Inclusion and Innovation Field Hearing
United States Chamber of Commerce
Washington, DC
July 21, 2022

SUZANNE CLARK: Thank you very much, Congressman. Is everybody feeling welcome? I'm supposed to welcome you. I have several pages here of things I'm supposed to welcome you with, but I think I think I've ingested enough to just want to say this. I really appreciate your leadership and Congressman Delaney, I understand he's going to join us later virtually - is that right? Yeah oh, he's here now? Virtually later?

FERGUSON: He's gonna join us later, virtually.

CLARK: I understand he's going to join us later virtually, and I really appreciate your leadership your willingness to do this, all of the Commissioners.

You know I think sometimes it's so easy to get caught up on the urgent thing of the day and miss the important just all together. And what could be more important than this topic? What could be more important than the national security, economic security, job security of our entire country and of all Americans? And yet it would be so easy to say, 40-year inflation, supply chain woes, you know, war in Europe.

We have a lot to deal with. We'll deal with this another day. And because of volunteers like you, we don't have to wait. A lot of people at the Chamber can do their day jobs and we can be thinking about the future. We can be getting smart about the future, so we're so appreciative of the four hearings that have happened, to date today's fifth, because we're really thinking it makes us smarter.

We can't imagine very many topics as important as this one, right? We're watching what Russia and China are thinking about doing together in this space, then we're watching Europe decide that – as a European commissioner recently said to me, "we're the Silicon Valley of regulation. We're going to get all the regulations right, you know, entrepreneurs of regulation here." And you know we're watching instead of building our allies up and what we want to do to compete and confront in this space. And our allies trying to regulate our industry.

And so really thinking about the balance of economic security, national security, but also growth and innovation. But also, things that have to be harnessed for good human needs and for us to be good global citizens and parents and grandparents.

And so, super complex issue. Aware of how much you're all doing on it. And we're having a Foundation board meeting today in another room, where we're talking about all of these issues, and what is it we should be incubating, and what is it we should be developing.

And I was bragging on you all, that you're over here traveling the country and really hearing from experts all over the place, so that we can at the end of the day make policy recommendations that are good for our country, good for our economy, and good for families, right? Which is really where we're trying to get.

So, I'm going to glance at my notes now and see if there was something else that I was supposed to say while Tom Quaadman glares at me.

Just reading, I know what I didn't say I didn't mention – the importance of intellectual property. But that's part of what you're doing today right? That's part of this particular hearing. It's so obviously really important to all of our members and to people who are willing to invest in the types of technology and innovation. And so, we obviously want to do what we can to protect them. I'm not going to read these stats to you, because you would not be here if you didn't know how important this was, but I will say that I just can't imagine a more important topic.

We cannot do it without thought leaders like you, willing to volunteer your time to do something that's important. And you can count on the U.S. Chamber of Commerce to do something with this. You can count on us to not just produce a white paper but to really turn it into action into work. So I just left one meeting to come over here and to say thank you.

I'm really excited to get to the root of what you're doing. In fact, I don't even know if this is public, but I think we've invited you to present to the Chamber board and forward to that.

FERUGUSON: I don't know if it's public either, but it's on my calendar.

SUZANNE CLARK: Thanks for having me and I'm just next to this other meeting. So if you want me to come back, I could welcome you again. I could come back but thanks so much I appreciate it.

FERGUSON: I'm going to kick things off now. First, I want to thank Suzanne, of course, and the Chamber for she gave a great recap of the work of this Commission so far and a little teeing up of what we're gonna be working on today. Uh, as Suzanne mentioned, this Commission has been hard at work since January, but we've been looking to meet with as many people as possible, different organizations and companies, entities to discuss how AI can possibly impact their lives. And while the public testimony portion of our work is starting to conclude they'll be concluding after today. It's important to highlight how different our work has been.

We've heard from top data scientists and students who are just starting their journey within the data scientist field. We've heard from labor unions, we've heard from civil society groups, we've heard from some of the largest corporations on how they recommend addressing artificial intelligence. We've heard from some of our governments most thoughtful leaders on these issues, like Congressman Will Hurd and Congresswoman Anna Eshoo, Congressman Ro Khanna.

And now we, as a Commission, have a really great opportunity to turn the public recommendations into the commission's recommendations, which I think will help drive our country and drive this technology forward and end up in the right direction. This, this technology is going somewhere and we need to make sure we're driving it in the right direction.

Before we get to that writing, though, we have one last and very important opportunity today to hear from stakeholders on issues, issues around AI governance, intellectual property, and national security.

So our first panel will be on AI governance, and it will allow this Commission to hear more about how AI is looking to be governed and how our policymakers should govern it.

In the intellectual property panel, we'll get an opportunity hear from experts on how we can protect America's intellectual property and assure that we can create an environment that allows for continued investment and innovation.

And finally, our last two panels today will provide us an opportunity to hear from national security experts who can speak about the importance of this technology and how to ensure that the United States is at the leading edge of its development. It's been an honor to help to lead these hearings with you all. I wanna thank the Chamber of Commerce. Of course I wanna thank all of the panelists, particularly today.

All of my all of our fellow Commissioners here who have been working very, very hard and we've been traveling the country and the world, that seems actually we have been and I wanna thank obviously my co-chair Representative John Delaney, who will be joining us virtually as Suzanne mentioned and a little while for helping to make this really good discussion. Taking a quick look at the time, we are almost exactly on schedule and as our Commissioners know from our previous four hearings, probably my most important job in co-chairing these things is keeping us on schedule. So I get to be the bad guy if folks are overtime.

So, I'm gonna try to keep us on time as much as possible, not just because we wanna make sure we're staying on schedule, but because we have specifically allotted time on our schedule and our itinerary of the day to make sure the Commissioners these really, really smart and talented people, get to follow up with. You to ask you questions and. kind of drill down to some of. the things you're going to talk. about in your prepared. testimony. So why don't we get. started? I'm gonna ask you if you can to keep your prepared testimony to 7 or 8 minutes. If you hit that point, I'll give you a very gentle reminder to wrap up and then ideally that will give us time to really get into some questions from some of our Commissioners as well. So, I'm gonna go in the order of.

Panel One

My piece of paper in front of me. First, we'll we will hear from Brenda Leong, who's a partner at BNH.AI. Brenda, welcome floors yours.

LEONG: Thank you very much for the opportunity to be here today. I am Brenda Leong. BNH.AI is a law firm chartered here in the District of Columbia where it is unique among law firms in that it was. It was founded by a partnership between a computer scientist and a lawyer. And this is the only jurisdiction in the country where there is possible, and it was done with the specific vision of addressing AI and algorithmic challenges with the expertise of both of those fields. Since the number one problem and almost any company in governance around their AI machine learning based systems Is the knowledge, experience and communications gap between their technical and data scientists and computer scientists and their policy, governance, legal teams, and how to bring those two perspectives and viewpoints together so that is the work we do and that informs what I'm gonna speak about today. And I'm going to speak fairly fast because I think I was timed for a little bit longer than that. Please cut me off when it's time.

As a society, we have been dealing with algorithmic decision making for at least 50 years. We've been doing it imperfectly, but we do have 50 years of precedent in the employment, housing, financial services, and banking industries to provide a solid foundation of strategies and skills for dealing even with these modern challenges. The second point of that is that it has been imperfect, and there is room for improvement as well as the need to build out those skills to address the specifics of modern machine learning-based systems. Let me walk through this. based on a public site called the AI incident database and other sources. The most common failure modes of AI systems are broken out as follows: Security breaches, unauthorized decisions, privacy violations, multi performance and physical danger. That is safety algorithmic discrimination and lack of transparency or accountability. Setting aside the aspects around the physical safety for the moment, these failures correlate largely to seven identified legal liability areas for AI that all already exist and have legal frameworks built to address them it’s just fairness. You might have heard the quote. All models are wrong, but some are useful. That is true but it also means, by definition that, some models can be biased or inaccurate and harmful ways. ARM tends to focus on already marginalized groups. This can show up in lack of basic access due to the digital divide or to disability-based access limitations, which are not sufficiently incorporated. Fairness harms are further exacerbated by the combined risk of bias and opacity across high impact domains. Credit and banking, criminal justice, gentech, fraud detection, healthcare, and real estate. Secondly, is the legal liability area of privacy. AI requires data which is intention with the tenant of minimalization and makes decisions that implicate a host of privacy laws and Regulations. For security -machine learning-based models have complex involving attack surfaces that create both traditional and new liabilities such as model extraction, membership inference and data poisoning. Transparent in some cases, there are legal requirements to explain how decisions are being made, but without clear guidance as to what level of explanation is required for what public auditor or regulator audience it should be targeted. The concept of agency: Some models are designed to act on behalf of their developers wants to deploy, and this feature is only going to expand as models, programs and robots are more sophisticated. Third parties: where data sharing, and model development can inject new sources of risk. Its unclear implications for liability and traditional negligence meeting reasonable standards of care in designing and deploying AI models. Too many times, we find that organizations seem to think there are no existing legal standards for to meet these challenges. But there are and for quantitative-bias testing for fairness, which is the one that seems to get the most attention, there are. There are plenty of precedents.

Existing legal standards vary country to country, state to state, and industry to industry, but do offer many useful tools for exploring standards and measures in the regulatory future.

Starting this traditional anti-discrimination law, which can be used as a measure regardless of programmers, system AI doesn't start or live in a vacuum. All of our existing laws apply and should be evaluated for use and application for these programs as a level setting exercise for where we go next. BCRA and Regulations along with it and SR 11-7 for model-risk management all have important impacts on the systems that function today and impact evaluations of access, transparency, risk controls and equality.

Under civil rights, law and employment and other contacts for protected classes U.S. law has relatively established rules around evaluations to protect communities. We know, for example, that disparate treatment is spatially unlawful unless or until very narrow exceptions apply. Rest is for impact creates an extremely useful evaluation of systems without having to directly explore the specific attributes of data set diversity or look directly at model code. As for impact substantially different rate of selection and hiring, promotion or employment decision which works to the disadvantage of members of a race, sex, or ethnic group. Therefore, when dealing with-with automated decision-making systems and informed statistical analysis of model outputs, is a first and giant step in identifying potential problems. There are two generally accepted legal measures for such measurement of these systems. The first is the standard for statistical significance. Does a protected attribute correlate to the prediction in a way that is repeatable? But in another way, If I know a predicted attribute like race for a given, sorry protected attribute like race for a given decision. Can I predict the decision the model will make? Test to evaluate this on from the field of statistics. Include the T-test the chi-square test the Fisher-exact test and there are others.

The second commonly used legal rules to evaluate is for practical significance. The difference between protected attributes -does the difference between protected attributes create meaningful real-world inequalities between more simply, if a model does impact protected groups differently, does the disparity amount to real world harm? Are those ports considering practical significance into the adverse impact ratio or AIR test and align it with the 4/5 rule to determine a legally permissible outcome? Other practical significance tests include percentage point differences. The standardized mean difference, also known as Cohens D, which measures predicted outcome scores and has equally established thresholds for allowable differences. At BNH we consider all of these factors and recommend for clients/companies struggling with these systems to build a governance model understand that statistical and practical difference testing can be established to reflect existing legal standards outside of their traditional applications. The exact test depends on the type of outcome, whether the information is discrete or continuous, etcetera.

To build on that, we can add testing for differential validity, which encompasses some newer testing techniques for bias with less legal precedent, but which are more appropriate for contemporary analytics and which we believe will be more heavily relied on by courts and regulators in the future.

FERGUSON: And I'm just gonna ask you to wrap up.

LEONG: OK. In addition to these existing legal tasks, there are different regulatory approaches that offer promise. Model risk management is probably the single other point I want to make today widely used in the financial sector, which offers the best tools and techniques for dealing with algorithmic decision making, and again offers a strong established record of use, trial and challenge that can be considered when expanding it to broader model context and newer industry. Why responsible AI is not working yet? It is too often used as a marketing ploy, where ethics and accountability equal marketing claims. Those responsible for implementing governance may lack fundamental resources like budget and staff, which usually correlates to the fact that teams and management have insufficient organizational stature. There's a misalignment of incentives within both companies, the market and the regulatory sphere, and the tech function usually beats the policy priorities internally, with testers expected to rubber stamp the outcomes. I hope that these thoughts have demonstrated that there is a wealth of existing knowledge, expertise, and legal precedent to leverage and many reasonable tools available to chart our path forward. Thank you.

FERGUSON: And thank you and thank you for being so kind. When I'm being so rude. Next on our panel, I'm gonna go to Evi Fuelle. She's the global policy director for Credo AI.

FUELLE: Thank you, Congressman, and thank you especially for the perfect pronunciation of my name.

FERGUSON: I've been practicing it for a little while.

FUELLE: No, thank you to the Commissioners. Thank you to the Chamber for inviting us here today. My name is Evi, and I'm the global policy director for

CREDO a I would like to thank also my fellow panelists for already a very thoughtful discussion. Our driving mission at Credo AI is to empower organizations to create AI with the highest ethical standards so that they can deliver responsible AI at scale. But we're still a startup. We were founded just two years ago. We are excited to have recently closed our Series A funding round and are proud to be a venture backed company - Fortune 500 customers from some of the largest cloud providers, financial services enterprises, and defense contractors. Our team includes AI and tech policy experts with experience at companies like Google, Microsoft, IBM, and others. Our CEO and Arena Singh was recently chosen to be one of the 27 people appointed to the National AI Advisory Committee to advise the President on the national AI initiative, alongside many of the experts that will be in the room today. with our in-house expertise. at credo, we've built a software platform that sits on top of a customers and loops infrastructure and helps to align both datasets and AI models with responsible AI practices. These include guidelines in this Industry standards, legislation, and frameworks with our assessment model, we help our customers produce information sharing artifacts that create transparency throughout an AI models value chains. You can think of these artifacts as St lamps along a busy St Illuminating specific aspects of the model and the data set throughout its use.

Many companies develop a model and want a simple checklist to ensure that their system is not biased before putting it on the market. To a Brenda's excellent point earlier, at this point, it's usually too late to align incentives for responsible AI development. Instead, we advocate for responsibility to be cultivated throughout the entire development life cycle, for AI. To encourage this, we've built an open-source AI assessment framework called Credo AI lens, which data scientists and technical AI development teams can use to assess their AI and machine learning systems, models, and data sets for different risks. Things like fairness and transparency.

With this framework stakeholders can see technical assessment results in the context of ethical, regulatory, and financial risk. Assessment is a critical foundation for responsible AI governments and development worldwide. We hope that by open sourcing creative AI lens, we can make it easy, free and a no brainer for all organizations to develop responsible AI. Practically speaking, we've developed our own testing methodology based on industry best practices and cutting-edge research as well as the policy ecosystem and distill this into six key tenets which we use to frame responsible AI.

Happy to hear that four of these overlap with those that Brenda has already identified and the tenets that we use to assess our models are fairness, transparency, safety and security, privacy, social and environmental impact, and accountability. Our work is not abstract. We provide real tools to measure these tenets for customers. There's so much conversation about responsible technological development, as Brenda also said, the OECD has over 1000 AI governance frameworks, but we are intent on making that conversation applicable through our product. So going from principles to practice. our platform is simple and practical, and it's a way for companies to have evidence-based governance of their AI datasets and models. We recognize that particularly in this line of work, words matter. For example, we choose to use the word transparency instead of explain ability because transparency is about so much more than explain ability. It includes things like making documentation such as model cards available and ensuring that users from all different backgrounds can understand how a system works. As nomenclature has decided, we urge policymakers to partner with researchers and industry to jointly find solutions that make sense, but good looks like is still actively being defined. In the world of AI governance there is a strong desire to eliminate the black box and create transparency. We have encountered phrases such as readiness assessment, technical documentation, set of guardrails, and certification scheme, all used by policymakers as they attempt to create this transparency for AI datasets and models. We need a common taxonomy in this space, but also one that can be operationalized, which accounts for the fact that AI models are designed and performed differently based on their use cases. Therefore, their assessments and measurements must also vary based on the design and deployment intention for both the data set and the model. One of the biggest challenges to making our responsible AI tenets a reality is the translation process translating high level policy authorship that is already been released into actionable requirements for AI and machine learning systems. We must answer the question how does this tenant actually affect decisions about the development and deployment of the AI system? So this is what we do.

At credo we believe that AI is industry specific, application specific and context driven. We're encouraged by approaches like the NIST AI risk management framework and the UAI Act, both of which align with this view and take context into consideration. We see the UK approaching this similarly also making the case for context in relation to governing AI systems. We’re encouraged by approaches like that of the Department of Defense DIU unit and they're responsible AI guidelines which had the clear goals of being actionable, concrete, realistic. Adaptive, provocative, and useful, which we have already operationalized within our platform. AI cannot set the objective for you. As Cassie Kazakov, chief data scientist at Google, eloquently said. That is the Human’s job. Intended purpose is a key factor for determining how to hold an AI model, and its creators and users accountable. Did the model behave as required by the use case? Is the type of question we ask rather than -is this modeled biased? There is no real view of what good looks like for most AI use cases, and organizations do not know what to measure or how to tell whether what they're measuring is good. We see this happen in industry with many of our customers who are building AI machine learning today. That brings us to what we do as the greatest challenge: moving from principles to practice. We've observed great technical steps forward in explain ability, bias measurement, adversarial attacks, and the security of AI systems. All these technical challenges are real. They are also being very effectively addressed by researchers. I think Brenda made a great point on companies using responsible AI as a marketing ploy, and we have experienced that for every company developing AI machine learning Systems every dollar counts and asking nicely to develop a responsibly Assystem and a responsible a value chain is not effective.

FERGUSON: Maybe, I'm just asking to wrap up.

FUELLE: Sure, so brings me brings me to my final point which-which is that we think the challenge for policymakers is creating mandatory checks for industry which require them to invest in responsible AI while preserving the flexibility that's essential to this field. We think that one way of doing this would be specific and targeted compliance checks throughout the entire AI value chain.

So, I'll reiterate that there's no one metric that's the - the key answer or the one size all fit solution, but we do hope to partner with policymakers as they attempt to determine what works best.

FERUGOSN: Super, thank you very much. Last, on this panel, we'll hear from Evangelos Razis --Is the senior manager at a WorkDay closure?

AZIS: Thank you, congressman, members of the I Commission, appreciate the opportunity to join today's field hearing and to speak on the timely and critical issue of AI governance. My name is Evangelos Razis, I join you on behalf of Workday where I lead federal engagement on AI and data privacy policy. Prior to joining WorkDay I was here at the US Chamber where I was director of

International Digital Economy Policy and Co led the drafting of the chamber's AI principles of 2019.

A software as a service company WorkDay is a leading provider of enterprise cloud applications for finance and human resources, helping our customers adapt and thrive in a changing world. Our applications have been adopted by thousands of organizations in the US, Europe and globally; from medium-sized businesses to more than 50% of the Fortune 500. At workday, we believe in delivering innovation that unlocks human potential and understand the opportunity the AI offers the positively transform how people and organizations operate. Workday incorporates machine learning into our software to enable enterprise customers to make more informed decisions and Empower workers to identify, communicate and grow their job-related skills.

For AI based technologies that have the positive impact that they are capable of, WorkDay believes that we must have a strong foundation of trust, namely trust that organizations are developing and using AI in a responsible manner. A 2021, survey by Axios found that a bipartisan majority of Americans believe that government oversight of the use of algorithms is needed with many expressing distrust in the use of AI to process loan applications, make hiring decisions and drive vehicles. This is why WorkDay supports smart AI policy, which we would characterize as regulation that is risk-based centers on the use of AI impact assessments and recognizes the different roles and responsibilities in the AI ecosystem. My remarks today will briefly discuss these three elements, which are also described in a white paperwork they published last year, which I would be pleased to submit into the record for the commissions benefit consideration. Before I do so, I should share why we believe that federal action Is needed in the AI space, recognizing of course, that many existing mature legal standards do exist as Brenda so artfully pointed out.

Simply put, policymakers in Washington, DC are not alone in wanting to address the AI trust gap. In state capitals and city halls around the country, lawmakers are taking action. Last November, the New York City Council enacted an ordinance regulating the use of AI hiring tools. Similar proposals regulating the use of AI have been introduced in New York State, New Jersey, and California State legislatures, and here in the District of Columbia. Across the Atlantic, our friends in the European Union, continue to develop and refine the Artificial Intelligence Act, which is expected to pass into law. To those of us who follow data Privacy, this emerging landscape sounds familiar. But in lieu of federal leadership, state, and local governments, weave a patchwork of law at home, while the European Union sets a global benchmark for comprehensive regulation abroad. WorkDay is therefore pleased that the House Energy and Commerce Committee took the important step yesterday of voting out the bipartisan American Data Privacy Protection Act. Thanks to recent improvements to the bill, the ADPPA has moved toward a risk-based approach to AI and embraces AI impact assessments. All we intend to continue working closely with the Bills author was the ADPPA represents meaningful progress to the national framework for AI and privacy policy. Such a framework is needed to avoid a regulatory patchwork at the state level and bolsters USAID leadership abroad.

Now moving forward to those three elements will begin. First by talking about a risk-based approach. WorkDay supports a risk-based approach to AI regulation because this ensures that organizations and regulators can focus their scarce resources on the AI applications that pose the greatest potential harmed individuals.

Given the thousands of potential AI applications, each with different risk profiles, one-size-fits-all approaches to regulating AI systems will not work. The risk-based approach to AI governance focuses on the consequential decisions that have the potential to infringe on an individual's legal right to access housing, education, employment, healthcare, and other basic goods and services without harmful discrimination. Adopting a risk-based approach to AI governance is also essential to ensuring interoperability between AI regulations across borders. At Congress' direction, NIST is establishing a voluntary framework for AI risk management, which is scheduled to be completed this winter. At its core, the EU's AI Act also adopts a risk-based approach to governing AI applications. As we have seen in multiple joint statements from the US, UK Trade and Technology Council, Risk Management and serve as a common language for AI governance on both sides of the Atlantic, Bridging these in future AI policy actions. Second, to moving on to impact assessments.

WorkDay also supports AI policies that center on the use of -of impact assessments. Impact assessments are a mature tool already used by organizations for privacy and data protection purposes. Organizations can use impact assessments to identify and mitigate potential risks that can emerge throughout the AI systems lifecycle. It can serve as an important assurance mechanism that promotes accountability and enhances trust that high risk AI systems have been designed, developed, tested, and deployed in sufficient protections. In place to mitigate the risk of harm. AI impact assessments are also an important transparency mechanism that enables the many potential of stakeholders involved in the design, development, and deployment of an AI system to communicate about its risks and ensure the responsibilities for mitigating those risks are clearly understood by all parties.

Impact assessments stand in contrast to other AI accountability tools that have been floated in policy discussions, such as mandatory third-party audits, which require technical and organizational standards to function properly. Indeed, organizations developing and deploying high risk AI systems can carry out impact assessments themselves, and in conjunction with their vendors in a manner similar, to the data protection impact assessments required under GDPR.

Consequently, AI impact assessments offer a way from policymakers to, effectively and pragmatically, address the AI Trust gap today without harming innovation.

As Evi pointed out, it’s a key tool for turning principles into practice.

My Third Point in terms of recognizing different actors in the AI Ecosystem: Building trust in AI is truly a responsibility shared by developers, Deployers and end users of AI. The role of each of these stakeholders within the AI governance life cycle, however, is conditioned by different technical, legal, and organizational considerations which vary from context to context. enterprise software providers, for example, are best place to understand how an AI system is designed, but they typically do not have full visibility into how they're customers are using their AI Tools due to various technical, legal, and contractual limitations, including for data protection requirements.

Consequently, deployers of AI tools are usually better positioned than developers to understand the specific organizational context where tools being used to communicate directly to end users. With that, I want to thank the Commission for their hard work and for-for the invitation to speak.

Obviously, these are issues of high stakes as Suzanne had mentioned and look forward to the conversation with you all and my thoughts.

FERGUSON: Thank you very much. Thanks all three of our panelists. We're gonna jump right into questions. This is not usually a shy group. You got a question, Rachel?

GILLUM: So thank you all. This is all super helpful and interesting. I might have an odd question. Actually wanted Evi and Brenda’s reaction that actually to this suggestion. This-this tension between impact assessments, which I think you're suggesting that companies do themselves versus a third party assessing the life cycle. I just wanted to explore that and get your reaction if either way, you know to-to those, they seem like their opposing.

LEONG: I-I mean, I think honestly, they both have a role they don't have to be externally opposed as in the way that these laws have where it's an independent third party. I think internal audit separately have a role and they could be complementary to impact assessments. Impact assessments tend to be planning and forward-looking audits are more monitoring; and you know maintenance focused or at least can be the-the drawbacks to either especially to being done internally is just commitment and resources internal to the company.

So having any sort of external balance overview of those if it you know validity and-and have asked is I think you know necessary for regulatory standpoint just because not every company will devote the resources or the, you know, sincerity to, to doing them accurately and it's very difficult to do an impact assessment. I mean it's-it's a lot to do. It does reduce the regulatory burden in other ways, But-but it’s not a checklist that can just be done on somebody's desk and half an hour, there's a lot of work behind that to do it well to do it right.

FUELLE: I thought, I think I would just add to that that I think context is key for every type of evaluation and so impact assessments are one way to evaluate different tenets of responsibility for an A system and its model. But I think that they're not the only way and I think that as Benda has illustrated very well if there's an A need to implement different types of checks throughout the entire value chain.

Evangelos mentioned Adpa which has this Impact assessment piece and I think there's still a question of well, what algorithms would even qualify for that impact assessment. I think the-the threshold of acceptability is very subjective and it is very much case by case basis. So, it depends on what the models being developed for and what it's being used for.

RAZIS: Uh. If-if I'm a react little bit- No, it's a great question. And certainly how a lot of policymakers, especially at the state and local level, are thinking about this issue. Do we go for an impact assessment, or do we go to a third-party audit? I completely agree that there are multiple accountability tools that are available. I think at the same time, there is this sort of trust gap, which was right in front of us.

To do audits well, especially if you're gonna include a third party, requires some advanced technical standards. I require some commonality around, what are professional ethics around auditing AI? What are some you know? Are there ISO IAC standards? For example, we see that in the privacy and the cyber security space audits work because they have that pretty balanced and decades long technical underpinning to it to make sure that they're credible. And so I think we sort of recognize that AI is a developing policy area to developing technology. But at the same time, there is this sort of need for federal action to address trust, but also to keep up with policymakers in the state, local level, and our friends in Europe.

FERGUSON: Any questions? Thierer: Yeah. So, let-let's drill down one more layer because obviously all roads in the policy land right now lead to some sort of either impact assessment auditing or is either being called prior informed assessment. So assuming the US does not adopt EU style, more of a top-down approach to audits and assessments. And there is more of a self-regulatory, focused driven or backed by the NIST framework.

What is the output look like? So, maybe Evie you can tell us what your company provides. The end of the day we're gonna be hearing from Mary Vogel later with equal AI is providing sort of a badge program like so there's some sort of a certification that comes out almost like an underwriter's laboratory kind of process, some sort of a stamp of approval. Or is it ISO, IEE, ACM driven, with some sort of professional, credentialed approach to, like, saying you have certified professionals who've gone through it. I mean, we need to know more about the outputs to the extent that we do, not get a more formalistic and regulatory. This what would be the alternative and the sort of ends and outs.

FUELLE: Yeah, I'm happy to react first. I think it's a great question and I think it's one that's obvious from the policy perspective. But when you're looking at the technology, I don't think that there is sort of that one-size-fits-all or the best model. I think test beds, regulatory test beds, regulatory sandboxing are one of the best steps forward to take to ensure that we can look at what-what assessments work for different sectors and different models, because I think it is very context specific and context driven.

So, the NIST risk management framework for example, is a series of tools that can be applied depending on how the model is developed and where it's deployed? Because I-I think again that threshold of acceptability is going to vary based on the use case.

So, I would-I would say there's no one assessment that we would advocate for, but more so a conversation and an-an opportunity for the developers to come together with policymakers to discuss why the assessment is being made. What is the fold of acceptability particular to that use case? I mean, I-I can give many examples, but you know, for a facial recognition system, if you have a threshold of acceptability for a system that's being used to open a phone versus a system that's being used at border control, acceptability and variation of error is very different.

THIERER: When someone goes through your process that you're offering, what's the output? I mean, in a regulatory context, it would be approval. Yeah, right. In a self-regulatory context, it would be what's certification of some sort or a stamp of Approval?

FUELLE: A lot of what we provide is technical documentation. So, artifacts as to how the data set and model are being used.

So, basically an explanation of what the model is doing and how it was trained.

THIERER: gotcha.

LEONG: If I could answer that as well. We do similar types of processes the-the core business that we do is model audits for companies because as-as I described in my comments. Believe and are working with companies that believe that they already have client mandates, but they must be able to show that their model based systems meet in employment and in finance and in healthcare and in these highly regulated fields that we do model audits of their existing systems with the outcome appropriate whatever the compliance category is… we might give them AI identification certification that they can use in an external facing context just if they're operating under HIPPA guidance to say that they Standard (?) Right. The patient's we might give them some sort of internal, but I.

FERGUSON: Folks who are joining online, we've got a large group. If you could do your best to keep yourself on mute, yeah. If you're not being recognized, that would be great. We're getting a little feedback here in the in the headquarters.

LEONG: And when we do an audit based on for example, the anti-discrimination standards that I talked about, we show what the output of the model where the output of the model falls. We might work to mitigate or ameliorate build a legal argument around business incessantly where things don't match up. If that's an allowable context, and then again get them to a point where they can show a performance level to a regulator, to an industry auditor, to whoever that would reflect the performance of their model and that.

THIERER : so issue a public report on that company once they ask for it to show the regulators or others they've been approved?

LEONG: If the company wants that. So-so what we provide can include a public facing piece that can-can have attorney-client privilege waived so that it can be used externally and that's-that's at the requirement of the company.

We've talked to a lot of companies who are starting to explore that option for the New York City law, especially if it gets picked up at the state level by different states as to what that might look like and how we might work with that.

FERGUSON : You wanna address that?

RAZIS: Yeah. Happy to. I think we're very comfortable with the regulatory backstop. Definitely, not a-a sort of pre conformity assessment process, which I know has caused a lot of discussion in the EU about the potential impacts on innovation, which is certainly promoting innovation is a priority a stated priority of the AI Act. And so we are very comfortable with. You know, again, still working out the specifics, but I think we're very compatible with the FTC. For example, with some sort of reasonable grounds, either asking, for documentation if there is an impact assessment, for example, if there's concerns around harm to consumers. But I think that that regulatory backstop is needed to signal consumers signal to the AI ecosystem that there is trust in the process.

THIERER: And that backstio is with existing authority or new statutory authority through algorithmic Accountability?

RAZIS: Uh, I would say certainly not the the-the Algorithm Accountability Act. While that proposal is certainly hasn't some merits. You know, they're-they're in areas that are quite prescriptive and still, you know, needs to be worked out as any complicated piece of legislation oftentimes needs quite a few drafts. That said, you know, I think it is an open question. I think we're still working to figure it out. Like many folks around the table.

FERUGSON: Very-very diplomatic actually like that. Thank you to our first panel. Really appreciate your participation. You're welcome to stay as long as your-your schedule allows.

We wanna take a two-minute break just really to allow switching in and out of from first panel to second panel. But thank you all very much for being here.

Panel Two

FERGUSON: We're gonna try to get started. If our second panel. You probably heard my remarks at the beginning of that panel about how my hardest job is being mean guy who tries to keep us on schedule? In that category, first panel is the easiest because there were only three of them.

If you look around, there's five of you. So we're gonna-we're gonna work even harder to-to try to stay on schedule here. And let me first thank you all for being here. Welcome.

I didn't get a chance at the first panel. I got to practice their names ahead of time. So, this panel did not. So, I hope you'll give me a little extra generosity as I work my way through pronunciations. So, we're gonna get started with our second panel.

I'm gonna go and order of the agenda that's in front of me. Uh, first we'll hear from Rama Elluru. Pretty close. Anyway, Rama is the senior director for society and intellectual property at the Special Competitive Studies Project. If you have other credentials, you're welcome to share them as well. That's-that's everything I have in front of me. But the floor is yours.

ELLURU: Thank you. Representative Ferguson and Commissioners for the opportunity to speak with you today on intellectual property and artificial Intelligence. In the fall of 2019 I was detailed from the United States Patent Trademark Office where I served as an administrative patent judge to the National Security Commission on AI panels here actually and the Congress established NSDAI in the fiscal year 2019 National Defense Authorization Act that mandated the Commission was to analyze and provide recommendations for the methods and means necessary to advance artificial intelligence and associated technologies to comprehensively address US National Security. My colleague and former director of the NSDAI Yuri Bajraktari will give a more in-depth discussion of the Commission in the next panel. The Commission and on AI dissolved last October occur the CONVERSIONAL commissions congressional mandate; in March of 2021, we issued a comprehensive final report that was 756 pages with the chapter focused on the interaction, intersection of intellectual property and AI. I'd like to share the Commission's IP recommendations with you today. Chapter 12 includes two core messages.

First, our intellectual party property regimes are antiquated and need to be modernized in the tech era that we find ourselves in.

Second, the United States must recognize IP policy as a national security priority, critical for preserving America's leadership in AI and other emerging technologies. America's IP regimes, which includes patents, trademarks, copyrights, and trade-trade credits, has spurred American ingenuity since the 18th century. Century with the 1790 Patent Act. The last major overhaul the patent system was in the early 1950s, right before AI emerged in the field. In 1956. U.S. government stakeholders with IP equity spent all three branches, but there's no single federal entity and power to develop comprehensive IP strategies across the government.

The US lacks a cohesive emerging tech IP strategy that safeguards and is integrated into national security, economic and tech competitiveness strategies, so the result is the US could lose its IP global leadership position, including its influence over other countries adopting its technologies. This is especially important in light of China's effort to leverage and exploit its IP policies, which have significant and domestic international implications for the United States.

The domestic harm is that we lack sufficient incentives for IP. The international harm is that the US loses its IP leadership position allowing China to attract in the innovation to its foreigners. Given the global tech competition that we find ourselves in, the NSEa (?) recommended that the United States develop and implement national IP policies to incentivize, expand and protect AI and other emerging technologies. The overarching recommendation was that the President should issue an executive order to recognize IP. As an actual priority and no require the development of a comprehensive plan to reform and create IP policies and regimes first, the executive order should direct the Vice President as chair of the Technology Competitive Council, another one of the NSDAI or recommendations or otherwise as chair of an inner Agency Task force, to oversee this effort. It would also direct Secretary of Commerce, in coordination with the USPTO director, to develop proposals to reform and establish new IP policies and regimes. The proposal should include both executive and legislative actions to achieve these objectives, the Commerce Secretary of the USPTO Director should coordinate with other relevant government entities and convene deliberations and, where necessary, establish a committee of multidisciplinary experts within and outside the government. And executive orders should direct the Vice President to assess which IP proposals come up from the Secretary of Commerce that should be integrated into national security, economic and tech competitive strategies, and, importantly, the Secretary of Commerce should be empowered to implement these proposals.

Lastly, it should direct the executive branch departments and agencies to resource and support this effort as a whole of government approach.

Finally, the NDAI (?) proposed a list not on on-exhaustive list of 10 IP considerations that should be assessed as part of this executive order. Or through suffered prioritization of IP by the White House, Secretary of Commerce and the

USPTO director. The 10 considerations include US patent eligibility, assess and articulate impact of the current United States patent eligibility doctrine on innovation of on AI, innovation in AI and emerging technologies from a national security trade and economic perspective. While China is making it easier to acquire patent rights, US courts is severely restricted patent protection for computer implemented and biotech related inventions. And to give you an example, recently the Supreme Court denied certiorari in a case involving an invention over a-a thing, a vehicle drive shaft that was resilient to vibrations and the courts held that that it was not eligible for eligible for patent protection because it was based on a natural - believe it was hooks law.

So, the expansiveness of the judicial exceptions to patent eligibility has severely restricted the subject matter that is eligible for patent protection. China also has filed massive amounts of patent applications domestically and internationally, and China ensures its presence and standard setting organizations and aggressively asserts its patents as standard essential. We need to assess how we can best counter this narrative that China has won the innovation competition based in part on its patent filings. Three, assess whether the USPTO requires additional resources to ensure high quality patent examination, including assessing the impacts of increasing filings from China and AI generated priorities. Four: assess impediments to the IP contractual ecosystem and proper mechanisms to strengthen the AI Public/private partnership and international collaboration. IP protections for data #5: assess the need for additional protections for data, including legislation if IP protections are deemed necessary, as well as ways to encourage hiring of datasets combating IP theft: we need additional executive branch efforts to counter. The statistics I've seen recently are that 2 billion to 6 billion Dollars of US IP that from China, which is, probably not even really telling of the actual numbers, given that future market effects are also hard to place. Seven Inventorship by AI: Assess the need for policies relating to AI generated inventions and creations. #8 work with allies and partners on global AI related to IP alignment. Nine: we need to expand that innovation base and democratize access to innovation, IP ecosystems. And lastly number 10: standard social and patent process. We need to assess policies to protect the integrity by process of processes by which standards such will patents are claimed, Assorted, and litigated. I'm happy to go into that than anyone on any of these topics. Thank you for this opportunity to speak with you today.

FERGUSON: Very helpful and really on time. Thank you. Next, we're gonna hear from Apollo Tankeh, professor from Bowie State University. Was I close? Close. OK. Thank you.

TANKEH: Thank you, Chairman, and the Commission, for the opportunity to talk here and I said thanks for my panel in here with you today. I've been. In the IT industry for more than 25 years now, I spent 20 years. In IBM, I say thinly pools supercomputer. We had this high-performance computer That the US government always part, not with Craig, IBM, and other American company to invest in it in order to increase our competitiveness. And must say that when I started at a young man arriving from London to Pierre College and Cambridge joining IBM on a team where will sit on a similar table like this, you know that to determine if we will be able to develop a system that will compete with the other system Overseas.

One of the things that you would hardly see will be whether that system will actually make a profit. We know that it would not make a profit that PC computing would not make it profit for IBM and for other companies such as Craig (?), but we didn't know that. What we are embarking on, which usually will take five to six years to build such a supercomputer.

When I joined in 2000, we were working on what you call (?) and we're competing with others in that space to be able to win that contract, and we did not release that machine until sometime 2005. But what we do in such enterprise, including engineers like myself and scientists is that we develop certain intellectual property that and that feels itself in society with that.

It would be hard to expand here, but I usually give lectures to students around when I talk about the next operational system and the history of it. I'm going back to 2000 when the next job started. And I can go and go for a better piece of invention in Linux and then trying to expand it to show how it impacts society in terms of the Commission implication of it in terms of the military implication of that invention and-and so on and so forth.

So, for the course of this 20 years, so competition have been at the heart of my work, I -I started looking at this as a young man when we had similar situations with the Soviet Union, and we needed to develop this weapons system as such as strategic defense measure to. I know that to defend ourselves and we also what that history, it’s all interwoven in some of the work that we've done in developing such systems such as blue gene and such and high-performance computing. They are to be used in commercial. But they also have implication to how we defend ourselves as a nation.

So, the situation we face right now in the competitive space and the IP and also in our own progress with China, is a very serious one. And I-I would just come on in my own reading on the course of that history that what we saw in terms of the standing that we put in RND, in order to create a defensive system that eventually led to go back to our regular agreeing on the table engineers like myself, player match part so but that is some of my recommendations to the Community to also seek out people like myself and others that have some of this history and see some that are going in.

It-it would our relationship with the IP and have AI with China and some of the prospects that we have and-and Russia was one of them with a defensive system which we eventually took off. It took their ways to-to Russia, and they eventually gave up and-and they arrested history today, as you see, the Eastern Europe was able to be liberalized to share similar values like with the share. So that's one of my comments. The other comments I do have is with respect to some of the benchmark that you know Eric Schmidt and other part of other committee that's been looking at-at this issue.

They have been worried that perhaps we don't know exactly where we are with respect to the race with China. - I and this is not new IT. It-it this has Precedent too. So, I think during the-the tool, or they have time when we don't exactly know where they were. The Soviet weapon the kind of a weapon that they have and some of the scientists do during those times have us to be able to find all that technology in order to survey that. But right now it is much harder to solve exactly what China has and what we have and who is actually leading.

So, one of the reasons why that is happening is probably because of the nature which that technology is not open-source technology, which means that when an

AI researcher published a paper, everybody around the world, because of the nature of being, they're being intellectually open source have access to it and therefore they could go ahead and implement it so that. That gives sometimes a new come out, which means like China, a little bit of advantage, particularly because they are coming from behind. There's some advantage that as a newcomer comes in an innovative process that they always have a certain advantage. But is that advantage sustainable or not? That is second questions that you know we don't know that yet. So, maybe some of the things that we're saying it’s a little bit as I whether they actually had.

So, those are still issues that need to be looked into. I could go on other issues equally. Other technology has been coming up to which we also would like to have some kind of speed up in terms of regulation and that is blockchain and integration with AI is becoming very rapid recently, particularly here in the US and other places. China is trying to kind of move it quickly ahead. So, I will stop there, I. No, I continue. If there's any questions, there will be. Yeah,

FERGUSON: We'll-we'll, we are gonna have questions at the end of after everyone has a chance to present. Next, we hear from Wen Xie, partner at Global IP Counselors LLP.

XIE: That's right. Thank you very much. My name is Wen XIE, and I am a US patent attorney and I represent stakeholders before the USPTO as they pursue power protection in the United States. I would like to make a case for why the American innovation system should enable the explicit protection of AI through patents. I will then highlight the existing legal barriers to protecting AI innovations.

First, the reasons we should patent AI. AI is an emergent technology. It is not yet integrated with every aspect of society far from it. The greatest AI experts are emerging in pockets suggest and startups, small companies and labs dedicated to the building and design of AI models. Many of these pockets are not yet known, even in their field of expertise. AI is not yet integrated with the manufacturing industry. Those who makes machines and mechanical parts. The makers of machines and mechanical parts are partnering with AI labs to design their next generation products. Autonomous vehicles, centralized air conditioning systems operated by Internet Of Things Technology. Unfortunately, they're not a big newsletter that informs the tech industry of what everyone is working on.

Companies and manufacturers use patent disclosures to learn about emerging fields of research, determine the best partners who to invest in. The current unstable nature of US patent laws surrounding AI and software inventions overall, has enhanced the risk assessment of companies including small companies and startups when it comes to filing for a patent, should we disclose our invention and research in a patent application Just for it to be immediately rendered part of the public Domain. The unstable nature of the current patent system unduly enhances the risk of seeking a patent. How many efficient cross industry collaborations are we losing out on as a society due to companies choosing to forgo this risk? Particularly for small companies and startups that they have secured more funding? Have they been able to disclose their and emerge victorious?

Another reason to patent AI is that models for building AI are actually being implemented into commercial products throughout several industries. Take autonomous vehicles, for instance. AI designers are working on anticipatory and predictive modules such that vehicles can be more and more capable of independent decisions. To do so, they are building AI models to train AI with all the infinite types of real-world navigation scenarios that may be encountered by a vehicle during use. That is, or to train AI for autonomous vehicles, commercial non-autonomous vehicles for sale are being equipped with the capability to gather information for training AI around the world for sale and public use of an invention while without a patent application within one year of disclosure as dedicating that invention to the public, these AI models would take years to build and perfect, but to get there they need to be implemented with commercial products today.

Again, inventors or companies must assess the risk. Do we invest in this technology that may take years? That R&D investment just for it to be rendered free game for all of our competitors, the American innovation system needs to be predictable and stable to foster the growth of critical emerging technologies such as AI in order to incentivize efficient and worthwhile long-term investments. So, why isn't the current system sufficient? It is well established in patent law to exclude from patentability mental processes. Patenting human mental processes is subject to abuse. However, our traditional perceptions must adapt in light of the developing technology, particularly computer innovations. Otherwise our laws will become antiquated and the field of innovation. AI definition is a computer processing information in a way that mirrors what a human being can do. And the United States computer implemented processes have been deemed mirror abstract ideas that are not subject to patent eligibility. This practice stems from the Supreme Court's landmark case and Alice versus CLS Bank in 2014, and which the court Established a judicially created rule for determining patent eligible subject matter. This case set forth the legal standard that the invention must possess something more than what is well understood, routine and conventional in order to establish the very basis of patent eligibility. Under Alice, claiming physical computer components such as processors, computer memory have been deemed abstract ideas. Under Alice claims to garage door openers.

I'm at this for adjusting the vehicle drivetrain are deemed abstract ideas not eligible for patents. Now, you may say that of course we should not be able to patent something that is well understood, routine or conventional. I agree our country should not grant patents to inventions that are routine or conventional. The problem, however, is that subject matter-the subject matter eligibility statute of 1 of 101 under Title 35 does not provide any basis for the establishment of an evidentiary standard. Section 101 only states whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter or any new and useful improvement thereof may obtain a patent, therefore subject to the conditions and requirements of this Title. But what is the fact Finder referencing when determining when their invention is well understood, routine or conventional? Section 101 is silent with respect to any evidentiary basis for this assessment. To make this point, compare 101 with 102 and 103. The-the statutes governing novelty and obviousness. I'll start with 103. I'm going to be paraphrasing a patent for acclaimed dimension may not be attained if the differences between the claimed invention and the prior art are such that the claimed invention, as a whole, would have been obvious. So, 103 says the fact Finder must reference the prior art to establish the differences. What counts as prior art is established in Section 102, which states that prior art is an invention that was patented or described in a printed publication or public use or sale. Therefore, an examiner can reference prior patents, Prior applications, prior sales, or public use to make a determination of novelty or obviousness. The question of what's well understood, routine or conventional is by its very nature a question of law based on underlying facts, just like novelty and obviousness. Just like novelty and obviousness and must be resolved in the basis of factual inquiries, you need facts and evidence to establish what is well understood, routine and conventional in order to determine what is more than well. It is well understood, routine and conventional, but instead of referencing facts or evidence in the prior art, patent applications are denied as unpatentable subject matter based on nothing but conclusory opinions. And this has been the case from the examining core at the USPTO to the judges on the Federal Circuit. In the past, the USPTO has attempted to rectify this problem, by issuing guidance on the matter. The USPTO subject matter eligibility guidance was limited in its in its effect because the agency cannot effectively set standards for this type of factually based examination under section 101, the agency couldn't just tell the examiners "establish what's routine by referencing prior art." Which is why the question of what is well understood or known in the art is already established in the statutes governing novelty and obviousness. When 103 as properly assessed under the manual patent examination procedure. Obviousness is a factual inquiry subject to the preponderance of the evidence standard that more likely than not, the invention was disclosed as obvious in light of the teachings of prior art references. When the USPTO fails to establish a preponderance of the evidence applicant has grounds for appeal both within the agency and to the Federal Circuit. The USPTOs procedure allows for applicant's rebuttal to prove non obviousness. The procedure allows for referencing commercial success and other secondary considerations. The procedure allows for a process of affidavit practice in which applicants can submit statements from those skilled in the art to establish evidentiary grounds of what is obvious and novel. None that this procedure occurs when a factual inquiry arises under section 101. applicants have had little to no procedural or legal recourse when faced with a 101 rejection. Our current procedure on subject matter.

Eligibility is unfair, it is bad for innovators, it's bad for innovation economy, and it corrodes America's reputation as a world leader. China, so China and Europe also do not allow for patenting mental processes. Yet they do not have a subject matter eligibility crisis as we do. They have allowed for the patenting of artificial intelligence forthright. Congress should amend section 101 to explain stay explicitly That computer structures and hardware are patent eligible structure.

Congress should amend section 101 to stay explicitly that's steps remains carried out by computer structures whether individually or in combination of patent eligible. Lastly on the issue of AI Inventorship, AI should not be inventorship patents. Patent inventorship governs patent ownership, whereas whoever is the inventor is the owner of the patent. So, will the AI be assigning the patent over to a human or a corporation will be the questions that you would then have to answer. Will the AI then be a certain its patent and District Court are the questions you will then have to Answer? Simply the creators, the inventors of AI generated inventions should be the creator or the creators of the AI as they would be the ones who would be incentivized to innovate by patent system anyway.

FERGUSON: Ok, much thank you very much. I'm from New Jersey, so we speak fast. She's a tour de force. It's happening to our force. It also keeps you from being interrupted. It's good. I like that. Thank you very much. Next, we're gonna hear from Andre Iancu

IANCU: Thank you very much. Congressman Ferguson, Commissioners, thank you for the to the Chamber of Commerce for holding this really, really important set of sessions. I'm an IP lawyer. I'm in private practice in Los Angeles. I'm here on my own behalf. Everything I say is they're my own opinions. For three years I was the director of the US Patent and Trademark Office. And I had the privilege of working with Judge Elluru here at my left as well as Mr. Hannah, who I'm sure is gonna speak next.

So, I-I want to back up a little bit and address a couple of the Points that have already been made, number one that we must modernize our intellectual property system when it comes to our official intelligence, and in particular though the question is what to modernize and Miss Xie mentioned, Section 101, that is the patentable subject matter section of the patent code. That section defines what's in the patent system and what's out of the patent system. For example, a machine.

Generally, speaking that's new and novel and nonobvious, we can give it the patent. a painting. It's out of the patent system. We don't give it a patent that section 101, the problem is. That section was written word for word by Jefferson and Madison in 1793, and I'm not kidding. That section has not been re addressed by Congress since 1793, and I don't know if it came up when you were in Congress.

FERGUSON: Hey don't blame me, OK?

IANCU: But it certainly hasn't happened since. And as brilliant as our family founders were. These and-and they were and the patent code that they put in place was fantastic. However, they still did not anticipate DNA processing, artificial intelligence, cryptography, software code, and all of the modern technologies of the Next Industrial revolution, so to say that the patent system, at least from that perspective, needs to be modernized It's an understatement. It is absolutely crucial, and it is a matter of immediate national security.

And let me give a little bit more detail-detail, then explain why.

First of all, what exactly about AI are we talking about? Let me talk when it's when we speak about intellectual Property? Two major categories: first of all, should. Artificial intelligence algorithms be patentable or not- Should they be within the statute? Section 101. But you know, just within the patent statute or should they not be? And #2? Should an artificial intelligence algorithm be allowed to be an inventor of a patent because we are at the day where artificial intelligence programs can themselves innovate and create new things. Should those things created by an AI System, be allowed to get a patent or not?

These issues we are far behind. We must address as a country, because otherwise we're falling behind and it's great that chamber is beginning this discussion now. Now, why is it important to consider intellectual property for these questions? Because in my opinion, in a free market economy, there is no better tool to ensure technological progress. First of all, Intellectual property protections, including patents and and-and the like, incentivize investments in risky long-term technologies were a free market economy, we don't have a centralized dictatorship where the central state can say we don't care what happens in the rest of the country, but you must industry invest billions of dollars in these three, four or five industries. We don't have such a thing and we shouldn't we're a free-market economy. But as a result, some mechanism needs to be in place in order for-for private industry to make these risky investments and be sure that if successful. They will be able to capitalize on them at the end of the road. Second, of all patents incentivized public disclosure. You get a patent in exchange for telling the public how you have done it, so others after you can come and create on top of what you have done and that is the very definition of technological progress. Without it, every new inventor would have to reinvent the wheel as they say from the very beginning. Third, intellectual property and patents in particular ensure the transfer of that technology as misery mentioned the collaboration between various labs, the collaboration between companies that transfer of technology from one company to another so you can jointly create something or to expand upon it. Without it, you don't have the faith that your technology will not be misappropriated.

So, for these reasons without these without these protections, we risk falling behind and in many areas. Unfortunately, we already have. The NSCI reports that Miss Elluru mentioned. You know, identifies that we might fall behind in terms of AI. Depending how you look at it, whether its 5G or 6G or AI or other technologies, we have already began to fall behind and we have to find ways as a nation to-to incentivize those investments, semiconductor Technology, Cryptography, Quantum computing.

All technologies that are super risky, super expensive and have a long-term horizon where our companies need the protections of the law in order to feel comfortable to make those investments and different as the free market economy. We don't address the law struck the legal structure that enables this. We have no other mechanism and we're almost guaranteed to fall behind, so we must right now, as a nation, begin the dialogue on the policy implications and how to balance those policies in order to achieve the right system for our country, and I'm grateful that the Chamber once again is beginning this conversation. Thanks for having me.

FERGUSON: Andre. Thank you very much. Last on this panel, we'll hear from Christian Hannon, patent attorney at the Office of Policy and International Affairs at the US Patent Trademark Office. Christian, thank you. Thank you.

HANNON: Thank you so much for the introduction. Thanks to Chamber and they are inviting the USPTO to speak here today.

So, a key priority for the USPTO is to maintain the US leadership and innovation, especially in emerging technologies and artificial intelligence. To do this, we must incentivize more innovation in areas like AI by ensuring robust and reliable patent rights and tapping into all groups of innovators from across the country. To further this goal, the USPTO has been actively engaging with the innovation community and experts in AI to promote the understanding and reliability of IP rights they relate to AI technologies especially. USPTO has also been working across the agency, government and industry, including through the Council for Inclusive Innovation, to encourage more innovation across the country to promote economic prosperity and US competitiveness, and to connect innovators, individuals, small and medium enterprises and those in traditionally underrepresented communities to the resources that they need to protect innovation and bring it to impact. This past month, the USPTO announced formation of our AI and Emerging Technologies Partnership. We held our first meeting on June 29th. This AI ET partnership as we know it provides an opportunity for independent inventors, small businesses, representatives from academia, industry, federal agencies, nonprofits, and other shareholders to share their perspectives, experiences, and insights, and it fosters opportunities to collaborate at the intersection of IP, AI, and other emerging technologies. In response to our request from Congress, the USPTO also has recently issued a request for comment and published a report on June 28th on the extent to which our current patent laws impact investment and innovation in critical technologies such as artificial intelligence. The report, titled Patent Eligible Subject matter Public views on the Current Jurisprudence in the United States, makes clear that while there are divergent views among stakeholders regarding the Supreme Court's jurisprudence that we've heard talked about here today, technologies that are eligible for patent protection may vary depending on what industry you're in. Therefore, there's general agreement that there isn't a-a key incentive that we need to encourage to innovate and make sure the investments in technologies like AI are there and the laws need to be clear, predictable and consistent as possible. PTO is currently analyzing our own patent eligibility guidance put in place in 2019 to assess whether within the bounds of the law, it appropriately incentivizes and protects innovation in emerging technologies such as AI. With the same goals in mind, we have also implemented a pilot program for the deferred examination of patent eligibility. This program is designed to evaluate whether examination efficiency and patient quality can be improved by delaying the complete evaluation of subject matter eligibility until other patentability criteria

As we heard discuss like novelty and non-obviousness are actually evaluated by an examiner as opposed to addressing all of these requirements for patentability. At the same time, today we have sent approximately 600 invitations to participate in this deferred program and 1/3 of those who have responded have done so affirmatively. We look forward to gathering the data from this pilot program and evaluating how it may inform examination practices, including for patent application is directed to AI and AI enabled systems. We're also considering guidance for patent examiners on functional claiming: a type of claim limitation that describes something by what it does, rather than the actual structural compliments of the invention. This may present distinct issues for artificial intelligence technologies. In addition to the work within our office, USPTO is engaged in international conversations as we continue to evaluate our approach on subject matter eligibility, particularly as it relates to AI. We've had several discussions and roundtables with colleagues from foreign offices, including those in Europe, Japan, Korea and China, to better understand how other jurisdictions are actually able to determine subject matter eligibility.

We have continued those discussions this month in Geneva when the USPTO met with foreign IP leaders at the World Intellectual Property Organizations General Assembly meetings. We are also working with Congress and the US Department of Justices' Office of the Solicitor General to provide technical assistance and other input on patent eligibility. With the goal of creating more certain and predictable rights to the foster innovation, including in the area of AI. We will continue to work with the Solicitor General and her office to identify good vehicles for achieving that objective while pursuing all other options in parallel. We look forward to more discussions on this critically important topic and finding a path forward that will optimize our IP laws as they impact AI for the benefit of our country.

In addition to the need for clear IP laws that incentivize innovation in AI, we are working to encourage innovation in AI across the country, including in communities that have been traditionally underrepresented. And I mean this in the broadest sense, not only reaching out to ethnic communities and women, but also expanding our outreach to parts of the country and among socio economic classes in which Americans have not had the ability to fully participate in our innovation economy. Bringing that innovation to impact is critical for job creation, opportunity, economic prosperity and US competitiveness. To better understand how AI has been diffusing across our nation, the USPTO recently published a study on the growth of AI, as evidenced through patent data. To carry out the study, we actually used machine learning to analyze our own databases. Found that 80,000 of our utility patent applications in 2020 involved AI. That's a 150% increase since 2002. AI now appears in 18% of all utility patent applications received at the PTO, and it's in more than 50% of all the technologies that we examine across the board of PTO. In addition, 25% of those submitting AI related applications are individual inventors. They're located well beyond traditional technology hubs.

For instance, we found that in Oregon, patentees are using AI and fitness training and equipment, and North Dakota AI is being used extensively for new agricultural innovations. Inventors from Maine and South Carolina actively use AI and digital data processing to adapt it for businesses; in Montana is being incorporated into inventions for analyzing the chemical and physical properties of materials. In Wisconsin, the use of AI applied to medical instruments and processes for diagnosis and surgery. And in Iowa, Kansas, Missouri, Nebraska and Ohio, we found that AI technologies are contributing to new inventions in telecommunications. This means we can capitalize in the innovation taking place in all the different industries located in all the different regions of our country. It's not necessarily any longer to be in a long-established tech hub to innovate and attract new investment, which suggests that there may be even more opportunities in traditionally underrepresented communities.

To summarize we cannot sustain innovation around AI without robust and reliable IP rights, which are essential to the prosperity of our innovative nation. To grow our economy and stay globally competitive, we must promote invention and patenting more than ever, including in those underserved communities. Thank you all again for the opportunity to be here today and I look forward to the panel.

FERUGUSON: Thank you. Really impressive panel and fortunately we have some time for our Commissioners to ask some questions. Who’s got a question?

TUCKER: So, the performance of AI algorithms are function of the data. AI architecture itself the hardware and processes. What components of this AI pipeline would you recommend?

ELLURU: I would say all of those components, I mean data is obviously very important to AI and-and there currently is really no effective incentives for protecting and expanding datasets as well as sharing those data sets. How can companies be incentivized to share data sets across public private partnerships as well as across borders if there are new detection for that data as well as those algorithms and Hardware. there is a balance between patents and trade secrets there. It's not a binary decision of whether. We should only have patents or whether we should only have trade stickers shortly. As a balance, there is a place for trade secrets, but we also need the disclosures of the knowledge shared in those patent disclosures to spur innovation.

IANCU: Let me add.

So, I agree with everything that was said. When we talk, we need to think about different types of intellectual property. Patents is just one type of intellectual property. Obviously, we have copyrights, trademarks, but for our purposes here for AI patents probably the most important as well as trade secrets, those two are effectively the opposite of each other, more or less. There is a role for both of them, obviously, but patents incentivize public disclosure in exchange for a limited term of protection. Trade secrets is the exact opposite. You, you it's a secret. You keep it closed within your company. So it is important to have both. For AI algorithms it is important in my view to make sure that if new and novel that the algorithm is subject to patenting in order for the reasons that I said before, to incentivize investment in those algorithms, the creation of new ones and the public disclosure of the algorithms. But to your point, Mr. Tucker, it’s really important to also think about the data. There is actually no intellectual property meaningful there. Let me put it this way, there's no meaningful intellectual property protection. There's no type of IP protection right now in the United States For the data sets that are so critical in training the machines for machine learning and the like, so companies therefore resort to pure trade secrets, there's like they're crown jewels, right? This data, they keep it to themselves. And because of that, you know the big companies that have a lot of data can get bigger and they can get their machines to be bigger.

It's really hard for the little ones to startups, the new brand, new innovators to penetrate that in order to access that data. So I again, this is important in a free-market economy because in centralized economies you can dictate what to do with that data. We don't wanna do that here. So, here we need to think about new forms of intellectual property protection for this data. Not necessarily a patent. Your question, not necessarily a patent. It could be some form of a patent, or it could potentially be a different type of protection for a much shorter period of time, perhaps with different incentives. But that's the type of discussion that needs to happen right away because a little.

JONES: Let me follow through quick. Couldn't licensing and contractual arrangements build part of the gap for datasets?

IANCU: Sure. Voluntary licensing between companies? Sure. But then what's next? If you're a big company. What's your incentive license to start up to? Who might compete with you? How? Having said that, the free market does allow for that to happen and-and it does every now and then, but it's an ad hoc way.

JONES: But if you had a patent, or if you had some type of intellectual property wrapper around that data, doing you still have the same problem? Why would a big company make that data available to the start up? Why would it make it public?

IANCU: You can incent you, have different types of incentives, right?

JONES: I mean, you're gonna get paid for it under a contractor license. You would get and you're gonna be licensing if you're given IP protection

IANCU: So, it depends how you do it right? So, could give you an example from the biopharmaceutical space. A drug has patents on the chemical formulation in the but in addition to that, what drug companies have to do is go through clinical trials. It's a very expensive and they generate a lot of data. There's a separate form of IP that protects that data from the clinical trial. Ok, now what do you do with that data? What do the pharmaceutical companies do? That data is protected for five years for small molecules, for example. Ok, but after five years, that data, which the-the FDA has, etcetera, can be used by generics in order to at the right time Get their Generic product to market quicker. Ok, so now it's that's separate and apart from any voluntary contracts between the branded drug company and the generic Company that is the operation of the law, a set of incentives protection five years with the disclosure obligation at the end of that five years, the benefits society over all of the win/win. Where you strike this balance, what incentives and what protections you have. That's a matter of public debate and negotiations. A similar, not identical, but similar concepts can be had for data sets in the AI world. Different, I want to emphasize than the pharmaceutical world, but it forms an example of what you can do with the data under the operation of law on top of then separate and. Apart from voluntary contracting Opportunities

JONES: yeah, this is a critical issue. And then our very first hearing in Austin, we heard a lot of testimony about the challenge of a startup and the cost to start up to attain data and have the initial capacity to create the need a solution for something, but the data was so expensive and figuring out a national policy around data availability. With getting the incentives in, you know, in a better balance appears to be a very foundational issue, making progress with AI innovation in this country. Otherwise, most of the innovation will come from big companies.

IANCU: And that leads to stagnation and in the long run, because usually disruptive innovation happens from the edge-up … Yeah. And I want to emphasize the critical, urgent need for the country to address this in the face of competition from China. China is not as encumbered as we are with the laws of privacy and data use and the like, ok and. They have other ways in which they're sharing data internally there, and their advances in using the massive data that they have there to train their computer algorithms, their machine learning algorithms far outpaces is what we're doing here, and we need to overcome that gap In our own system, making sure that we respect our sensitivities and privacy laws and the like, that's why we need them legal mechanism.

FERGUSON: Jerry. Couple of other folks looked like they were chomping at the bit to say something about that. Yes, literally jumping out of your chair. Go ahead. Go ahead.

TANKEH: Let me give that question. Is that address that question with a simple use case a simple use case for- Let's take a-a startup that wants to be involved with actually providing storage for data. Ok, now the way that AWS does it with the S3 service, which is that provides, and it gives you an URL and what you have that-that you can put your stuff in there. But you have to pay because you have to have you don't use account. But what about blockchain? In the blockchain scenario, that particular folder we will have a protocol that works that will let anybody to provide that S#. And that is with a blockchain. You create a fast. The same file system that we used to have in IBM to let various nodes on the supercomputer communicate with each other and share that information by throwing that forecast data on many different storage. The same protocol that we develop, which is a lot of money that the US government has spent with us to develop that. No, its simple math, it's. It becomes a problem here. the US government see the ohh.

There are some of this protocol we can engage with university with That is expensive to develop, but where does exist? And that bottom layer is 3/4 American companies for us to be able to use. But any other layer on top of it for any other startup leveraging that protocol. And now that you have their own S3. for there to be able to sell. And it's become the new investment invention because it sits on top of what is already in the barrier of entry, has been lowered by the state, which I think is the model that have always worked historically, and which will continue to work. And so while we are seeing the emerging of Blockchain is that some of this protocol that makes AWS hegemony and-and like that would be make more democratized and then give opportunity for peer-to-peer young startup to be able to have access to include Western Union will no longer be in between. But for example my daughter, I want to send some money to-to-to her in school; I'm already forcing them to use type of wallet that she hasn't wanted. I have a wallet or my; she will be able to. I will be able to just send the money to her just like that peer-to-peer. So, that is one way in which to If you know going back to your original question, which is which layer would be patented, which layer will not all those kind of discussion, it-it had happened in many major lives.

FERGUSON: Yeah. Rama, did you wanna add something?

ELLURU: Yes, correct. That's two data versus software versus hardware that needs to be protected.

Software and hardware have some sort of protection existing data does not have any meaningful protection now. So I would say if the IP considerations that I refer to for IP eligibility would be the number one priority.

HANNON: And I would say data IP protection for data. Some type of IT IP protection for data would be the. If I could underscore that point, we actually undertook a certain public basically back in 2019, I believe issued a report about sort of all the public views that they had regarding what forms of impacts a I had on the IP system. That was one of the unresolved questions that we actually got back from the public was they were all over the place, right, different views on different things. But one of the things that emerged was that is something that we should look at further as USPTO is really investigate, what are we doing in terms of data protection laws in relation to AI systems? The other point I wanted to make was going back to sort of the time between AI and IP is that you get this back to the first panel and regulatory side. I think it's important to call the patents to put pro quo is the disclosure, right? So, I think it goes some way that if we encourage patenting of AI systems, you actually add some value to the societal benefit of the patent and that you have some disclosure of what is actually being done rather than keeping it veiled in secrecy under our trade secret or something like that. So, I think pattern right actually provides some incentive benefit in sort of seeing what an AI system is doing and how it operates.

FERGUSON: This panel is a bunch of superheroes. Your great conversation, great testimony, great back and forth Q&A thanks, Commissioners. And we did it on time. Thank you. That was fabulous. You, you are excused.

We're gonna take a five-minute break and then we're gonna reconvene for our next panel. Five-minute break.

Panel Three

FERGUSON: We're going to jump into this panel. We have four witnesses on this panel. We are gonna try to stay on schedule once again. We've done a good job so far. We're gonna keep-keep at it.

First, on this panel, according to my agenda is Yll Bajraktari, National Artificial Intelligence Advisory committee. Floor is yours.

BAJRAKTARI: Thank you, Co-chairs representative Delaney in Ferguson and commissioners of the US Chamber of Commerce Commission on AI Competitiveness, Inclusion, and Innovation. Thank you for inviting me to speak to you today on AI national security. In case you don't know, from 2018 to 2021 I serviced the Executive director for the congressionally created National Security Commission on AI. Congress established an NSCAI, the Commission I led in the fiscal year 2019 NDAA, the NSCAI. I was an independent federal Commission with a mandate to consider the means and methods necessary to advance the development of AI and associated technologies to comprehensively address you US national security. I'd like to emphasize to many audiences that we were not commissioned to look at the app for humanity or for economy. We were specifically looking at AI for the purposes of national security. The Commission was led by the former Google CEO, Dr. Eric Schmidt, and former deputy Secretary of Defense Bob Wood. The Commissioner on AI, dissolved by statue last October, put the Commission's congressional mandate. In March of 2021, we issued a comprehensive 759-page report, but I'm gonna leave with you. That provides a blueprint and a strategy for the United States government to lead and win the global competition for AI national security.

Today, Congress has already moved to legislate more than 50 recommendations based on our report. Let me take this opportunity to provide a high-level overview of our main conclusions and recommendations before turning to my fellow Commissioners to discuss different topics in more depth. We reached a few overarching judgments. Number one: our government is not organized or resourced to end the technology competition against the committed competitor, or it is prepared to defend against AI enabled threats. #2, our nation must be AI ready by 2025 to defend and compete in the coming year of AI accelerated competition in conflict. We build the final report in two main parts, part one defending American in AI era is about how the United States government can responsibly use AI technologies to protect the American people in our interests. It focuses on implications and applications of AI for defense and national security. Part two winning the technology Competition, recommends government actions to promote AI innovation, improve national competitiveness and protect critical use advantages in the larger strategic competition with China.

There are four priority areas where our government action. Number one: is leadership. We need organizational structures to accelerate the government's integration of AI and the governments promotion of AI across the country. They should include a technology competitiveness council at the White House, and I can elaborate on that further. Second: Talent, we have a huge talent deficit in government. We need to build new digital talent pipelines and expand existing programs more broadly we need to cultivate AI talent and nationwide-nationwide and ensure that the world's best technologies come and stay in our country. Third: hardware. We're too dependent on Semiconductor manufacturing in East Asia and Taiwan in particular. Most cutting-edge chips are produced at a single plant separated by just 110 miles of water from our principal strategic competitor. That is unacceptable. We must revitalize US cutting its semiconductor fabrication capabilities and implement a national microelectronic strategy. The goal should be to stay two generations ahead of China in the state of art microelectronics. Fourth: Innovation. AI Research will be very expensive. We need the government to help set the conditions for broad based innovation across the country. That should include a national AI research and infrastructure, and we should reach $40 billion in annual funding in the next five years to cover AI R&D for defense and non-defense research. Finally, 2 themes cut across all report. The first is partnerships. We need to build coalition with like-minded nations to advance the development and use of AI and other emerging technologies in ways that support democratic values. 2nd is we need to do in a responsible way in the face of digital authoritarianism, the United States needs to present a democratic model of responsible use of AI for national security. Public trust will hinge on justified assurance that our government use of AI will respect privacy, civil liberties, and civil rights.

We have a set of recommendations to help ensure that they're all in our book. Before I close, I'd like to take a moment to underline the importance of leading in Afor national security and put our final report and recommendations in perspective. The implications for our national security when China or any other authoritarian model sets the standards and rules for emerging technologies are rather severe. Who the leaders are in emerging technology also matters? Tech leaders, tech leadership means setting the rules for how they're used, controlling the infrastructure for they use building the indices of the future and fielding the best militaries to protect our societies. The first mover advantage in technology is enormous. It is important for our country to be in the lead of China because this is a values competition. We want these technologies to be developed according to our norms and ethics, which is the antithesis of how China is using it against their citizens. Up through surveillance, oppression of their minority groups. When we don't have these democratic partnerships and dialogues, China moves ahead and sets the standards. 5G is a clear example of when we were absent from these forums, and we didn't have an alternative approach to China that has what happened. That's why China has said their standards on how we should use these technologies. I'm happy to go into more depth on any of these topic areas during our conversation. Again, thank you so much for the opportunity and I wish you all the best.

FERGUSON: Thank you very much. Next on this channel will be Terry Roberts, founder, and CEO of White Hawk.

ROBERTS: Thanks for having the hearing. Glad to be here. I come at artificial intelligence from a military intelligence graduate student of the 1980s, a Navy captain who ran scientific and technical intelligence for the Department of Navy and led an intelligence community of interest of the first implementations of AI in the 1990s. An IC see executive who ran the general Defense Intelligence program, the Military intelligence program, and the former deputy Director of Naval Intelligence. And then went on to be the executive director of Carnegie Mellon Software Engineering Institute, an industry VP for Cyber Engineering and Analytics, and then started my own company that is AI based global cyber risk analytics online platform six years ago. When I entered the intelligence community in the early 1980s, we owned drove an advanced, a huge sector of the computing power and data sets. This started to change in the 1990s. The.com and the worldwide web. Still, I don't believe the national security arena fully understands that innovation in the data and analytics space is driven by global industry, R&D universities, and startups. That's where data and analytics innovation is born Every day. I lived this transition, and I can tell you that I am still very engaged with our national security arena, and they don't get it.

As you know, staying ahead of national security and global risk dynamics and issues is all about connecting the dots, in order to tell us a complete story as possible and optimally provide decision advantage to key stakeholders. Such as a warning of an impending event, analyzing or quantifying risk in order to mitigate it, and near real time. AI based algorithms and models are a means to do that automated and at scale. As many have published, automated decision making, Adm, involves the use of data compute and algorithms to make decisions across a broad range of context. Data from a range of sources such as databases, text, social media, sensors, images, speech, and the World Wide Web. While I have spent decades on global risk and national security. I want to focus today on the love of my career since 1998: cyber risk, resilience, and operations. In this arena, publicly available data sets are rich, broad, easily accessible, and very telling. As a Cyber intelligence executive, I have seen capabilities dramatically advance over the past 20 years and especially in the past five years to where my company and our amazing partners and compete-mates, can assess any legal organization in the world regarding their cyber threat landscape, key risks, maturity, compliance and generate a foundational action plan mapped to solutions and best practices and all I need is their legal name and URL. It is nonintrusive. This is the result of dramatic advancement of AI based analytics across a global breadth of data sets across millions of businesses. It provides a 60 to 80% perspective of that company or organization, all automated and scalable and empowering for that company regardless of the level of cyber sophistication. And we know this because as a part of my business model, we have interacted with thousands of these companies after we run the assessment.

So, we have the ability to drill in and validate our findings, in a unique way. In addition, three years ago, we conducted a proof of value across the US energy sector, 3400 plus public and private entities, and demonstrated the power of placing AI driven cyber risk management frameworks across an entire sector. The findings, down to the individual entity level by region, subsector, or size. Frankly, it is the only way you will ever gain real insight into the risk and maturity profiles of 90% of all companies and organizations because they don't have CIO's and Csos, they don't have in-house expertise and resources. Last month, in fact, the Board of Governors of our Federal Reserve System put out a cyber-risk monitoring market survey for implementation across 5000 U.S. financial institutions. This would be brilliant, cost-effective way to enable the resilience of all for individual bank assessments can be shared directly with each bank and the portfolio trends can be shared with all, helping to prioritize initiatives and limited resources. And the portfolio analytics could be shared with the financial sector ISAP (?) as a hacker view of their sector, cyber risk, and trends. One of the key limiters to achieving cyber resilience is adoption across all. These kinds of methodologies could empower individual companies and organizations to own their cyber risk, share their cyber risk rating and reporting with others as they do business. In closing, a few challenges that I have encountered. The acceptance and mainstream integration by the US national security community of Commercial best of breed risk analytics. Many of the companies are Represented in this room, but in addition, companies like Graphica, White Space Range, Geology Act and Taras Black kite. They are the mainstream, main commercial, unclassified analytics and data sets that don't use national sources and methods but can form the foundation for all of our national security analysis and assessments. Two: US and allied patent constructs for AI based algorithms.

Everybody was singing my song earlier. I have invested $2.5 million in RND in our research and in our platform and have been banging our head against the patent pending wall for several years now and this is what we're told -- that our algorithm save man years in time and effort, but don't optimize compute power and as a result we can't get the power. That is, and happy to go into details at another time with all of the patent legal paperwork behind it. And then lastly, systemic protection of our most advanced algorithms from foreign adversaries.

My entire career, I've had to think like a bad guy. I take for granted that every one of our commercial companies and all of their algorithms have been stolen by the Chinese. Its, it's-it's cotton candy, they're not protected. So, along with everything else we've discussed, I think we do need to discuss are there some key jewels of the Kingdom that have to be encrypted, you know, and-and what is the construct for doing that; so that we can truly protect what is giving us our analytic advantage in the national security arena. Look forward to your questions.

FERGUSON: Terry, thank you. Next is Benjamin Harvey, founder and CEO of AI squared. Alright.

HARVEY: So, so kind of looking around here, its-it's really an honor to be in a group of such amazing, amazing, prestigious individuals. I'm so again, my name is Benjamin Harvey. I'm the founder and CEO of AI Squared. My company will be the first joint agency CRADA cooperative research and development agreement organization between the National Security Agency and the NGA National Geospatial Intelligence Agency. Or I will trustworthy AI as well as AI integration. OK. We are a Silicon Valley startup, we are, you know, top tier VC investments from new Enterprise Associates on our way to Series A with trying to catch you out there. That's Ok. We'll talk later. We we've got customers and we partner with the likes of Microsoft, Salesforce, and video data bricks as well as contracts from DoD, the joint Official Intelligence Center. Our mission is really, you know, and I'll talk about this in a second, but it's really the simplify and accelerate the path of integration into currently existing mission applications. So a little bit about my background. So, I’m a three-time HBCU graduate, Historically Black college, and University. Have a PhD in computer science. I did my postgraduate research at Harvard and MIT. They have the joint program that's focused in Health Science technology, where I focused in on large scale cancer genomics and applying machine learning algorithms to those types of data sets. I'm a professor at George Washington University, right down the street. And I'm also an appointed professor at Johns Hopkins University where I helped build the COVID-19 risk tools that have been used by three to four million Americans. I worked for NSA for over a decade, as well as the CIA. My last two positions were. I was the lead data scientist for the Edward Snowden leaks and an organization called the Media Leaks Task Force and the Corporate Disclosures Action Group. My final position was the Chief of Operations, data science, over at the National Security Agency. I ran an organization called the Operations Data Science Hub and we really had two areas of our mission was to scale machine learning.

So, you know, think about machine learning algorithms running at scale across the large-scale repositories of collection that's coming into the agency, but also the intelligence augmentation, right.

So, this is really, you know, enabling not only the embedding of the machine learning results into the applications, but also making sure that the results are actionable, relevant. Timely, and there's contextual information that's associated with it so that when you have the intelligence analyst and the military warfighter that accusing that data, they can report on it, it's-it's effective for decision making. So, I, I'll tell. I'll tell. I'll tell a little story. I-I think this is a-a really good opportunity to do this so. I, I've got two brothers, and, and I apologize if I get a little choked up here.

FERGUSON: Not counting this against your time. Getting extra time.

HARVEY: One’s a captain and -and one is also a major in the US Army. They're both deployed to hostile Middle Eastern territories. They both are affected by the deployments, both mentally and physically. And, you know, all I could think about was when I was at NSA, I was the data science chief and, I couldn't get them. There was no one from our data scientists into the applications fast enough. And all I could imagine is if-if we would have been able to do that, we would have been able to, you know, prevent some of the injuries and save lives. Not only to my-my brothers, but to the other military warfighters. That were in hostile-hostile territories.

So, when you think about the greatest challenges, I'll talk about them and it's really a couple of things.

So, thank you, Sir, for the analysts and the-the war fighter. It was really the inability to get models. So, these are the results from the from the data scientists. So I had an organization about 40 data sciences. So is the challenge was getting the results of the models into the application fast enough so you could build a model. 90% of these models are sitting on the shelf and they're not never making it into a mission production application, right? So, when you have military war fighters and the intelligence community analysts that need to utilize the results of those machine learning algorithms, we couldn't get it fast enough because the time and the cost that's associated with the integration, it's just too much. On the organization, regards to the IT component to be able to get the results, instrument the applications, add the buttons you know, do the intelligence augmentation as needed in the application to make it actionable to relevant contextualizing information. Because without the contextual information about the explain ability the analyst won't trust the results and and-and-and the results will never get into a report, right?

So, you're trying to go through the entire process from collection all the way through reporting to dissemination. They don't trust the results if they don't have it in the application that's in their workflows, right? So, these are the applications that the analysts use is they're-they're one, two or three applications. And that's all they use. So, if you build a one-off capability that they have to jump outside of their workflows, they'll never use it, right? Mm-hmm. Because a lot of the mission work that they do is its-it's-it's extremely timely, right? So, what we're focused on at AI squared is figuring out how do we get the results of the machine on your models into the application and also making sure that it's augmented in a way where it's ready for reporting. Ok?

So, so-so you think about all the collector comes in, right? If There's Olsen. There's ELAN (?), there’s FISO(?) There’s COMET (?) Communications, intelligence. You're- You're bringing that collection and you're transforming it, and you're doing one or two things, right? You're building a machine learning model or you're building a rules and a lot of times, these rules engines are utilized because the old GC needs attribution, right? Because there could be catastrophic. First, second order, 3rd, 3rd order effects. If there's a bad decision that happens. Ok, so, and then it finally. What? What-what? What's very important is that there's kind of a-a couple of stages here.

So, there's a cost and time that's a challenge. You know the the-the results that are embedded, the machine learning that's embedded in the application, it doesn't support decision making. That's another big one and then the final thing is really the contextualization, like the-the background information I called the why behind the KPI that the analysts needs in order to report against the intelligence that they're collecting. Ok.

So, so how do we solve this, this-this last mile problem, right? So, what our company is focused on is-is really reverse machine learning, right? So it's one thing to build these world class models. What we're seeing is that 90% of those models are sitting on the shelf, right? So then how do you reverse the process to take the results of the models or the models themselves to be able to take the results and transform them and map them in a way that they can be easily injected into the applications, ok? But it's also the intelligence augmentation like like-like I said before. We had an analyst; she came to us. She said she gave us four criteria. We-we lived by this. You can ask my wife, my head of field engineering over there if-if it's not. Actionable if it's not relevant. If it’s not timely, and if it doesn't have contextual information, she told me, they won't report on it. Period. Right? And that means that there are people out there right in the field that aren't getting the Intel that they need because of the inability of IT organization to provide it in a way that they feel they-they have trust, right on what they're reporting on, right.

So, they need those four criteria and that's really the intelligence augmentation. So, it's how you need it, where you need it, why behind the KPI as well as making sure there's timely. And then the last two things, so it's the value of the models. There's a huge emphasis on technical accuracy, but there's not an emphasis on the impact and the value that the models are having across the organization, right?

So, if-if you understand the performance but you don't understand the impact that it's having on the organization, you'll never increase AI adoption, right? So you'll never understand the-the level of engagement, the level of productivity, the usage of the AI capability across the organization, which is really important and is necessary for an organization to adopt the machine learning. And the last thing is the human machine teaming for trust. Right? And this is the-the final recommendation.

So, its, it's-it's we're focused on making sure that the tools are instrumented and when I say instrumented, it's the implicit and explicit behavior of the end users in the applications, right? So, that you can understand that and then as they are creating the-the data as far as the usage you're reporting that back to the data teams so that they can update the performance, but they can also tell the organization how impactful and how valuable the models really are. And it enables the organization to focus investments because if you understand the impact, you can focus the investment on the model and say, hey, we need to scale this. Otherwise what I've seen is that there's a lot of top-down Identification of machine learning capabilities that need to be used, but you need to hear it from about a lot more perspective. You need to hear from the organization that's important.

So, if you instrument the tools, it gives you a better understanding of the level of engagement, the productivity, the usage of the capability and that can inform investments for the organization. So thank you.

FERGUSON: Thank you very much, Benjamin. Important powerful stories and examples for us. Last on this panel is Brian Drake, the federal chief technology officer at Accrete AI Government. When Brian is done, we're gonna have some time for questions for this panel. Some of our Commissioners I know haven't had a chance to ask the question yet, so I'm gonna try and prioritize you if you haven't asked a question yet, so get ready. Be prepared. If you want, Brian.

DRAKE: Thank you so much. Yes.

So, I'm Brian Drake. I just left a 10-year career at the Defense Intelligence Agency. I ran a number of AI projects while I was there. I was an analyst first and foremost. So, I worked counterintelligence, counter narcotics, counterterrorism, and emerging and disruptive technologies. Did that for majority of my career. Two of those years I spent as a director of artificial intelligence at DIA. I ran a $20 million portfolio and countering measured the challenges that then described in trying to transition technology to folks that actually needed to do the mission. And then the last year of my time at DIA, I was running the briefing team in the Pentagon for Secretary of Defense, Deputy Secretary and Under Secretaries of Defense. So other E-Ring principles. So I am also equally humbled to be here today. I really thank the Commission for the invitation, and I hope I have a message that resonates. And I really just have two things I want to share.

The first is that when we think about this space from a national security perspective, at least when I think about it, I think it is a full spectrum attack on our country. I think it is an unrelenting deluge of activity against our most precious assets. And when I think about it that way, it makes the second point that I wish to make clearer. If we do nothing, we risk losing our economic and national security competitiveness across the board without question. And I'll give you a couple of examples of that.

So, when I talk about a full spectrum attack, what am I talking about? I'm talking about all the instruments of national power from our adversaries being directed at all-of our national security instruments and economic power centers. That means their intelligence apparatuses. That means their direct and indirect funding apparatuses. That means they're commercial military integration activities. All of those are being directed toward artificial intelligence. And make no mistake, it is about winning the future war. That is all they care about.

So, from that departure point I wanna drill into those three areas. The first is wanna talk about intelligence. So, when we think about China and Russia, they have three primary ways they go about doing that. The first is they use economic espionage, they use force on the inside, they use tools to steal from traditional human tradecraft that happens at the time. They also use a fair amount of cyber theft, and Terry was going... [web disruption]

FERGUSON: If you are joining us virtually, I just ask if you keep yourself on mute until we, perhaps, recognize you just so we can. We're getting some feedback here in the main conference room. So, thanks very much for keeping yourselves on mute for now. Thank you. Bye.

DRAKE: So, when we talk about cyber theft, I wanna use a case example. Cyber Reason, which is a cyber security company based out of Boston, they did a study on something they called Operation Cuckoo Bees. Can't make it up. And looking at an attack that occurred from 2019 to 2022 by what we think is a Chinese Cyber activity called APT 41. They discovered that there were hundreds of gigabytes of data being stolen from North America, Europe and Asia. That data included things like, you know, actual property, blueprints, diagrams, formulas, all things that we can be using for national security apparatuses. All of which were under consideration for patent or prepatent. Right? They estimate and it’s hard to understand kind of how much we're talking about because it is patented technology.

So, it's a future projection, but they estimate that we're looking at about $225 to $600 billion of wealth gone in 2-3 years of activity. This is one example of what General Alexander describes as the largest transfer of human wealth in history, and it's all going to China, ok. That's just one example.

Here's an interesting coincidence. In 2019, China surpassed the United States in international patent filing. According to the World International Intellectual Property Organization, and even at the height of COVID, when everybody was home in a country that was foreign quarantined and arguably more grossly affected than most countries on the planet. They surpassed our lead again by 17%. How is that possible? I have a clue. I think it's because they're stealing our intellectual property and doing a copy paste into the patent system. Now these patents haven't been legally challenged. I'm sure our counselors that were here before would probably say there's a long road to home. It doesn't matter. They have primacy and private mover advantage. So, in a court of law, they can continue to infringe on all of them intellectual property. They can continue to issue technology without restraint and our industry falls behind.

So, I absolutely echo the AI recommendation that we need to treat IP as a national security asset. Second thing I want to talk about is direct and indirect funding. From 2010 to 2019, one of our competitors, called Govini did study of supply chains across the Department of Defense. They estimate that over that period of time, there's a 420% increase in Chinese investment in the-their budget. That means that they are starting to put their tentacles into apparatuses that are not just what we're doing in predesign, but actually at the manufacturing bit. And so they can't steal it they will change it at the back end to affect battlefield operations. That comes through lots of different ways. One of the primary ways is through venture capital money. Then they can they get that venture capital money on the table that allows them to get access to intellectual property, seat board members, have sway over boardroom strategy, and it has a direct effect of what we do in the government. And I speak from personal experience, working with a lot of Silicon Valley units out of the defense Intelligence unit. When we found a company through vetting that had some sort of degree of Chinese venture capital, we walked away. We walked away because we knew that that encumbered us with other headaches, concerns, that we wouldn't be able to [unintelligible]. That is a strategic win for the competitor. That means I, as a government buyer in no longer going to get access to that technology because it's already in the hands of the Chinese, at least it's safe to assume it is.

So, what is our competitive advantage in that? And let me tell you that investment was $100,000. Pocket change, pocket change. But we have to take them seriously. Third thing. Civil military integration. This is not a new phenomenon. The Chinese Government, the Russian Government, our government is integrated very tightly with our military enterprise, right. Our defense contractors, of course, you know, make a lot of our technology The only reason I raised it is because China and Russia's rules around this are much more fluid. It's a bigger gray space. We have rules, we have contract processes, we have budget authorizations and then appropriations. We know where that money goes. We know how it gets directed around. We don't understand that fully in China and Russia, it moves very fluidly. So you might have a company that has a joint venture with the US company, and you might see IP move right across the street. So going right into a technology difference area application. That is particularly acute in artificial intelligence, and why we need to pay attention to it is because what we are seeing is artificial intelligence technologies transiting not just intelligence processes that we're doing in the NSA, but lethal systems. They don't care about having a person in the loop to make a lethal decision. We care about that. They are deriving competitive advantage by taking that person out of the loop and being able to backward faster than we can. And that's an ethical issue for us. We will not - I hope - we will not take a person off that lethal loop. I hope I never see that. Our adversaries don't care about that. These are people that bomb hospitals, ok.

So, I worry about joint ventures. I worry about where that money comes from. Also worry about the rise and strategic doctrine and academic literature about the degree to which an integration is occurring.

There's three things I wanna talk about in terms of actions that I think that are within our realm.

FERGUSON: If I can just ask you to.

DRAKE: ...very fast, very fast. So, first is outreach. I think that a lot of folks in industry who are on the cutting edge, especially small businesses in the valley, they don't understand what we're talking about. But even start talking about how you need to think about where the money comes from. That's a very unusual conversation. They won't understand it - primarily because if someone comes to you and says I have $3 million, I'm ready to give to you. You don't ask a lot of questions to be able to make payroll this week. So, we have to think about that. And I would say you should focus on something like the FBI's office of the private sector. They have a mission to do outreach, but most of it is focused on counterterrorism and like national events, like NASCAR and Super Bowl. You probably want to broaden that to focus more on legal protection. Second thing is education. I think we need to stop pretending that the thousands’ talents program is some sort of economic program for the Chinese. It is a veil, not even veiled. It is an open program to take our talent from the United States cultivated in our universities and moving back to China. That means we need to have a series of changes around how we think about granting student visas and who comes back. I've already talked about venture capital money, but there is an initiative in the DoD called the trusted capital digital marketplace, which allows VC's to lobby for access to become a certified venture capital provider to DOD systems. And that has a degree of trust. Kind of this under(unintelligible) laboratory and trust stamp. I think that should be expanded across the whole government. The last is, this is our opportunity to punch back. If we are not investing in programs that kick China in the teeth. I don't know what we're doing. I just don't know. That's how they're thinking about it. We should be thinking about it the same way, which means we need to change our immigration rules and get the most talented folks they have to come over here to get training and get education and keep them here. Do not kick them out, do not send them back. It also means we need to better protect things like our dissertations that are sitting on shelves where they get copied by foreign nationals and then sent abroad. Last part is, I think we should empower industry to partner better with government to go after our adversaries. Industry is the first canary in the coal mine to know when something bad has happened, whether that's a person that they found out was working for the other side or whether it's cyber attacking infrastructure. Industry will go first. But we're not allowed, we're very, very limited in our ability to affect that in the various (?) sector. Thank you for the time.

FERUGUSON Alright, thank you. Thank you. This whole panel for you can't ask a question. You. No, we got plenty, ok, so go ahead. Hit it

MESEROLE: Yeah. Well, first of all, I just thank you for a great fan out. Almost wish we could spend the whole afternoon on just this. I think there is. But so I guess I'll just kind of have two questions. One would be for you Yll the PDF was you know the physical copy is downright daunting for bringing it with you. As you mentioned you know, I think Congress has taken up something like 50 recommendations. There's now that we're kind of a year out from when it was released. I'd be curious to hear from you and just like what are the recommendations and if you had to prove our test and that haven't really been addressed yet, then you see still kind of low hanging out? And then the other question for the-the rest of the time, I think one of the common denominators among all of the experiences you've had is this issue of integration of a kind of a startup company in the private sector trying to interface with the government. Which of the difficulties and bottlenecks there Which of those are kind of policy or regulatory that kind of we could offer, you know, suggestions about how to ameliorate or if it's kind of investment or you know what is the pain point that I think it is most central that and-and that needs to be Resolved?

BAJRAKTARI: So, like working for the government?

MESEROLE: Yeah. Yeah. Like we have great private sector kind of startups and as you're trying to interface with the government, what are the payments that make that's all the go ahead first Chris.   Thanks a lot. Thanks for all the support.

BAJRAKTARI: Provided in Brookings during the NCI days, I would say three recommendations that are highly think we need to prioritize in the next fiscal year would be: number one is Brian really depicted the whole competition with China in a way that I also Indicated in my opening remarks were not organized or resource to go after this competitor. And so this has to come from the top. And so when it's when I say it has to come to the top, it has to come from the White House.

After World War Two we created the National Security Council because Soviet Union and particularly the security was the primary threat we faced was Soviet Union. I have the Cold War. We created the National Economic Council because economy became the seven peace of our competition. I believe technology is the central competition. AI is fundamentally the center of that technology. And if we don't place it at the highest levels of our government, we will still not be organized. Every department and agency will do their own thing, but we will not have that coordinated approach and organizational structure to go after a competitor that Brian depicts so well.

So, that's one is TCC technology competitive and console It's bigger than just a folding it, Chris under NDAA, we were tasked by NDAA so this is a bigger recommendation. The second one, the two, the two other ones are really related to people again or advantage over China or people: how do we create a talent pipeline for our federal government to have access to these technologies really matters, because at the end of the day how we get organized, how our military operates, how our intelligence community operates really depend on how fast we bring these technologies to help our military.

So, two recommendations to that end: number one is we recommended creation building the US Digital Service Academy, all the military academies have their own educational systems or federal government doesn't have access to any kind of Academy where they can hire talent, run out of college, and keep them for five years until they pay back their time. So, creating a civil service Academy that are focused on educating young people on technologies is a key is a fundamental thing we have to get it right. And then the last thesis is we recommended creating the National Digital Reserve Corps. All the military services have reserve corps. We talked to a lot of photonics in Silicon Valley, a lot of them want to help our government, but they don't want to leave the private sector jobs.

So, what is a middle way you can create for them? You created reserve program where they offer two weeks a year to our government, their services and this will allow you to have high end access to the best technologies, people that don't wanna leave Apple or Google or Facebook, but they wanna help HHS. They wanna help commerce or DoD for that matter.

So, creating a civilian digital reserve corps would be my third biggest item that. I would like to move in the next fiscal year because these three ideas will really get us aligned and organized towards this competition that Brian spoke really well about.

ROBERTS: If I could talk to the federal government, national security procurement and contracting out trust, right? It was designed for fun tracting (?) in the 1940s and 50s and 60s. That flip I told you about, you know where computing and-and technology is driven by commercial industry and the R&D universities you-you have to spend millions to know what's going on in the national security arena from a Requirement, request for Information, market surveys request for proposals. You know, even someone who ran a $21 billion program Right? (unclear) Ok. In my last company I had a $45 million budget focus on knowing what the heck was going on in the national security arena. Who's paying for that, the US government? How stupid is that? So many of these requirements are ubiquitous, so you could, if there was a consistent way to get out those requests for information market surveys, request for proposals more OTA's, other transaction authorities that are quick turn, then commercial companies could play in that mix and they don't need to know who's asking for it, right? It could be CIA, or it could be the IRS, right? It doesn't matter. Opening that up would change the dynamic of federal government access to commercial innovation and save billions of dollars in business development and sales BS time. I don't feel strongly about it (laughter).

DRAKE: I really don't have time because he's-he's in the middle of it right now. The only thing I this is just my opinion. I'm not a big fan of procurement reform. I think our contracting off, I started in contracting is where federal job, I think a contract specialist contract officers have every instrument they need to access industry. It is not a question of the rules, it is a question of the right person and the right place saying yes and it's not just the contract, it also the GC’s, the lawyers. Yeah. Guys like that they have to be in a position to say this is in the interest of the US-US government and here’s why. they have to be, well, conversion of that. I think a business advocate inside of agencies would help. I think that that is one of the things. I was in an innovation shop at DIA, and they would always kind of cock their head and look at you strangely when you say, well, I think that's (unclear). These are our partners. Like we don't succeed without them, and that was a very different view than most things in the NCL. One of your experience with? Yeah.

HARVEY: And, and so I-I see really 22 core areas. One is we think about people in a sense, right? So a lot of you know investors right that are not focused on investing in dual purpose technologies, right?

So, these are technologies that will provide value for industry as well as the federal government. They will not let you focus on the federal space until you hit 50 to 100 million in R (?) it just can't because the time it takes to get a relationship in the federal government all the way through to working through the-the policy, the compliance, the governance, the security, all those elements, you will burn so much cash that you will not be able to survive, right. So, the-the opportunity with a company like myself is a cooperative research and development-development agreement, which is a research contract with the National Security Agency and NGA, right? So, so literally and our investors, you know, you know our flavor, we come from federal government, so they understand where we're coming into the startup game as a dual-purpose technology. So, they have more leeway for us to work with the federal government to burn cash servicing federal government needs, but The challenge is really getting through those hurdles of the technology processes to get the tech inside of the door, but you also need the champions on the federal side, so the creator for us is a way to engage. We've got the head, the, the, the lead for trustworthy AI from the agency on our research team, right? Same thing on the NGA side. So it's an opportunity to-to kind of understand the needs of the agency to incubate your technology in a way that it could service and address those Needs, but it also provides that pathway. Two integrations because you're working through policy compliance, governance, security challenges as you're incubating our technology.

FERGUSON: Shakur got time for one more question for you.

KATURI: I wanna take it back to a little-little basic level. Umm, if I connect the dots between this session and the earlier sessions, the earlier sessions argue that if you cannot make the data available- so AI is on top of Data-, if you cannot make the data available to a lot of people, the innovation is gonna be so. So that's a very strong or. On the other hand, you're walking in here and saying hey, this is a national security, you have to be really tight about where that data goes. sitting on this side of the table, how do you find the right balance in driving innovation by making data more available to those who want to innovate versus how do you balance that against national security? Your thoughts- Roberts: So publicly available data today is 100-fold of compared to national sensitive sources and methods data, right? So what I was trying to get across in my original discussion is start with that publicly available global risk data because it's 100 fold of what we can acquire in the national security system. So, that should be open. But then once you have sensitive sources and methods sets right and maybe comingled among people, then that has to be protected for national security reasons.

KATURI: So basically arguing that we need to look at data sources causing a public completely made available, including China. By the way once you open it, it's done. Mm-hmm. And then identify across the board in the country. When I say across the board, private sector, the banks that I belong to right now, banking data to sit with the public services there. Everything that's. National Security Ministry protectors you were tagged along the way. That's what I'm getting. I

ROBERTS: I believe so. Any of that, but please other thoughts.

DRAKE: Yeah, I think that data…understand I'm coming from a perspective that was about combat effectiveness. So what I think about this type of issue, I think of data as a battle space.

KATURI: It is.

DRAKE: I think that. There is competitive advantage in which we derive from having access to data and there is competitive advantage we derive by denying the existence of data.

So, and I'm primarily thinking about. The egalitarian ethical thing to do would be to democratize data and let everybody see it. My opinion is that you are not entering into that game with an ethical fair player. That player is gonna do things like repress other people with that information. And so I believe it's an Interest of the US government not to be a party to that activity. I think we should be blaming and shaming our adversaries for doing things that we find in moral and ethical, and we should be taking that high ground and I'll attack on top of that. We have friends they don't. We need to be more tightly coupled with our Five Eyes(?) partners, our partners in Africa, our partners in India, are partners in Eastern Europe and we need to get in we need to be more acceptant of the advantage we derive by allying against our adversaries. We do not do an effective job of this. I'll illustrate one point: Where is China focusing the most activity in terms of international developments? Not at the stump the chump question. To Africa, Africa forever. We have a body now in the CDO that organizes our international competition on AI and includes some of the countries in areas I mentioned. The only continent not Included is Africa… why are we ceding what our adversary views will be most important strategic battlegrounds for them, to them?

FERGUSON: We're going to have to wrap. Fabulous panel. Thank you all so much for both your testimony here, but also for all of your work outside of this room. So thank you for spending time with us today.

Panel Four

FERGUSON: First up on this panel are 4th and final panel of the day. Collin Carroll, director of Applied Intuition.

CARROLL: Thank you. So thanks for the opportunity to testify today, guys. You don't know me. I'll start by saying I'm not a policy person, right. I'm an engineer. I found myself sort of in the Marine Corps, and then I was a senior executive at the joint center mentioned which by the way, it's not. They're kind of international competition. Uh, I-I ran punch maven, which some of you guys made heard about some news. I ran an atomic program for the OSD – a SAP program called SMART Sensor, That I left just recently as the head of development for the joint Ad Center, now in an industry I've run the government team at Applied Intuition, an autonomy company. Do you see back small business in Silicon Valley and we're here in the DC Office .my approach to the next industry AI and national security stems from my observations over the last six years, both in government and now out of government. So lots of reports have been spoken and written about a new study I brought my Hard copy version of Yll's final report there. Yeah, 700 plus pages, 340 recommendations. I'm not gonna try and sum it up, Yll did a good job summarizing his findings. I think I'm gonna try and focus on an issue that I'll say it's like big and national security, IE resulting in like big P policy which is required in order to set the stage like the next 30 years o- of American National security. So I think since we're all here and you guys invited everybody, like we'll stick to soon, that we all think AI is important and relative to national security is critical not just by itself, but also in the form of it's like applied use, which is really automated systems and autonomous systems. I think it's gonna continue to revolutionize industry and military operations. And I think that we probably would agree that the nation that best capitalizes on the employment of the applied uses of AI will be most positioned to optimize the domestic workforce, deter aggression, and then dominate in conflict. If we ever get to that point. Underlying truth, it kind of came out in the earlier panel from explicitly stated here. So in software technology in general and in AI software, it is 3 and not the Department of Defense, the-the research institutions that are really leading driving innovation. I think specifically that's Silicon Valley. And it's offshoots in a couple of places in the country. The duty research enterprise plays a role, but it's not the tip of the spear like it was 30-40 years ago. And, so, what does that kind of mean for the US? I look at like the this and kind of three building blocks. So on one side, you have talent not talking about talents like in the Department of Defense talking about broadly speaking the talent pool of technical people in America. I think there's technology development, which is really the tech itself plus the investment required to build it. And I think there's a how do you get to technology into the department of defense now like I could literally spend all day talking about the last point about acquisitions reform. And I completely agree with Brian when he says that contracting officers have every tool TIGRIS has authorized us to do exactly what we need to do in the Department of Defense. We just have people that don't. They're not educated, they don't know, or they're scared. So I'm going to focus on the 1st area, which I think is like the foundational component to this whole thing, right? If we don't have the right people, then, then everything falls apart. We can talk about like fixing microelectronics or actually some form or you know creating more bureaucratic leadership structures and investing $40 billion. I can tell you like if you gave my company half billion dollars a year, said go fix AI for the for national security, but we'd have the talent, it would be completely irrelevant and not worth our time.

So, the nation like any Team organization succeeds or fails space and the people who are in it. For those of you guys who know me from my DO days, you know that I say people are the most important thing hands down in any organization. That's the bottom line is our national security depends on our ability to attract nurture. And retain technical talent, and without this talent pools of foundation, everything else is kind of irrelevant. You know, it’s a technical fields, it's math and computer science, right, software engineering. And so not everyone wants to do that. And then some people that wanna do it aren't gonna become world class at it, especially here in America. Talent is fluid. It'll shift locations based on really, I see it's three things: right?

So, education job opportunities and quality of life. So, I think we the United States need to provide these things better with other places in the world in order to sustain that out here. So, that means tackling third real topic of immigration reform. So, I heard someone saying was Brian said earlier about like restricting student visas, I mean he said in one sense restricted student visas. The next sentence he said. But we need to, you know, have better resources, let me tell you what, like-like people come here to go to school. Why? Because we have the best institutions with the best instructors, and we're incentivized by grants from federal government. That's why they come. That's how they get here to start on the whole. Then they go on and they get degrees, and they work, and they-they end up having to go back a lot of times. I know my company experiences this right now most of the work that we do is one commercially focused on the autonomy industry. It's not two defenses focused That's why I take half of our small businesses, probably foreign nationals, ok, and they end up going back to where they came from. So unfortunate. Uh, I think we still in America have world class instructors. We still have a cache at schools like MIT, Stanford, Berkeley, they're centers and innovation. I do think if we restrict this talent pool and that, you know, there's all sorts of people writing and talking about this Down's gonna give somewhere else studying research, then these structures will follow and then the grants will follow. Everybody wants to supervise the best researchers and best academic students, and that's what's going to happen.

So, I think if we enact Nativist immigration policies for even the status quo that we have now I really do predict it by the end of the decade, the transition of the AI education and research power base to basically China, India, that'll be complete and it's gonna be really, really hard, if not impossible, to overcome that. I think the-the nativist policies that restrict workers is the same, same issue. So in Silicon Valley. Foreign work is what we survive and thrive on like Silicon Valley would not exist if it was just, you know, guys named Colin Carroll graduating from wherever and trying to work in Silicon Valley software engineering. It's just not, it's not accurate. My fiancée, she emigrated from Ukraine at age 17. She's now a technical PM for Azure federal for Microsoft. My CEO emigrated here from Pakistan when he was five years old. He's he managed a billion dollar, multi-billion-dollar Unicorn startup that's really driving innovation in the autonomy sector. You know, these are just 2 analysts I don't have, like, an army of researchers or, you know, like binders and statistics. I didn't do any Googling here, but I-I do think my observations are really will be backed up in in fact. Uh. I think the bottom line of this kind of end this way at the bottom line is that we need immigration reform, ideally bipartisan, that prioritizes incentives for foreign talent to attend school, to conduct research, to work here and to become really U.S. citizens. I think a lot of the-the, the I would call fear mongering, but a lot of the cause it is true, right? I mean there are students who come here, there works to come here, and they leave with the IP. They go back to where they came from either go to foreign company, they go to state-owned enterprise, or they go back to intelligence service, and they-they give our IP away. That is a massive problem. I think the-the solution is problem are probably more counterintuitive, definitely controversial than people think, and it's really how to incentivize people to stay here as a citizen. That might involve policies like-like the family plan for citizenship, right, which is get the-the. The leverage that China, for example, has over a student or a worker’s family and just eliminate that leverage, there's a lot of times. That's why people go back. There's a whole lot of reasons about quality of life and kind of like America that there are policy problems. But I think in general, most people would say it's better here than it is other places on the planet.

So, I'll just end by saying this. I think that we need bipartisan immigration solutions now with respect to tech talent, you guys, I don't know, maybe, maybe not. Maybe I'll age myself here, but you get the dog in the in the house fire meme everyone knows I'm talking about or the dogs. Like everything is fine like to me, we're-we're at that moment right now. We just might not. And my biggest fears of taxpayers like waking up three years from now, four years from now and it's too late to recover this. My big fear as a company is as well, right. We wanna continue driver 350 people. We want to be 650 people. In the next year. So I appreciate your time. Thanks, everybody.

FERGUSON: Colin, thank you very much. Next, we'll hear from Sean Gourley, founder, and CEO of Primer.ai… Sean.

GOURLEY: Hey, thanks everyone and thank you for-for putting this session together and for the other speakers that are joining me today. I think it's, you know, obviously been a huge amount of discussion about the impact that AI is gonna have, but I think we've actually underestimated massively the impact that it's gonna have in the world of warfare. And I think the biggest impact actually that artificial intelligence will have in the next decade will be in the world of defense and intelligence. And the reason for that I think is what we're looking at without official intelligence is really what's known as third offset. The first two offsets being nuclear weapons and stealth weaponry, right? Where an offset in conflict renders aside that doesn't have this technology effectively obsolete. So when we sit here now, I think it's-it's important to kind of look back at the last two offsets, nuclear weapons, end of the Second war. Second World War and precision guided munitions and stealth weaponry rendered the US against the 6th largest army at the time the Iraq army. Rendered the conflict over and about 72 hours.

So, as we look at this, my position is that our personal intelligence will actually have a bigger impact than those two combined. So, if you look through this is not a hypothetical discussion. This is not something that will happen in the future. We are already seeing artificial intelligence play out today on the battlefield and

Ukraine. And this is something that's really emerged from the ground up, its people sticking computer vision on top of homemade drones with homemade grenades looking for image classification of camouflage vehicles and dropping bombs on them. It's artificial intelligence listening to all the radio transcriptions, combining those with object detection and social media videos and. and real time information about the exact movements of Russian troops and of course the impact that official intelligence is happening today on a very, very important part of information operations. The battle for the hearts and minds that different populations, the manipulation thereof. So, we're seeing that here today, and it's important to recognize that Russia nor Ukraine are neither AI superpowers. China is an AI superpower, and that is where we are gonna be very much in an arms race for this next decade. And as we go back to this thing, the third offset the winner of this arms race will determine the political landscape of the world we're in. It's that serious.

So, as we look at this, I think part of this is to come and say, well, what are, are we sitting at right, I think look, the United States and its allies have huge advantages today, but this is not gonna be one on the advantages we have today. It's gonna be one on the speed that we move, and China is moving very, very quickly. We talked about AI in the abstract, but I think we should talk about it in the components that make up. And, for me, I'd like to frame this with four different components. The first of these are the algorithms is the neural Nets that we're very familiar with. It's where a lot of our focus goes, but there's three other components. It's also the computing resources. And it's the training data of these systems are trained on top of, and finally it's the deployment that we can put these things into actually the hands of our warfighters.

So, let's start with the first of these ones. And algorithms really, I think US does have a clear advantage. I think a friend he had talked about the power of the-the research institutions, the power of the R&D labs that our companies have. But again, that is changing quickly. When I started Primus six years ago, we'd pick up our research papers in about 1 or 2% of those would be from Chinese institutions. Fast forward today. The research papers that we take that have significant results that we use to look at commercialization, about 20% of those now come from Chinese institutions. They are moving quickly. So, we've got the advantage but China as closing. And the second component which is computing power, right?

The computing power that drives and trains these algorithms. This is largely graphics processing units and GPUs. the US and Taiwanese companies dominate the space at the moment and indeed China has massive issues Here -Only about one in 20 of the chips that they consume internally are produced internally. They have to import those chips. This brings Taiwan very much into the front and center of the space, Taiwan. If you don't know produces, 92% of all the advanced processing chips in the world, and if China were to take Taiwan, it would leapfrog forward and its capabilities to produce things with the very least that would render our ability to utilize those chips have been put that into a significant disadvantage. So, we're gonna see a battle at the chips, and I think it's best to consider this: You would never start a war previously without any energy independence. We're never gonna start a war in the future with our compute independence. The third is data and we talk a lot about data, but I wanna get very precise on this, specifically human labeled data. It's the data that has been labeled by humans that allows computer vision algorithms to determine whether or not it's a tank or a missile launcher to function. These are subject matter experts that are literally drawing boxes around different objects by the 10s of thousands and allowing the computer to know what they know so they can the computer can operate at a scale and speed that they can't. Now as you look at this, the labelling capacities actually are Huge because it-it takes 10s of thousands of labels to make these systems work. When you look at that, it's also crucial to have this labeling on tap, because whatever algorithm you go into a conflict with your opponent is gonna try and deceive that. We're already seeing experiments with China painting tanks. Yellow and black to try and confuse them, to make them look like construction vehicles. These are adversarial opponents that are looking to defeat the AI that we're bringing to the table. So it's not just about labeling, it's about having that labeling on tap and ready to train algorithms quickly so that the system can learn from that. China has a huge advantage here. They've already got a massive army, the $0.50 army of people that are there basically determining whether or not things are you should be censored. They can be very easily repurposed to train algorithms. And they are. And the final bit of this is-is actually I think the most important. And that's the deployment of-of artificial intelligence. I thought you can have all the advantages of compute data people, but if you don't deploy the AI then it's of no use. The deployment is crucial. Getting into the hands of the soldiers, gamblers the operators is really what we hear about and the and the reality is we're in a world where have the procurement cycle that has got all sorts of problems. The speed of that is the major problem and whilst the three-year procurement cycle for a new jet fighter may be fine a three-year procurement cycle for a new AI system renders the system that you put in place. Obsolete by the fact that it's three years old. The system moves so quickly that in three weeks you can be out of date, and if we can't move faster than three years in procurement, we are gonna be fielding AI that is obsolete and that just is not gonna be acceptable given the importance of the space that we're in. Yeah. So the speaker deployment is-is crucial. Umm. And there's bits of that where you see as a company that had just incredibly frustrating. You can go through this and you're seeing just archaic regulations and you're wondering why that these things exist. You're also saying procurement cycle that is longer than the runway of the startups that are supposed to be going after it. If you're a young, innovative machine learning company, you can literally solve anything in the world. People will pay you to solve any problem you're gonna come in and say we're gonna solve the defense problem, but it might take you three years. You say I don't have three years of time. I've got two years and I've got to show progress before I can get my series basic four day. So the deck is just literally stacked for insiders, it's stacked for the big contractors and those that have the time and the space to never create, navigate these bureaucratic regimes can weigh out the contracting process and ultimately are putting in a place where they sprinkle a few buzzwords or an application. They pick up the dollars because they were the ones that were there. We need to make this more and more accessible for the best and the brightest minds and make this something that our technology companies want to be part of.

FERGUSON: Sean, can I just ask you to summarize.

GOURLEY: yeah, and it's all summarized here, but we're head and people. Which is good, you know, and the algorithms they go with that I think China has the advantage when it comes to labeling where hid when it comes to the GPUs and the chips. But I think we're behind when it comes to deployment, which is the most important piece of this.

So, I think we need to do a lot better because we've it's not a race that we can end up losing.

FERGUSON: Thank you. Thank you very much. Next, Ryan Lewis, partner at SRI Ventures. I'd like to thank the members of the Commission and the US Chamber of Commerce for the opportunity to testify this afternoon, us, my name is Ryan, Lewis from SRI Ventures. That's the corporate venture arm of the SRI International. For those of you that may have heard of it, that maybe it's a notice of fresh memory as which was former Stanford Research Institute to nonprofit organization that focuses on advanced & public and private sector use cases. Since our founding in 1946, we've been involved in creating a wide variety of Silicon Valley innovations, including the computer mouse, which people the office still mock me. If you're using, I'm powerless, here are up in that and more recently serious now. Apple's virtual assistant you have about 1700 researchers and scientists that conducted about 1000 projects a year, ranging from Bioscience to computer science. On the venture side, you know, we specialize in commercializing deep tech innovations that come out of the lab. Majorities if you look at our portfolio, are AI technology. Right, beside it takes the form of creating new companies and building entrepreneurs and venture cap around that or transferring IP into existing startups. My comments today, I'd like to consider how in some ways, and we fit a little bit on it already, the old has become new again and I'm not referencing Tom Cruise in the new Top Gun movie. Great movie, more-more importantly I'm referencing the challenges associated with performing our policies and strategies to better leverage dual use technology. You know, as early as the 1980s, Jack Gansler who was an executive at the Pentagon and went on to lead acquisitions under Clinton ministration, he wrote quote, you know, we have "to find and implement ways to strengthen the US economy through dual use investments in security and economic growth "and quote right. That was over 40 years ago. And this topic came online. And the problem that he was thinking about wasn't AI, but it was similar today where he saw a majority of innovations that were occurring Because it helps leverage the defense industrial base happening in the commercial sector. And, what's interesting enough is in the NSCAI found a report. It identified AI as the quintessential-duties technology. And so while the disruptive effects of what we've been talking about today are perhaps new, right in the American experience, the strategy and challenge or the strategies and techniques that maybe we used to resolve them are not and perhaps we can leverage some lessons learned from the past. And so to perhaps help realize this or like to offer three considerations: Point number one- is we should work to leverage some of our existing R&D and mission programs in both the DoD and the IC. You know, a lot has changed since Alice? net one image net in 2012. I remember when I was, I was working any can tell. We first proposed to launch an open-source computer Vision lab. This was tied closely with some of our Members in the IC. In terms like training, data volumes, data labeling schemas, evaluation metrics were not a term of art right outside of like a couple core groups. Now their mainstream lexicon that whether or not they're being executed in the best way, we, the best or most efficient way, that's a different story. But the concepts are there and some of the program funding is there. Right, our goals. Initially we just launching the lab, we're more modest- introduce these core concepts of practitioners, see what fits, and builds, start building relationships. Today the environment is much different. Yeah. On the one end of the spectrum, we have numerous multimillion dollar programs focused on deploying AI capabilities in scale, right? Aren't being commercial needs from these end users and programs include making the systems more cost efficient, optimizing them for promote performance against different use cases, integrating them with the existing toolkits. Because how many times have, I heard analysts don't want another UI to look at data and harden them against adversarial Perturbations. These programs, which are already funded, already working for better or for worse. It should have the flexibility to experiment with best of breed solutions, whether they arrive from current providers- i.e. contract winner or the sub subcontractors under that. Or they're completely new entrance, right there. Have some best of breed that have passed and evaluation criteria. In Brief, we have these large programs they need to be flexible enough to address the technical dynascism and that we're seeing in the market today. And yet, interestingly, in the other end of the spectrum, there are a wide variety of R&D programs and research initiatives, both in the public and private sectors, right, that are already developing the next wave of technologies that would fundamentally disrupt the very architecture we're trying to build now, right?

So, as we talk about ML operations at scale and making it more efficient, we also have research that's saying what if we built a large language model that disrupts the need for some of this complex? That we're trying to deploy in the 1st place? This is to quote the NCI(?)This is uncharted territory for us.

And so we actually have a dual problem right in the acquisition world, the trying to deploy what we can now and making it efficient and why they put these here are helping do That, then simultaneously figure out what's already coming next. Because the chain motivation occurs much faster, right than perhaps past technology's work. But 2nd is miss some we've already heard today, so I'll keep my comments brief Here, is just increased market access and transparency. I've worked with a lot of a startups and entrepreneurs over the years and a lot of interested right in pursuing dual use businesses, even if they're not fully aware of what it takes and they're gonna a lot of innovations on the acquisition front for rapid procurement. We've already heard about some of them today, but then we hit the inevitable What's next question? When those programs reach their life cycle or the companies as well as companies, do they wanna grow, and they ask questions like, well, what's the total addressable market right for SAS products inside, you know an agency? I don't know you. I don't know how one would carve out, you know, a cost estimate from a large multi-year contract that includes everything from help desk support to advanced application development.

So, if we're going to be bringing these companies in, it's these different innovation techniques or acquisition vehicles have been doing it, ten merits to say well, what comes next? How do we help these companies think through what it means to build a sustainable business inside of our DoD and defense community? And, last but not least: this is a, you know, a term of art, you know, from the venture side, but keep things founder friendly. There was mentioned a question that I believe on the previous panel about access to data. Right. And it is true that there are lots of open-source data programs increasingly that are hosted by a variety of the cloud service providers that can serve as a launching off point for companies. This is it's been said, both at this hearing as well as many others, I want today out is still based on specific use cases. And I I've-I've run PNL from these programs and I can tell you many a times we said we have a cool prototype, does it apply to this specific use case I'm trying to Do- And until you do that, you're not gonna build trust with-with the end users that we have. And so while I'm not certainly advocating for open sourcing. A labeled data from, you know, special government use cases. There are perhaps other techniques that we can use such as like trusted boundaries where we can do provide more exposure to companies that want to learn more about government applications. We're doing different types of line evaluation tests, right to serve as a gating function for companies. We have these tools and expertise, and it serves as another way to not only attract more companies that hopefully will want to come in and support both commercial And government use cases, but also keep them there.

So, with that, I'd like to thank. You for opportunity to speak today and look forward questions.

FERGUSON: Thanks very much. Finally, on this panel, we'll hear from Mark Elszy, who is regional Vice President at Dataiiku.

ELSZY: Thank you. I'd like to thank the Commission for the opportunity to feel like it's my job to summarize everything from the day and I think I might have accomplished some of that. I run the federal business at DATAIKU, but I think some of my comments will really kind of apply to private industry as well. We have an end-to-end software platform for developing all sorts of AI from data ingestion all the way through governance and-and the bleaching of a data product. You know the insights here we've gained from advising over 500 clients around the world, supplying with them the tools to build and scale responsible AI. At Dataiku we see a future that we call everyday AI? Where everyone across government agencies, civilian industry and job functions has the tools and training to contribute to artificial intelligence in a way that improves everyday life, from decision making as well as enabling game changing products and services that we hear about. But we believe that the future of AI will require all of us, and not just some of us. In the context of national security, we've heard about safeguarding IP, cyber threats, supply chain security, all of which are critical issues. But when it comes to artificial intelligence, I'd ask you to consider some foundational challenges that, if not addressed, could prevent us from leading an AI and making us safer. The overriding challenges from our perspective is readiness. At Dataiku we are focused on three foundational issues When it comes to readiness: the 1st and most important factor is our people. Within the government and private-private industry, we simply don't have enough. Skilled data scientist at data experts and we lack a coherent broad-based plan to upskill the workforce that we do have critically important. Second factor is trustworthiness of the AI predictions of paramount importance in trustworthiness is transparency, transparency of the data used, the predictive models developed as well as continuous, always on monitoring of models for changes in accuracy and bias. And then the third factor is speed or what we call speed of mission. Quite simply, we must go faster in industry with federal agencies and as a nation. As we've heard, the number of AI patents filed worldwide is growing at an annual rate of 77%. Last year, China filed three times more patents than we did. Throwing more money and people at the problem is insufficient. We need an industrial scale production model for AI, analogous to what Henry Ford did for automobiles. Such a model would enable automation, collaboration, and continuous improvement. Now I'll get into a little more detail on each of these. First, on upscaling, we can't hire or outsource our way out of this problem. Some report that the demand for AI experts is 3 to five times the supply, and with that kind of a labor environment, federal agencies will have a difficult time competing with Google and Facebook for the number of workers that we need. Miter(?) estimates that 20% of DoD civilian workforce could be enabled with some degree of AI skills, which would add approximately 157 thousand people to that skilled workforce. Now, that doesn't mean that we're gonna turn every Excel and PowerPoint user into a coder. We need broad adoption of low code and no code capabilities as a way to get more domain experts involved. For anyone that might not know, and I hope I don't insult anybody, low code and no code refers to software development functions that often requires just the click of a mouse versus actually writing software code. With these kinds of tools, it's possible to have a business expert with context working side by side with a PhD data scientist on the same project. Other non-coder roles are required like data domain experts, data engineers and stewards, model catalog managers, AI operations, architects just to name a few. We know that upscaling works because we have experience at Dataiku with massive upscaling programs that companies like Pfizer, and General Electric and Schlumberger. Some best practices in upskilling include branding and publicizing the program within your company, providing multiple self-service, learning paths for your employees, And creating multiple levels of certification so that everybody can get started immediately without regard to their current skill level. Upskilling hundreds of thousands of workers that we currently have on the job would create a flywheel effect both within the federal government and national security infrastructure, as well as across the-the economy in general. Now next is trustworthiness. This issue has multiple layers, and everybody is very concerned about this when it comes to readiness. It's critical that the frontline workers have trust in the AI products where they won't use them. Without trust, even the best AI products can't generate value. For example, let's say that an AI model predicts that we have sufficient spare parts on hand to service mission critical aircraft for the next 12 months. If the sailor or airman who's in charge of the Uh, the depot doesn't trust that insight. They'll overstock and we miss an opportunity for efficiency (?) consulting group estimates that less than 20% of global 2000 companies have generated significant positive ROI(?) from AI, and the primary reason is lack of trust of the insights. So what do we do about this transparency, traceability and monitoring will help generate that trust? The transparency and the data features that the model uses to make predictions and an explanation of each individual-individual prediction if needed if asked for. For example, if a satellite image processing application estimates that a certain factory is operating at only 20% capacity, it should be able to explain how it came through that for that. If. Umm. Auditability, Traceability of every step that the through is a way to do that. The third factor is speed or speed of mission as I said before, speed comes from involving more people in the Process, collaborating in real time and employing reuse and continuous improvement at every stage. 50 years ago, when software engineering was first being developed as its own discipline, separate from coding. Brooks's law was observed. It said that adding more people to a late software project just makes it later. There were no economies of scale because software was mainly developed by artisanal experts highly skilled individuals, often working alone or in small groups. Artificial intelligence today is mostly developed like this. Artisanal gurus that do not scale. I we're gonna go faster. We have to take some of these learnings and put them into practice. It's time that we apply what we've learned over the last 50 years about software development though AI and create A scale processes that include data and model catalogs, data, and model operations. Interdisciplinary teams collaborating together, and that continuous improvement and continuous integration that I mentioned. So in conclusion, I know everybody wants to get out of here. The reality is that every day AI is just around the corner, closer, to meet the moment and we need to address and strengthen these fundability building blocks of readiness by not focusing just on the moon-shot items like self-driving cars and things like that, but upskilling current workforce, developing transparent processes, and industrializing AI development for scale and speed. Thank you.

FERUGUSON: Fantastic. Thank you very much. Great panel, we've got time because everyone was so great on. your comments on time you got time for questions. Yeah, I just all I have, all the Commissioners had a chance to ask question today? I think so. Yeah, he's wrong. Alright, now it's a referral. You're gonna have at it.

CARROLL: I have a quick comment. You have data questions, so I don't really hear like great answers from the last panel. So the bottom line is the government is gonna advantage itself and retain its data because it has to be. It's like is it to fly or Sean's gonna sell it back to the different part of the government. Right. So the right answer there is twofold. One, create an environment where. We can bring companies like us to the data unflavored off you do your work, Peter IP and-and so the duties like trying to do (unclear) that. But they what I just said to you is like foreign to them. The other is synthetic data, right? So I can generate the exact same datasets with synthetically simulate restrict time and location along the classified aspects. And then you can-you can make that available as well especially it comes like SAT data sets or SCI datasets where maybe we don't have a facility clearance. So I don't have engineers you can see that anyway you could come to the data I don't know about Sean But, that's where are right now (unclear above)

GOURLEY: Yeah, but thanks for sharing.

ELSZY: No, I wanted to come on that too. If I could, I remembered that. Yeah, no. We work in, in, in government and commercial and the-the rules apply the same. If you're building collaboration and transparency in the development of the AI, so you know, at Pfizer, they've got these interdisciplinary teams, hundreds, thousands of people working on the same project. They didn't need be and they can see everything that's happening all along the way. If you're not a technical person. The same works in the Air Force you create that team, even if it's an enclave. The same principles apply in that group. We need transparency of how everything's doing and rules that can be enforced, through governance and whatever. So it's similar, even though it.

MESEROLE: Yeah. I had a question on something. We've kind of come around a few times today, which is the role of open-source software and algorithms in particular, and kind of whether, you know, we had a prior panel, for example, on IP law. And one of the kind of Reasons for IP is actually to incentivize disclosure, right? And make kind of breakthroughs public. What's interesting about AI is that Like the leading firms are by and large kind of open sourcing. Both their algorithms and increasingly for some of the larger foundation models like the model itself, and I'm wondering there are some There's obviously some real coordination benefits and kind of benefits for innovation. But there's also this issue that, you know, Sean, you mentioned just you kind of walk through the competitors, the US versus China, some key dimensions including algorithms. And one of the questions I would have I guess is do you see it as a sustainable kind of Ecosystem where, you know, researchers in the US and-and to some extent China are kind of open sourcing their models, Or do you see that Driving nature of AI development changing over time and becoming a little bit more and closed off and proprietary, in which case we might need to kind of develop better IP protections and things like that.

GOURLEY: Yeah, look, two things on that. One is we already see what we call these kind of dark curves, you see technology development in China, you track it, different things that goes dark, right? It's like didn't stop doing it, right, right. Like just running docs. So that's one, right? So it's as you look through that, not everything is obviously in the open. Secondly, you can read the. outright prints on-on artificial intelligence, we-we see them when they come, but we know people in the industry as he alluded to that are ahead of that space already and are opening all that stuff up. So, there there's bits of that, the third bit here is these open-source models are great if you want to recommend some clothes, but do you know where the open-source model came from if you're using this to target computer Vision? Now one of the things that is you can inject attacks into this, these things are incredibly sensitive to different adversarial attacks. Injecting noise, it turns a bus into a stop sign. It turns to stop sign into a cheetah. You can make these things do whatever you want. There's a large-scale language model that the Russians just produced. Do you wanna use that?

MESEROLE: Why not? LEWIS: Some good though. It's also it's a product of what particular-type question you're gonna answer, right? And so for a lot of cases, like if you're seeing a highly performant open-source model, but you may wanna tune that or whatever the particular use cases you're dealing with. And we've seen this time and time again and that one could argue the actual tuning part, the application, the integration into a workflow.

So, in this case talked about detecting things on satellite imagery Cradle to grave, And, then understanding a feedback loop of clicking to say this is correct, and then that reintegrates into, you know, whatever you're retraining cycle, is that sort of entire application, right? Is the value component, right? And so if you look at is the model the most valuable thing maybe in certain cases, yes. But in other cases, it may not be right. And so in a lot of these cases, like, for certain analysts, that it's like all source, they may say I just want good enough Right. Like I-I don't need this to be the best thing ever, especially if my budget for running these types of computational resources is-is end. I have to keep it within that, right?

So, they miss maybe one of them to accelerate their workflows. So, so much. It is still comes down in many cases to what use case or cases are you trying to address to where you need to go to the next level on whether it's a custom model architecture or something very computationally intensive? Yeah.

THIERER: Well, thank you all for your testimony today. We've had two excellent panels on national security, but it's mostly been about how we make sure we have the right capacity to achieve our national security goals using algorithmic systems. The flip side of this debate is the proposals by some to restrict these systems and you hear a lot today about so-called existential risk, global traffic, catastrophic risks associated with lethal autonomous weapons systems, so-called killer robots. We haven't heard much discussion about What are government’s Policies should be towards these things. Couple years back I was asked to sign a-a campaign to stop killer robots petition and I said no because I said anything that the Russians and Chinese won't sign on to, I don't think America should either. It basically was asking us primitively to tie up hands on a lot of these autonomous systems and deploying them. So there's many different components to this debate including export controls and other types of treaties we might enter into. Is does anyone on this or previous panel have any? The actual duty policy for…

CARROLL: I've read some of what the DoD is published on this from its 3000, not 09, so duty Regulation pulled off the Internet.

So, we (unclear) absolutely we either America you and I have a policy for this. Yeah, it's undergoing revision right now and it's like 4 with I think we've yeah very (unclear) Policy and emerging technologies. It was said earlier Brian said, hey, hope we never have a human is not the policy, right? The policy is not that policy is we will make we've all time as weapons systems. There's a board you have to go through before you start development. There's a board that you go through before you deploy the system. The bottom line is an autonomous weapons it’s-it's just like any other weapon system. I've deployed many weapon systems, right? It's up to the commander to understand his rules of engagement and make a risk assessment on employing that system just like any other weapon system. The big difference is the test evaluation that the department needs to do on these. On these weapons systems, and it didn't close to being there yet it’s not even close and a lot of its outsourced to the-the developer- It's Boeing and Lockheed and Raytheon that's making the system, and they're incentivized to just make it crap a test evaluation framework so that the thing gets goes out there. And I can tell you all about certain ones that are already kind of in development that that don't work. It's supposed to because the-the framework is not good.

GOURLEY: You look, and I-I think if we give the-the situation in Ukraine another six months we'll have I'm a lot of that answered for us. It's very clear that you know there are advantages by deploying human outer flip(?) systems and we're gonna see that experiment. We are seeing that experiment runs today. I think the issue here though on that is the lack of clarity around that. You know the killer robot’s space I think has hindered the ability to actually work on these problems and the social license to operate to The tech companies, particularly Silicon Valley, to go and work on these and space I think, always renders itself as an ethical dilemma when the fact is, the institutions here that are in this country have made very clear decisions around it. They're just not very well known. And I think to the general population.

KATURI: Just change the topic just a little bit. You talk about workforce, you talked about workforce. Now hear the question about ground truth labeling being a big issue because as more AI systems come through, you just need to know what's true, what's wrong? What is your suggestion from a policy perspective in handling the workforce requirements, the ground truth levels?

GOURLEY: Well, increasingly, we're gonna have to take it in in house to Defense because as the models become more sophisticated, the labels need to become more sophisticated. The issue on this is-is not often ground truth from an individual, but ground truth across teams, and so teams can look at information and say that this is a missile launcher. That's not a missile launcher. So, the agreement that they have is really important because the model can only be as good as the agreement of the people labeling it.

So, that stuff is gonna have to come internal. We're not gonna be able to Mechanical Turk away through this. We-we don't want people doing recaptures to kind of get into the e-mail to say whether or not that's a Target we wanna hit. This is obviously gonna be subject matter experts. So that means we need to build that labeling 1 capacity, but it's not a one and done. Right, as soon as the war starts, if I've got a model that identifies Russian tanks and I didn't update that, with Big Z's on the side of it, my model's not gonna be as good. So the models have to develop. And that actually brings in this human of the loop is actually very much the loop, but you're training the models in real time as the opponent tries to adversarially avoid detection. So this is the workplace we need to start making and bringing, but it's only one piece of the labeling, the training, and the deployment that the other final. But here is you've got a model. That's great. Take six months to train absolutely useless. If your opponent finds a hole on that to say what was the war come back in six months when my model's ready.

FERGUSON: So we have time for one more Jerry?

JONES: you know, soon on autonomous tactical weapons we can live with that. Ok, that's not gonna kill the world. But autonomous nuclear weaponry. We know it's public source that there are several times when nations thought that there were being attacked with nuclear weapons, and luckily there were people that said hold on a minute we're not gonna power back and they literally save the world and our side. And to Russia's side, if we put AI in you know, those go back in time and now we're in a different environment where we have AI, we may have hypersonic. We may have a very, very open window of reaction time, so we may end up having to put more trust in the system. How should we be thinking about that? You know, for the next decade? Not just for our country, but on an international perspective, how do we build this fail safes that inevitably will be important?

GOURLEY: Look, I-I think it’s-it's-it-it's the-the-the most important question he gave in that we have to actually answer on this is-is-is-is gonna be right in front of us with hyper sonics.

So, speed of human cognition is gonna render that loop of a human decision of any kind of substance can be very, very difficult, right? So, you're gonna have to start instrumenting our automated responses once hyper sonics. And then if you want first rate capabilities, which is a fundamental tenet of the current geopolitical structure that we're in. So if we find tiny first strike capabilities, we're gonna have to think very closely about our emotion (?)with hyper sonics.

So, that's what the one end of that on the other end of this, how do you maintain, you know, autonomous image recognition, you know, too-to identify an enemy vehicle and ensure it's not stalled (?) that's a different side of that problem. And I think we need to kind of like look at, you know, I think the-the problems that we can solve, you know, along that spectrum, right? And so nuclear one ended kind of image recognition for autonomous drones to the other. Where? Where does this come? One thing we do know is that you know, automation of anything will lead to improvements, but occasionally leads to catastrophic collapses and you only need to go. So as far as the financial markets and high frequency trading and the early 2010s to see flash crashes that we don't really understand why they happened, but a trillion dollars, a market cap is removed for no apparent reason.

So, we know when you put algorithms together, behaviors that don't make sense to us as humans unfold and we can't really predict them very well, right. So, this is a space that we're in. Automation will happen in a competitive environment. When it comes together, there's gonna be failure modes that we're not really aware of. And, finally, you've got a spectrum of, you know, you know, computer version all the way through to nuclear responses.

So, it's-it's a space that we have to confront and deal with, but I'll, I'll say it's also one that's gonna be fraught with a lot of difficulties. So, I don't know if we have the answers today, but one thing I will say is we do need to simulate these behaviors a lot more than we're currently doing.

ELSZY: Yeah, I'd like to come on that if I could. You know at Dataiku, we have this notion of this natural tension between in data science between the mundane stuff they gotta do, and the moon-shot stuff that you wanna do you got really creative together with the mundane and boring and the boring can be how do I get my data and wrangle it down and wrestle it to the ground so I can actually use it? And then how do I build algorithms to train against the right data and all that stuff? You know, I think policymakers are gonna decide what we do and how we fight wars and all that stuff, but we have to equip the operators with the training and the tools to know that this is how you build responsible AI. These are the processes you have in place in the checks and balances, and we're going to continuously monitor it so that nobody's put in that position either where they're miss something and something that happens, or somebody can do something that nobody knows about. You have that transparency; you have that continuous monitoring and it's out there. We're doing that today with really big companies and the operators are buying into it because they're the people that are doing this want to do responsible AI they just want to know how to do it.

FERGUSON: That's gonna be the last word on this town. Great panel. Thank you all for your time and your expertise and your work. They're certainly gonna benefit from your insights. So thank you for that. We are gonna take a five-minute break. We have a fireside chat coming up with Miriam Vogel, but we'll come back in five minutes. Five-minute break.

Fireside Chat

FERUGUSON: So this is our this is the close of our fifth hearing of this Commission. We've never had a fireside chat before, so here we are. This is a special treat with a special guest. I fireside doesn't look much like this, but. You get the picture, right? We're just gonna have a. Well, conversation and-and, I'll-I'll kick it off with a couple of questions, but it's I really. Most interesting part of these hearings is always when the Commissioners get into it, so they are expert in so many of these areas, and at least seven fabulous insights. But Miriam Vogel is currently the president and CEO of EqualAI, which is a nonprofit launched by Arianna Huffington and Robert Locascio and others to reduce unconscious bias in artificial intelligence and to promote responsible AI governance. She also serves. As the Chair of the recently launched National AI Advisory Committee mandated by Congress to advise the President and the White House on AI policy. She has been a trusted advisor to high level federal government officials and business executives for her insights and experience in the responsible development of emerging technology. She also co-hosts a podcast In AI We Trust with Kay Firth Butterfield of the World Economic Forum. Mariam, thanks for being here.

First of all VOGEL: my Honor, thank you.

FERUGSON: We’re delighted you're here first; can you tell us a little bit about EqualAI? What are you doing and what are you trying to accomplish there?

VOGEL: Thank you for asking. And thank you for having me here. Truly, I'm so grateful you're doing this work and-and to be able to speak with you. So, it EqualAI our focus is, as you said, reducing bias and AI reducing risks and vulnerabilities, improving AI governance, making AI governance more translatable. We see AI as the new cyber threat that people don't yet realize. And by the time they see the landscape, they see the risks. It will be too late. And so we tried to really help get people ready for AI by focusing on three main constituencies, we work with policymakers.

So, with NIST with different US agencies and abroad, we work with lawyers and that's my own bias as a lawyer that lawyers are the partner to companies and identify risks, liabilities, harms, and lawyers need to be doing more here to ensure that we have frameworks and safeguards in place so that companies are on the right path. And the third area where we spend most of our time is with companies. So for instance, we have a pledge that we have for companies to take to help them understand how they can reduce their liabilities and discrimination and other risks by pledging to reduce bias and AI. We've a badge program for senior executives because once they understand the risks that they want to understand what to do. And it's very hard right now because we don't have national/ international consensus on best practices. But we do a lot of work with boards (?) because like in cyber and other areas, I think ultimately, they will have some of this. Fiduciary responsibility and other liabilities and they can play a key role in ensuring the C-Suite is ready for AI. Sure.

FERGUSON: So on top of your day job at equal AI as you've just described, you are also serving our country. Thank you in your capacity as a Co-chair of the National AI Advisory Committee. Tell us a little bit about that and I know what it's like to be a Co-chair of this Commission. Tell us about what it's like to be a Co-chair of-of that committee.

VOGEL: Well, it is a true honor. And it's exciting because I think right now our leadership in this country is taking shape in terms of AI. And I am fortunate to be one of 27 who have been selected to help us drive forward on policy recommendations to the President, to the White House as mandated by

Congress. And so. Hopefully with congressional support and input so that we can create action, our goal is impact. There are so many great studies and resources, you will have the report that you all are creating. We have so many reports out there by the top experts. Our goal is let's drive this to action.

FERGUSON: so we're seeing a lot of things happening internationally. We've spent a good bit of time with our at least last couple of panels today talking about national security. What's going on internationally? There are countries whose Values and agendas don't necessarily align with ours in the United States that are collaborating. You have other folks who are looking to regulate AI. It all impacts us in one-one in a, you know, some way, shape or form. What's the US role? What is our competitive advantage here? We've heard a lot about that in our previous hearings. The US can be a leader if we decide to lead. What are our competitive advantages when it comes to artificial intelligence and what-what ought we to be doing?

VOGEL: I would argue that it's not that we need to be a leader, it's that we need to maintain our leadership because our brand is trust. I think what we have that some of our competitors don't is faith that our AI does what it says it's going to do, that it's effective, but it's inclusive. And I think right now we have this opportunity at this critical juncture when AI is becoming such a fluid part of our daily life and is well part of our key functions. It's very rare to talk to a company these days that's not using AI in pivotal functions and they often don't know it. So we have this opportunity for a reckoning in companies to understand the power at their Fingertips to have scaled impact that can improve their functions, and they can do HR functions better. They can do financial determinations better if they integrate (sic) our values within their AI systems, right?

So, to clarify on values. I mean it in a in a broad term that where whereas in other countries where the focus is purely on data retention, we have a focus as well on being inclusive. And I think that is also a competitive advantage because the more people who are included in the framework of our AI creation, the more people who can benefit from our AI.

FERGUSON: So part of our work at this Commission is look at AI governance, what would effective regulation like, what would responsible regulation look like? What would reasonable regulation look like in the area of AI as is impacted by government policy. I mean ideally, we would provide some guardrails, you used trust as our brand like how-how do we safeguard and build that public trust in AI And prevent harm Societal harm. What recommendations do you have? Might you have for us? And I know that's a big question, but maybe just off the top of your head.

VOGEL: Yeah. Thank you for that question. The way I think of this is that we are this high speeds freeway right now, but we don't have lanes, we don't have speed regulations and we don't even have mandates as to who is allowed to travel on this road. So I think first and foremost it's clarify what we intend for the road that the basic structures, the lines. So look like, I mean, we know in a new city building a safe road is a whole different story than going to the old streets in Italy and trying to build backwards just almost impossible at some point. So I think first thing we can do is move quickly. So I'm glad that this report is coming out in the near term and-and that others are moving quickly because we don't have five years to set the rules of the road. AI is being deployed at scale today and the more that we wait the heart, it will be, if not impossible in some cases to unpack what it is that we expect a companies and I think some of it is just basic expectations which many companies are now taking on-on their own.

But we have to make consistency so that customers know what to expect, Government knows how to understand what's happening and that companies can ensure that what they're doing puts them in the best place 5-10 years down the road that they are in compliance and that they're doing what is expected of them. So for instance, routine Testing-most companies that are savvy to the-the risks of AI are doing this in some way right now. But it's not being done with consistent expectations. How often are you testing? That'll depend on what kind of AI systems you're creating, but it needs to be routine. AI iterates, your testing has to be consistent as well, and you'll want to document what it is that you're testing so that down the road, people within your company know what has been tested and win what hasn't. And as we know, AI is-is, you know, moving across the borders across companies. People who are creating the AI are also the final users.

So, we want that consistency. So, at the end of the day, when people maintain their testing, they know what has and hasn't been tested and what to look for.

FERGUSON: Sure. Well, you mentioned the report we are about to get into the maybe our hardest work is actually drafting our report. These Commissioners are all gonna be homing in and specializing in different areas/ Sections of this report and you know, they have questions that I know they will want to benefit from your expertise. Rachel, do you want to kick us off?

GILLUM: Yeah. I have so many questions. For-for being here, I'll start with kind of the high level, but you know one and I wish it wasn't attention that I think it's sort of this attention. You know, we're looking at innovation, competition and then but of course responsibility and equality and are values in that. Can you say anything about how you're approaching that tension as you're considering regulatory recommendations or how you think about that tension space? Yeah. And to be clear, I can't talk about recommendations for NAIC because we are not yet there. But for now, I think we are still in the briefing stage. We will help to get recommendations in the spring, late spring of next year, but we're still early stages. I can tell you from my perspective, it's a healthy tension but again goes to our brand of trust. I think that first of all, we don't have those. We know enough workforce to produce the AI that we need. If we don't make sure that we have a broader cross section of our population creating the AI. On the flip side, once we do find ways to get more women, more people of color participating in the AI ecosystem, and I don't mean just coders, I mean, I think one thing that we need to do is define what will the AI economy look like, what is that ecosystem? It's a broad ecosystem of managers, of supporters of, you know, there there's going to be tons of new jobs and some of them similar to ours in different. I think we need to define that so that we can make sure that we have that workforce in place. I think we need to make sure that it's a broad cross section both because we need all hands-on deck so that we can compete, but also all the evidence shows that AI is better when you have a broad cross section creating the AI. In our experience, our operating thesis is that bias and risks embed at each human touch point along the AI life cycle, and so you need to make sure that in each of those touch points you have people who can help, ask the questions, help think outside of their own imagination, which you can only do with your lived experience.

So, the more perspectives, geography, age, race, nationality, you can bring to those different touch points from its creation, development to testing at the end, I think that's a real opportunity testing what have we missed along the way, and we'll need to keep testing and it keeps iterating. So the long answer to the fact that that it requires some investment of that now. But I think that's our path to.

FERGUSON: Can rotate around a little Conrad?

TUCKER: Question. Sure. So from the hardware side, we're-we're already seeing. This proportionate allocation of. Access to hardware. Some of these models take weeks, months is also change (?) What do you recommend? They are thoughts around leveling the playing field for (unclear) To have access to these training, not only the models of Themselves but the ability to train these. (unclear).

VOGEL: That's a great question. Access to the data sets is another piece of that with significant costs and reduced access. Umm, I do think that's a place for government to play a role. I do think that You know when you're talking about leveling the playing field, creating incentives.

Uh creating more data sets, first of all I think that's a way ensuring that you have anonymized data sets that are useful, and whether its healthcare, population data, other sites set.

I think that that is a role for government to provide and serve. But I'm-I'm glad you're thinking about it, and I would welcome. I'd love to hear what you're thinking about too, because -I think you're absolutely spot on that that's a tension.

KATURI: In my mind and it's stuck on the data aspect. in my mind. Yeah. AI is a lot of (unclear), It's really data that drives inside. It's like a big hammer on data that's if Have data you can drive a lot of value. Should look at a country that we have land and the rules to make sure land is common, that is not afforded by a couple of people. And what data you will see that the data that's driving value in the country is kind of controlling specific words at some corporations, driver data in one area versus the other. Has it not testimonies for last several months, one of the key things is how do you really give this data or have policies to make this data available for more innovation? Otherwise, we're not able to deploy even if you create a lot of workforce, unless you make this data both what exists, what is getting created in a manner that's controlled, protected made and valued In the-the right way. There's no way you can drive the Innovation. I was just curious if this is something that has come up in your talks. Talk to us and how are you thinking about this?

VOGEL: Yeah, I think that's a key element we need to train on data that we trust as well as that is large enough as well as that many people have access to but yet can't correct it. You know we've got out with sharing it you also bring on different risks so. I yes, this is something we think a lot about. I should mention it in case it's useful- The way that we plan to proceed with 27 Members is we've divided our work into five working groups, plus there's a subcommittee created by Congress. So or we've been mandated to watch. So we are soon going to launch a law enforcement subcommittee that's separate track within our 27 members. We have a trustworthy AI. And that certainly comes up. We have research and development where suppose that these pieces are key discussions. We have competitiveness and-and that's where we think about our government's preparedness to ensure our leadership; we have workforce no common great interest and then international collaboration. So on several it's interesting to try and divide it up even because there's so much overlap. Each of those are served by data you know, and-and each of those are served by trustworthy AI. The other piece that we decided on in our first meeting was that first of all, in addition to our recommendations to the President and the White House, we would use the mandate of being a public Commission to amplify the AI discussion. So trying to engage a broader cross section into the conversation, making sure that our panels include new voices and just trying to think about how to engage more of the population in this conversation. The other piece that we all agreed to is that while trustworthy AI is one working group, that that's in every work stream that if AI is not reliable, trustworthy, and inclusive that it's not on brand, which is not how we define it there. But for our conversation today so.

Uh, yes, something we give great thought to.

FERGUSON: Alright. One more question, Chris.

MESEROLE: Umm yeah. Well, as the Congressman mentioned, you know, it's kind of the last of five hearings and I think one of the one of the tensions that's become apparent in all of them is this balance of how much of responsible AI or equitable AI really should be the result of kind of self-regulatory efforts or kind of principled commitments that private firms make when developing the AI and how much of it really should be regulated and kind of policies mandated by government? And I think given the kind of unique virtue (?) where you've. worked both with companies and also the government I'd just be curious to hear how you think about navigating that AI balance.

VOGEL: So, I do think at the end of the day, the reason we spent so much of our time working with companies and-and executives is because this will be within the company's purview. If they are committed to this, I believe they'll benefit from a competitive advantage. But at the end of the day, a company that is committed to this is the only real way to achieve trustworthy AI in the deepest sense. They have the ultimate purview. They have the decision of-of how much investment and and-and-and credibility they want in in this realm. That said, I think big picture, there is some need for the traffic lanes. There are some need to establish what are the basic. I mean, even if there are no other practical reason, then the litigation and the regulation will be coming, whether it's through the US or elsewhere, we know that it's coming. We know that litigation is gonna be coming.

The lawyers as soon as they're clued into the fact that there are scaled harms and discrimination based on laws currently on the books, let alone ones to come and that it happens to often come from the deep pockets, this will be a cottage industry and so I think the more we can do now to help companies understand our expectations and what basic compliance looks like, the better served they are.

FERGUSON: Miriam, we wish you the very best. We really thank you for spending some time with us here today and you have really important work ahead of you. And as do we.

So, I'll just close out our last hearing today. We want to thank everybody at the Chamber for all the incredible work you guys. Jordan, Michael, you guys, and your team do to make all of this come together, you kind of brought us all together, convened us. It's been awesome. What an incredible group of people.

Thanks to these Commissioners really appreciate your dedication and just the vast brain power that you bring to this. My kids like to say so. People have really big brains. We have a group of Commissioners that have really big brains and it's been fantastic to benefit from that.

And now, as I mentioned our maybe our hardest work is gonna be is-is beginning to synthesize summarize and come up with some-some recommendations. So I look forward to that and I appreciate your willingness to continue down this path.

Thanks for all of that work, and we're looking forward to hopefully doing some good for our country in the world as you are in your work.

So we're gonna try to do that on this Commission as well. So thanks everybody.

This concludes our fifth hearing. Wish I had a gavel.

Thank you all.