THE BROOKINGS INSTITUTION

FALK AUDITORIUM

THE DAWN OF A NEW ERA: OPPORTUNITIES AND CHALLENGES OF ARTIFICIAL INTELLIGENCE

Washington, D.C.

Tuesday, June 12, 2018

PARTICIPANTS:

Introduction:

DARRELL WEST
Vice President and Director, Governance Studies,
The Brookings Institution

Using AI to promote security:

JOHN R. ALLEN**, Moderator**
President, The Brookings Institution

DOUGLAS MAUGHAN
Director, Cyber Security Division,
U.S. Department of Homeland Security

SUSAN HENNESSEY
Fellow, Governance Studies; Executive Editor, Lawfare,
The Brookings Institution

How AI is transforming transportation, healthcare, and resource management

DARRELL WEST, Moderator
Vice President and Director, Governance Studies,
The Brookings Institution

DAVID SILBERBERG
Director, Large-Scale Analytics,
Johns Hopkins University Applied Physics Laboratory

CAROLYN NGUYEN
Director, Technology Policy, Microsoft

MARTIN FLEMING
Vice President, Chief Analytics Officer,
Chief Economist, IBM Corp.

AMIR KHOSROWSHAHI
Chief Technology Officer, AI Products, Intel

The policy and legal issues involving AI

NICOL TURNER-LEE, Moderator
Fellow, Governance Studies,
The Brookings Institution

JULIA POWLES
Research Fellow, Information Law Institute,
New York University

NICOLAS MIAILHE
Co-Founder & President, The Future Society;
Senior Visiting Research Fellow,
Harvard Kennedy School of Government

THE HONORABLE JOHN DELANEY (D-MD.)
U.S. House of Representatives

* * * * *

P R O C E E D I N G S

MR. WEST: Good morning. Thank you all for coming out and braving the Washington Capitals parade traffic which will intensify a little bit later this morning. I am Darrel West, vice president of Governance Studies and director of the Center for Technology Innovation here at the Brookings Institution. And, we would like to welcome you to our ninth annual A. Alfred Taubman Policy Forum. And, we are webcasting this event live, so we'd like to welcome our viewers from around the country and around the world. And, we have set up a twitter hashtag, #AIera, if you wish to post comments during the forum. That's #AIera.

So, Al Taubman was a good friend and a strong supporter of our program. He passed away three years ago at the wonderful age of 91. So, I want to thank him and his family for their generous support. His children Gail, Bobby, and Bill are not able to be with us today, but they send their best wishes. And, we are certainly grateful for all of the support that they have provided us over the years. Al Taubman was a forward looking individual. He always had great insights into new trends and important developments. I always learned many things from my conversations with him.

So, we thought it would be fitting to devote this year's conference to the opportunities and challenges of artificial intelligence. This is a topic of great importance, because AI is the transforment of technology of our era. It already has been deployed in a wide variety of sectors from health care, transportation, and education, to defense and national security. It is altering how we operate in many different areas. I have a new book out entitled "The Future of Work: Robots, AI, and Automation," that looks at the

impact on the workforce, and it is available in the Brookings book store right outside the auditorium.

This morning, we have a dozen different experts drawn from government business and academia. They will present their thoughts on AI and suggestions on ways to move forward. I think the central question we're going to be addressing throughout the morning is, how do we get the benefits of AI without incurring the downside?

To moderate the first panel, I'm pleased to introduce my colleague, Brookings President, John Allen. John, not only is the leader of this institution, he is a serious subject expert on artificial intelligence, and other types of emerging technologies. He has deep knowledge about many different aspects of AI, and the issues that it raises for society and governance. So, I can think of no one better equipped to launch our conversation. So, please join me in welcoming John Allen, and his panel of experts.

MR. ALLEN: Thank you ladies and gentlemen. It's wonderful to have you here with us on this wonderful day dedicated to the Capitals. I thought briefly, it would be about artificial intelligence, but it's actually about the Capitals. (Laughter) As Darrell makes an introduction like that, I always recognize that there is a difference between artificial intelligence and natural ignorance. So, what I'm trying to do this morning is set the case for this panel to help us all to understand about the use of artificial intelligence to promote security. We have about 55 minutes for this panel. I want to welcome the audience that is in here today, but also welcome all of us -- all those who are coming in to us today by the webcast. And, you're always welcome to join us. And, we're very grateful that you're with us today.

Today, the panel is -- we have several folks joining us on the panel today. James Baker, Susan Hennessey, and Scott Tousley. James is currently a visiting

fellow, here at Brookings, Jim, where he writes on issues related to artificial intelligence, cybersecurity, and national security. He comes to us after a long and illustrious career with the Federal Bureau of Investigation, having most notably served as the Bureau's general counsel for four years. And, he's also a lecturer at Harvard Law School, where we're very lucky to have him joining us from time to time. And, frankly Jim, thank you very much for making the choice to come to Brookings.

MR. BAKER: Thank you.

MR. ALLEN: Next is Susan. Susan Hennessey is a Brookings fellow with our governance study program, as well as executive editor of our excellent blog, Lawfare. Similar to James, Susan focuses on national security issues surrounding cyber security and surveillance, as well as federal terrorism prosecutions, and congressional oversight of the intelligence community. And, prior to joining Brookings, Susan was an attorney in the office of the general counsel of the National Security Agency, NSA.

And finally, we're joined, and we're very fortunate to have with us this morning, Scott Tousley, who is the deputy director of the cybersecurity division of the Homeland Security Advanced Research Projects Agency, which is part of the Department of Homeland Security Science and Technology directory. In his capacity at DHS, Scott supports several initiatives in critical infrastructure protection, and cyber physical systems, as well as project leadership for efforts such as computer security incident response, and other similar projects within DHS. Scott served for 20 years in the United States Army as an officer in the corps of engineers. Spending much of his time doing the important things that engineers like to do. We talked about that before. It's a wonderful community, and congratulations, and thank you for your service with the engineers.

So, we'll talk for a few minutes, I have some questions to ask the panel -- this panel of experts, and we'll come out to the audience about halfway through the hour. So, let's talk first and foremost about the tactical to the strategic. AI has the capacity to drastically impact virtually every aspect of our national security as a concept, but also in the apparatus. Let me just ask each one of the members of the panel. From your perspective, how will AI most change the way we think about national security? Jim, could we start with you?

MR. BAKER: Thank you, and thank you for having me, I greatly appreciate it. So, in terms of how AI will most drastically change things with national security, I think we don't really know. And, I think that's one of the things that concerns me the most. It seems to be a very powerful technology, so it -- the answer is, we really don't know, I think.

In terms of, sort of, thinking about my background and the kinds of things I've worked on, counterintelligence, surveillance, cybersecurity -- I think in those fields, it could substantially revolutionize how we approach those types of issues. How we approach data. How we understand and analyze data, and how we then deploy investigative resources as a result of that. So, what do I mean by that? For example, one thing that I think we have to think about, and I'm not quite sure that we're -- I'm sure that we're not quite ready to deal with this -- is in terms of using AI for example, to understand and analyze the investigative holdings, for example. That the FBI and other agencies have. To utilize AI tools to look at, and look for patterns --

MR. ALLEN: Right.

MR. BAKER: -- with patterns, relationships within what it is that we have already. We have a lot, we -- speak of the FBI still in the present -- the FBI has a lot of

investigative holdings from a variety of different sources, including from electronic surveillance. And, I think utilizing AI to understand and analyze that, potentially could have huge benefits for us. But, it raises a number of privacy --

MR. ALLEN: Sure.

MR. BAKER: -- mainly, I think privacy and issues with respect to the Constitution. And, making sure that what's done is in strict adherence to the Constitution and laws of the United States. So, I think that's an area that would be, I think, highly significant for us. And, I think we need to give a lot of thought to that. I think lawyers need to spend a lot of time thinking about that, and I'm happy to chat about that more as we go here.

MR. ALLEN: And, I think that's hot burner issue, frankly for us these days. Scott, any of your thoughts please?

MR. TOWSLEY: Yes, sir. And, thank you for the chance to be here. My boss, Doug Mawn, got called away so I'm sort of stepping in here for him. I also want to give a shout out to Mike Garris, who I work with at MIST, in a lot of areas and stuff, another serious expert in this space.

We don't know exactly how it will play out, but it's pretty obvious it will have significant -- huge impacts in multiple different areas. You know, we've seen a lot of cases already, over the last decade especially. The back and the forth of offensive techniques of cyber activity versus defensive. And, it's pretty clear AI can help both ends of that, which is both good and bad. It's a double edged sword like so many of these technologies, and technical capabilities, and explorations turn out to be.

This is maybe one of the most significant breakthrough areas that's taking place in a globalized world where lots of money is going into this that is not in the

United States. And, that gets really interesting because it's not just our social science policy. Legal questions getting folded into the tech capabilities. It's also different experiments being done. Germany, South Korea, Russia, China, you name it. And so, everybody is experimenting with it in a social way, not just a technical way. And so, we've got to be really attuned to what's being experimented, tried out, piloted. And, that's a topic that's pretty significant to me in the science and tech organization where we've got to think of this in an engineering, let's try some things way, not because we've settled the policy. But, in a lot of cases you have to park the policy while you explore to see what even makes sense to do it. And, we're naturally pretty good at engineering things and trying stuff out. It's harder to convince people that -- when there's people involved and there's policy and legal, and all sorts of other issues involved, that you still have to try the same experimentation.

MR. ALLEN: Sure.

MR. TOWSLEY: It's clearly going to have a big impact in lots of different areas.

MR. ALLEN: Thank you. Thank you. Susan?

MS. HENNESSEY: Yes, so I'm -- I largely agree that this is all a double edged sword. There's going to be good and bad. On the positive side, I think it does have the ability to revolutionize a speed capacity -- the ability to deduct patterns. I'm not just augmenting human capacity, but really going beyond what we ever could have possibly imagined.

It's also going to introduce entirely new forms of vulnerabilities. And, we're going to have to think, not just about the promise of AI and machine learning, but also what's known as adversarial machine learning. So, deploying these systems when

there is an attacker, or in the presence of somebody who wants to manipulate them for bad.

So, Dawn Song who is a professor at the University of California at Berkeley, has done some really interesting and rather scary research if anybody out there wants to get their pulse racing in the morning, on what this adversarial machine learning might look like. So, some of her experiments have shown, for example, how easy it would be to modify a stop sign, such that for a human who was looking at a stop sign, it would look like an ordinary stop sign. To an autonomous vehicle system, it would actually become entirely invisible. So, whenever we start to think about the ability to manipulate objects in the physical world, in ways that can have really, really dramatic consequences -- I think that's a little taste of the kinds of security challenges that we're going to be facing here. That, not only are we moving deeper and deeper into the cyber space, but we also need to care about the kinetic world as well.

MR. ALLEN: Very good. Now Scott, you spend a good bit of time in the whole business of cybersecurity. And, we know that as Susan properly said -- and I think it's a very important point to recognize the speed at which things will occur, will be revolutionary. In fact, you'll hear the term now, hyper war in the context of how fast conflict can both unfold and be prosecuted. But, there's also a real implication for that in the context of the cyber domain. And, protecting and acting in the cyber domain in terms of cyber security. Can you us give some of your thoughts on that please?

MR. TOWSLEY: We find a lot of applied research efforts trying to improve capabilities that CIOs and CISOs have within DHS, the federal world generally, and the critical infrastructure world. And, it's common already for elements of AI to be folded into something that somebody is doing that may actually serve to protect an

emergency call center, or protect against an ES attack, or all sorts of other things. So, the AI elements are percolating into the applications that use the explorations in lots of different areas, and that's going to obviously continue.

I think the other interesting thing is that we're only still part way through the really large mash up of historically, information technology things with the unfolding operating technology changes across the different infrastructures. Internet of things, applications, the pervasive censoring of everything everywhere. And so, AI is really just the analytics and the insight, while everybody is still trying to understand -- a decade ago, I was trained on how to manage a water plant by managing things that were there. And now, you can almost autonomously do it. And, figuring out how to do that in a safe and secure way, ways that insurance companies are happy with.

MR. ALLEN: Sure.

MR. TOWSLEY: And so, AI is really just a significant layer of learning and application on how to do that. And, I think that is the one thing that I think helps us a little bit, is that all of our systems are so heterogeneous that that gives us a little bit of a break in our governor on the AI stuff. That helps us keep an eye on, where it's going to go, and how it's going to help us manage things in the right ways.

MR. ALLEN: Good, thank you. And, either other panels. Jim?

MR. BAKER: Sure. In terms of cyber security, I would -- I mean, I agree with that. It presents a lot of different novel challenges. It strikes me that, first of all, AI -- to think about AI, at least from a perspective of a lawyer, so keep in mind, I'm not a technologist. But, when I think about it, I think about it as part of a much larger digital ecosystem. So, it doesn't exist on its own somewhere out there. Right? It exists on technology. It exists on computers, and the faster the better, I think, at least in terms of

how it is able to operate. And, it also then, as we've sort of touched on, it helps analyze data in ways that we've been chatting about, but it also -- I'll use the term, feeds off of data. It learns from data. It needs to be exposed to data. The algorithms need to be exposed to data sets, and that raises all kinds of issues in terms of biases, and so on.

MR. ALLEN: Mm-hmm.

MR. BAKER: So, with that, you've got AI technology, you've got fast computer technology, and you've got big data. And, all of that together, from the perspective of an adversary, makes a very lucrative target.

MR. ALLEN: That's right.

MR. BAKER: And so, -- and as we go forward with 5G and internet of things, and as more and more data is collected, that trove of information is going to be even richer, and even more desirable for an adversary to obtain. And, most likely, that will be done through malicious cyber activities.

MR. ALLEN: Mm-hmm.

MR: BAKER: And so, when I think about -- when I start to think about that, I become depressed. Because our cybersecurity posture is so grim, quite frankly. And so, the incentives for the adversaries to go after those kinds of assets, their abilities, their resources, are quite substantial. And, that -- that will, you know, we've already seen the erosion of U.S. technical edge, loss of intellectual property, loss of money, those kinds of things that have harmed the country. And so, I think the desire for adversaries to obtain that information is even going to be greater. Because I think they understand, also, how revolutionary this technology is. And, if they don't keep up with us --

MR. ALLEN: Sure.

MR. BAKER: they're going to be in a bad way. So, they have a substantial incentive to try to steal that kind of stuff.

MR. ALLEN: And, we've recently been declared the most cyber vulnerable society on the planet. And so, this is a really important issue at this particular moment. Susan, your thoughts?

MS. HENNESSEY: Yeah so, I think whenever we think about, the problems we have been unable to solve systemically in secure software. The ability to, bring it up even to minimal standards. This -- AI starts to pose a really interesting potential solutions in that space because we have insufficient regulatory frameworks --

MR. ALLEN: That's right.

MS. HENNESSEY: Because of the first market incentives, or the things -- it might be that -- the trying to build secure software on the front end, we throw up our hands and say that's not possible. But, we have seen, or we actually see these AI tools deployed is the ability of machine learning systems to go out in capture the flag type simulations. Go out, identify vulnerabilities in other systems --

MR. BAKER: Mm-hmm.

MS. HENNESSEY: learn how to exploit them, come back to their own systems, identify that same vulnerability in themselves, and then patch it. Right, so we're seeing now, this continuous loop. Things that can happen without any human intervention whatsoever. I think what we're heading towards is a system in which -- that it depends on the -- how asymmetric the broader landscape is. So, you're naturally going to have a race in that space as things get, hopefully, better and better, more and more secure. But, it's why I think we're seeing so much anxiety, especially in the United States right now, about our perceived lack of a strategic edge here. The first to dominate this

technology really is going to be able to set a lot of the broader rules. And so, some of the early indications that we might be lagging behind, I think that that does have really troubling long term implications. In part, because we don't really know where any of this is going to go, and we don't necessarily understand the technology itself.

MR. BAKER: And, I think as we see -- to your point, the improvement of dynamic cognitive defensive systems, which in very real sense, given the speeds involved here, where we have cognitive systems who are seeking to breach a network, while we have cognitive systems operating against it, seeking to defend the network. This is a very intriguing dimension, I think, of the whole business of cyber security as it evolves. Now, for those of you who have taken notice, we're doing a lot of writing here at Brookings. And, a number of public events. We're going to do a lot more in the near future. One of the things that's very important to us here at Brookings, and Jim and Susan, I'll ask you to comment first, and Scott, you can come in behind it -- is the whole issue of an acronym, which I'm sure for those of you who are familiar with this community are familiar with. It's called ELSAI, which stands for the ethical legal and societal implications of artificial intelligence, and the community of technologies associated with it. It really needs to define much of who we are as a people, and what we seek to achieve, with respect to the implications, and the employment of artificial intelligence. Let me just ask Jim, in the capacity both you and Susan, in your long careers within the law, and as having the general counsels, what are you thinking about when you hear about those ethical issues -- ethical, legal, and societal issues?

MR. BAKER: All right, so as general counsel I was -- one of my -- one of the main parts of my job was to worry. And, I worried a lot.

MR. ALLEN: That was -- made you a very good general council. Thank you.

MR. BAKER: And so, yes -- anyway, I worry a lot about those kinds of things. So, I worry about -- let me just highlight two things. One is to make sure, for example, that an agency like the Bureau is -- when it's using AI, it's using it in ways that are explainable and ethical. And, consistent with the constitutional laws of the United States. Right? And so, to make sure that we are buying products, that we understand what is happening. Again, I'm speaking the present, it's the past, but anyway, that the Bureau and other government agencies are buying products that they understand, that they can explain, that the can defend in court, that they can defend to Congress, and the American people. And that, they -- and that are consistent with all of our values. Right?

So, that's one of the most important things. Because, well, we don't want to show up in court with bad AI. We don't want to send scarce investigative resources chasing after leads that's based on some type of bad algorithm, or bad application of an algorithm. Because it says, these people are the ones that you need to worry about, these are the most likely terrorists, for example. And, devote a lot of resources -- the FBI is limited in terms of how many resources it has, so I worry substantially about that. So, the Bureau and other government agencies need to make sure that they have in place -- excuse me -- mechanisms to make sure that they're buying the best AI. Okay. I do worry significantly about what adversaries will do.

MR. ALLEN: Mm-hmm.

MR. BAKER: And, whether their values will be the same as ours when it comes to ethical and explainable AI. They may not care that they understand how it works, so long as it produces a result that they like. And, they may be willing to tolerate,

I'll call it collateral damage. Damage to people, damage to institutions, damage to innocent individuals that to their minds is an acceptable cost, given the highly beneficial result that they're obtaining from the black box AI that they can't really understand. And, I'm concerned that that will put pressure on us to try to keep pace with them.

MR. ALLEN: Right.

MR. BAKER: And, that their AI, even if it has a lot of negative externalities, so to speak, if it's producing something really good for them, and they're pushing forward with that, that's going to put pressure on us. And, whether we can keep up with that, with our AI. If our AI is explainable, and ethical, it's probably going to be better in the long run, and will prevail in the long run. But, it's going to be, I think, challenging to try to keep up with the adversaries, if they're willing to go down this route.

MR. ALLEN: Susan, your thoughts? That's a really important outcome, Jim. I'll come back to that. Thank you.

MS. HENNESSEY: Yeah, so I do think that that's going to pose really tremendous legal challenges, in part because our legal structure is predicated on being able to hold someone accountable for making a decision. And, as we -- as fewer and fewer human beings actually make decisions, it's going to be more and more difficult. Who can we ultimately hold accountable? Right? If you go back to the designer of the system, is it the person who created the training sets?

MR. ALLEN: Right.

MS. HENNESSEY: Is it the person who deployed it, who didn't notice compliance mechanisms? We're really going to need to think through the core framework here of how exactly we're going to regulate and think about law and responsibility in this space. I think in some ways, though, the more difficult or vexing

challenge is going to be those broader ethical concerns. And, whenever we think about training sets, for example. We know that it's possible to introduce bias, right? So whatever goes in, is what comes out. On one hand, that might -- that might be a point of vulnerability. Somebody might manipulate training sets intentionally.

MR. ALLEN: Mm-hmm.

MS. HENNESSEY: And, we might also unintentionally manipulate training sets. So, one of the most, sort of, influential and important AI data training sets is the Enron emails. Just these 1.6 million emails that were released by the FERC after the Enron case --

MR. ALLEN: Sure.

MS. HENNESSEY: for transparency reasons. It's a huge free trove of data of human beings talking to each other. It is really invaluable, and so, lots and lots of researchers have used it in their work, just because it's there. Now, if we step back for a minute and think of the values and the choices, and the assumptions about human expectations and behaviors, we would want these systems to have. Is the behavior of Enron employees in 2000 -- is that the model --

MR. ALLEN: Right.

MS. HENNESSEY: that we want to put into these systems? And so, we really do -- you know, there's -- the technology is moving at such an incredibly fast pace --

MR. ALLEN: Right.

MS. HENNESSEY: that it's difficult to, sort of, say hey let's stop and take a step back, and think about what we're doing here. I think ultimately, this sort of leads to a need for transparency.

MR. ALLEN: Mm-hmm.

MS. HENNESSY: The need to understand what is going into these systems in order to understand what is coming out of them. That fundamentally is intentioned with security, because as people understand these systems more and more, they're going to understand how to manipulate them, potentially in negative ways more and more. And so, we are going to really need to think through what we care the most about because there really is a risk here of not only introducing this bias, but formalizing and hardening it in ways that are going to be really difficult to, sort of, unwind later.

MR. ALLEN: Mm. That's pretty tough. Scott?

MR. TOWSLEY: A big part of me is a little more optimistic than parts of that. This is a huge challenge in communication of science and technology, and its implications. One of the most profound talks I ever heard was one given by Alan Alda in an AAAS meeting some years ago. He's got a center at Stony Brook that communicate -- specializes in how to communicate science with the public.

MR. ALLEN: Mm-hmm.

MR. TOWSLEY: We've all seen TED talks, and they're all really insightful. When the edge isn't there, they're just talking about how to explain it. You know, I remember vividly, the testimony of Richard Feynman at the Challenger Commission. We need to find ways to explain what's being tried, how it worked, what didn't work, in a way that makes it simple for people to follow, and simply trust the citizenry and our country to do it. And, it's you know, we're a fractious place. People talked about that, but there are strengths to that sort of thing. And, this is a technology that everybody on the globe is going to be experimenting with. And, that's actually going to be a huge strength because we'll see what works, and doesn't work in European place

versus a South American place, versus an Asian place, or whatever. And then, we can draw our conclusions and listen and learn from that. And, I think that actually is a significant strength to this technology and our choices in how to employ it.

MR. ALLEN: So, Microsoft this week -- sorry, Google this week, issued a document where it takes a position in that document, that none of the work that Google will perform will either support the development of the weaponization of AI for weapon systems or for surveillance purposes. So, we've -- we're talking about that. We're talking about the ethics of AI. The ethical, the legal, the societal implications. We have a major tech company that has taken a social and policy position with respect to its willingness to participate in AI for the purposes of national security.

And then, we have the issue of global competition. And, I think we know that there will be those that seek to adopt and adapt the algorithms of artificial intelligence with supercomputing and access to big data that may not otherwise be so constrained by ethics as we are. And, when as Susan said earlier along, as one of the key aspects of this international competition is both speed of development, and speed of employment. What are your thoughts about this? Where are we right now as we move into the digital future with respect to these intersecting lines of tech giants being unwilling to participate in national security with respect to AI? The inherent flow of resources and commitment by certain nations to the development of these capabilities. Where do you think we stand? And, I'll -- Scott, let's go back to you. Since you're part of the government now.

MR. TOWSLEY: Absolutely. I think it's still early in this evolution of how this is going to work. I understand the Google statement and position. There is a need for transparency. Again, as somebody steeped in technology, it's a problem for me not to try an experiment, show people how it did or didn't work, how it was set up, be able to go

back to it later and talk about it in a fairly dispassionate way. And, clearly AI, there are a huge system social elements to all this, but we still have to try and figure out how to experiment, because the experimentation contributes to the decisions about how to ultimately make it work. And, there are lots of companies that are still playing in the space, and supporting the government they're working with. And, the government is still trying to figure out how to run these experiments, and where the boundaries ought to be. And, the Google statement, I think, contributes to that discussion of, we don't want to just blindly support everything, but we want to think about that.

MR. ALLEN: Right.

MR. TOWSLEY: So, I think it the end it will work out pretty solidly as long as we have an open mind to it -- an open technical and purpose mind, and we explain things about why we're trying to do it. And, think of them in experimental senses, in demonstration activities, in engineering problems and analysis, and things like that. Because, that's really where we're at in a lot of these cases.

MR. ALLEN: Jim, any thoughts?

MR. BAKER: Sure. Well, so I think the -- you would definitely know better than I do, but the military implications of AI are vast. And, we're not going to be able to cover that right now.

MR. ALLEN: Profound.

MR. BAKER: They're profound. They're substantial. And, a lot of money is being invested in that, in the United States, and around the globe. I'm quite confident that there will be -- if it's not Google, there will be other contractors that step up and fulfill that role with respect to the U.S. military. The militaries of our allies, and our adversaries as well. And, that's the point. I think that we are going to -- if companies

don't want to deal with, or don't want to participate in the production of those kinds of products, I guess I'll call them, our adversaries will. And so, the United States will have to figure out how to deal with that. So, we're going to have to figure out some way to develop that type of technology to the benefit of our military in a way that's consistent with our values and U.S. policy. Because that's the world that we're going to live in.

MR. ALLEN: Thank you. Yup.

MR. BAKER: Yeah. That's the main point, I think.

MR. ALLEN: I think so too. Susan.

MS. HENNESSEY: So, this isn't the first time that we've had to confront the issue of duel use technologies. And, so I think that in some ways this is novel and in some ways it's not novel. I'm -- I can speak less to the weapons element of this, but as a former member of the intelligence community, as we think about the surveillance tools, clearly there is a capacity for harm here. But, by not -- by one of our large companies decide just not to participate, I think two things end up happening.

One, I think you forfeit the ability to actually shape these technologies, and I think it is an accurate prediction. And, it doesn't mean these systems aren't going to be built, it means they are going to be built by you. And so, sort of, that as a threshold matter, just saying, hey we're not going to operate in this space. That might be a reasonable choice to make, but you are giving up the ability to bake in some of your values there.

MR. ALLEN: Sure.

MS. HENNESSEY: I also think, whenever we think about the surveillance context specifically, there's a little bit of an assumption, especially from technology companies right now to discuss U.S. surveillance, and U.S. National Security

surrounding U.S. national security purposes, as sort of, necessarily an evil. Right? It is not a neutral technology that can be used for both good and evil, but instead, it is a bad thing. And, I think that is a little bit of a shame, in part because the intention of the U.S. intelligence community is to make the world safer for people and ideas. And, I understand that's a controversial position, but that really is supposed to be the core of what we're working towards.

One of the core issues that we've had in the U.S. surveillance debate has been discussions about privacy. How do we protect the privacy of Americans and innocent individuals abroad while also allowing them to conduct the critical mission? One tremendous potential use here is the ability to use AI in order to minimize privacy intrusions. Right? Have fewer people looking at personal information. Ensuring that we are only looking at that which is strictly necessary, right?

MR. ALLEN: Mm-hmm.

MS. HENNESSEY: So, there actually is a lot of ability to maximize privacy values, potentially that mythical space in which we don't have to give up privacy for security. This thing that we've all be discussing really just aspirationally, this is the technology that really starts to move us there in a real way. And so, I take the concerns here, I think they're real, and they shouldn't be minimized, but I do worry as a threshold matter, I'm just saying, hey we're not going to allow any systems to be built or used in this way. I worry that we're leaving a lot of good on the table by doing that.

MR. ALLEN: The points that all of you have made, which are very important, is that this is going to be a crucial consideration as we move forward. The whole business of dual use AI algorithms, the improvement of supercomputing, the access to data, the scope of which we can only now begin to imagine is going -- it really

forces us to have to come to grips with these whole ethical issues. And, that's completely apart from a conversation I don't want to get into today, but it deserves our continued consideration, and that is the whole business of autonomous weapons systems, and their -- the capacity of the United States to wield these systems in a hyper war environment where this is no -- theoretically, no human in the loop. And, I'm not talking about a U.S. human in the loop. I'm talking about in the theory of, where in the process of autonomous systems, where weapon systems are employed at an ethical level, is the human in the loop to ensure that we remain true to our values? That's really the pivot point of much of this conversation, and all of you have touched that in one form or another.

We have about 25 minutes for questions. What I'd like to do is go out into the audience. As you ask the question, I would ask you to identify yourself please, and your organization. And within just a couple of sentences after you begin to speak, I'll start looking for a question mark somewhere in your conversation. (Laughter) So, let's go ahead and go out to the audience please, for some Q&A. Yes, sir please, in the middle aisle.

MR. OPLEM: Thank you very much for this fascinating, eye-opening discussion. My name is Jeff Oplem, I'm a recently retired state department diplomat, now managing my own consulting firm.

MR. ALLEN: Thank you for your service, by the way.

MR. OPLEM: Thank you for your service, sir. You began to touch on this question, but I'd love to hear a little more about it. The question is this. Given the vulnerabilities that we face as a government and as a nation, to this threat of adversarial weaponized AI, what approach should we be taking as a government on the international

level to try to mitigate that risk? For example, should we be -- is there a role for the UN in trying to help prevent an AI arms race, or for setting international rules or standards about weaponized AI? Should this be a diplomatic priority for us? Thank you.

MR. ALLEN: Who would like to try that?

MS. HENNESSEY: I think it's an important question without a clear answer, but I think -- as we've seen in other elements of cyber conflict and cyber agencies, eventually whenever you're asking people to -- you're asking nations to not do that which they are able to do. And, on a pure technological level, we know that they are able or will be able to do it in the near future. You ultimately have to come to some sort of norms agreement. And so, where ever we end up, I do think this ultimately ends up on the international stage. Whether or not it's the UN or other international engagements that poses a difficult question for the United States because the way in which you get others to constrain themselves is by being willing to constrain yourself. And so, I think that is why it's so important that we get really, really clear on our values in this space early on. So that we can make decisions to start shaping the international landscape.

Because, ultimately we are going to have to come to some sort of normative agreement about what is acceptable and not acceptable with this technology. And, we're going to have to make those decisions in a landscape in which even the brightest -- the best and the brightest minds working on this don't fully understand the technology yet. We're going to have to start making the values decisions. We aren't going to have the luxury of having it all play out and then making a choice. So, ultimately, I do think there is that international engagement. I don't know that now is the moment, in part because I don't know that anybody knows what that would look like?

MR. ALLEN: Anyone else? Scott?

MR. TOWSLEY: It's happening to some extent already, and it comes out of a history of technology standardization and collaboration worldwide. We've done this for decades. I mean, my colleague Mike, and the MIST organization, that's one of the big things they do is figure out how to make things cross link and practice and details with other countries, because that's what we all come out and gain. And so, this will percolate into that space in the same way. And, in some ways it probably already is in different parts and shapes and ways.

MR. BAKER: I would just add, picking up on what Susan said, the U.S. it seems to me, has a hard time developing national policy on technology issues. And, until we have a policy, I don't know what you march in and ask these international bodies to do. So, I think that's the work we should be doing is just what Susan said, developing our national policy on AI and the rest of the digital ecosystem as I was talking about before.

MR. ALLEN: And, to exactly those points, we have a definitional challenge ahead of us. You used the term weaponized AI. Where does weaponized AI begin? Does it begin when the round comes off the rail of a predator and the system was entirely autonomous, and it identified the target through facial identification and engaged it autonomously? Or does the weaponization of AI begin somewhere well upstream with a surveillance system that identifies key individuals who are later to be prosecuted as targets? So, we've got a definitional challenge ahead of us with respect to AI, and that's something we hope to strap on here at this institution. That's a great question. Yes, ma'am?

MS. REDMAN: Barbara Redman, New York University Division of Medical Ethics. Just good to have a nethesis -- I'm sure there are many of them. Here's

the question. What degree do you think we will be, our social, our ethical norms will be shifted as we work through this problem? Shifted from where they are now?

MR. ALLEN: Barbara, can I ask a question? Are you satisfied with where our ethics are now? Could, in your question, our ethics be improved?

MS. REDMAN: Of course.

MR. ALLEN: Okay. Good, I wanted to make sure we weren't on a death spiral here. (Laughter) Okay, please.

MR. BAKER: Well, I guess I would say that ethics, it would seem to me, stem -- they stem from a set of values. And, a set of values that we as Americans hold. We want to try to -- we are now confronted with a new technology that raises, I think, profound and challenging questions. And, what really we need to do is figure out how we apply our ethics in that new -- or how we apply our values in that new arena.

And, I think what's hard is we don't completely have a picture of what that new arena is. We don't really understand what this technology is going to do. It's apparent in some ways, but I don't think the public understands it fully. Companies, and other organizations that are dealing with it and employing it, and working day in day out, are understanding it more and more as they go through. But, that's not necessarily transparent to everyone. So, I think a significant issue here will be transparency because of the value of these assets. Private companies that are developing them are going to guard that intellectual property quite vigorously, I would assume. And so, it may be that the thing is done, and finished, and ready to be deployed, and there really has been no transparency, and nobody really understands what's been going on. So, I think that's part of the dilemma. So, maybe -- again, picking up on what Google did, laying out some high level principles. Starting that discussion and that debate --

MR. ALLEN: That's right.

MR. BAKER: with the public, I think is a highly beneficial thing to do. And, you can agree or disagree with what their principles are. Whether they're sufficient and go far enough, in some people's minds, but I think making this a public debate, at least at some high level, where then the people deploying it, and thinking about it, and working day to day, can benefit from that type of thinking. And, not to mention, the law needs to keep up with all this, and that's a -- I'm fairly --

SPEAKER: Separate issue.

MR. BAKER: and I'm depressed about that too.

MR. ALLEN: That's a real challenge.

MR. BAKER: Yeah.

MR. ALLEN: Any other one? Any from the panel, Scott or Susan?

MS. HENNESSEY: I mean, you're infinitely more qualified to answer your question, I think, or I should kick it over to our colleague Darrel West, who's thought about this more in terms of the medical space. This isn't really an answer, but a shared concern, that I think a lot of the way we think about the ethics questions and issues focuses on the process. Do we have a process that has integrity, and then whether or not -- and then we can tolerate particular outcomes as long as we're confident in a process with integrity. We're going to have to ask how we think about this whenever we don't really understand the process, and really all we have as human beings to judge is the outcomes. And so, I think that is going to be the shift or the struggle is, how do we even understand what has occurred in a way that we can fix it, if we're just constantly being reactive to what has happened, as opposed to the system that actually produced the outcome.

MR. ALLEN: That's why I asked you, could you be optimistic about this? And, I think we can be quite optimistic in some respects because as we do more big data analytics and predictive analytics, what we've discovered is that many of the data bases that we've been working with for years have inherent racial bias, and gender bias, baked right into them. And so, as we go about the business of employing big data with AI algorithms, we are now, I believe, far more attentive to preventing that from happening, which inherently improves us as a society, and this is, I think, an unintended, but very important optimistic outcome in this regard. So -- yes, sir please. Just in from the aisle.

MR. WU: Hello, thank you. Jesse Wu, ELITA Consulting. So, there's been much discussion about transparency and explainability in the algorithms, but I think there's a growing recognition that -- especially with deep learning algorithms, which are the most powerful transparency -- just being able to see the code doesn't really get you the -- doesn't tell you enough. So, there's talk that there might be audits or other measures. But, how -- what kind of policy frameworks would you suggest be in place to ensure that either audits or transparency, or some other measures are in place to control for these bad outcomes, especially in the national security context where things are more complicated?

MR. BAKER: All right, I'll just jump in on that.

MR. ALLEN: Sure, please.

MR. BAKER: I think that's a great point, and that's my understanding too, is that the technology and the mathematics are just moving so quickly that it's very hard for people to understand it. We may just have a point where you -- humans can't understand it. That's one thing. And, the other thing is, what I talked about before with

the adversaries' use of the black box where they don't understand it, and they don't care. And, they're willing to use it anyway.

So, I think, we as a society -- again, back to the earlier question, have to come up with what are our -- how are we going to think about that. Is that acceptable or not? I don't sit here and have the answer to that. But, it may be that the reality is that we just can't understand all of the activities within the box. And, that it actually is black. So, I think we just need to have a public debate about that, and come up with a set of principles. I'm not sure how you're going to reflect those, perhaps in law, that articulate what it is that's acceptable, at least in the United States. Other countries -- excuse me -- other countries are going to have to confront the same thing and decide what they're willing to tolerate and how they want to guide their private entities in terms of the developments that they're willing to engage in, or allow to happen.

MR. ALLEN: Thanks Jim. Scott?

MR. TOWSLEY: I think there's one powerful positive, and one troubling or challenging negative from a homeland perspective, which is how I'm thinking about it right now. The Homeland Security Department of the United States, deals with the public every day in all sorts of different places. And, it isn't going to take long for the question, why, provided to a Homeland Security leader somewhere. And, you're going to have to explain why something was done, somebody was picked, somebody was -- all those sorts of things. And, that's a powerful strength of our system is, you answer to the public, you answer democratically. And, all that's going to actually help. And, we're seeing bits and pieces of that already. The challenge we face, again in the homeland perspective, is how do you explain to somebody what didn't happen because of what you did?

MR. ALLEN: That's right.

MR. TOWSLEY: And, it's the old phrase, the dog that didn't bark. And, how do you explain that that was a valuable outcome and things like that? And, that's a very difficult thing to do in a democracy, but it's actually one of the important parts of the communications challenge. It's not that hard to explain from a physics perspective, why the Challenger exploded. It's a whole lot harder to explain the different systems that together, collaboratively broke down, and then what you do about it. And, I think the 9/11 Commission was an awesome exercise in democratic exploration of things. We don't want to see that happen again, and have to go through that drill again, but we have to have that quality of examination and system improvement, even without the sparking point. And, that's going to be hard to do.

MR. ALLEN: Susan, any thoughts?

MS. HENNESSEY: I think that this -- especially in the nation security specific context, which tends to be a context in which there can't be public transparency. One of the challenges is whenever you have the people designing the systems also designing the compliance and auditing mechanisms --

MR. ALLEN: Mm-hmm.

MS. HENNESSEY: whatever they missed in the original system design, they are likely to miss. So, they are likely to design compliance and auditing systems that confirm the things that they already believe the system should be doing. And so, I do think that especially in that space, the challenge is going to be, how do we red team ourselves? How do we build something where we can be really, really confident, that's going to involve diversity of thought. Right? And, having lots of different people working on shared challenges.

That's not something that the United States government has been very good at in the past. It's exacerbated by the brain drain and challenge of getting really smart people into the government in the first instance. I think one thing we might see is that the private sector is on the cutting edge here. This is going to be where they develop, not only the tools, but the compliance control mechanisms. And, that's going to be responsive to a regulatory regime. And then, we're going to have the legal infrastructure within the government catching up. That's a little bit of the inverse than what we're used to. And, I do think it's going to produce problems. I just -- the systemic challenges that led to that place are really, really complex, and so we might just have to -- the best we can do might just be to recognize the state of the world and understand how we can operate within it. Because honestly, I don't even know how you would begin to go about solving those problems on the scale and with the speed necessary.

MR. ALLEN: Just into your point, the speed of government is much slower than the speed of the private sector's capacity to both develop and deploy the technologies. So, to Jim's point, to Scott's, and to Susan's point, we are behind in this process.

Now, an area that I think it's very interesting to consider this conversation, is in the employment of force. In the context of the use of artificial intelligence broadly, and then very specifically. The law of armed conflict requires that all commanders, before they employ force, have the necessity to employ it, have the capacity to discriminate between combatants and noncombatants, and use only enough force to accomplish the mission. Now, that's relatively understandable, and explainable, and accountable, in today's weapon systems, by and large. But, when we find ourselves in a realm where there is a certain amount of autonomy occurring, and artificial

intelligence algorithms are making decisions in order to maintain a speed of conflict, it's -- you're no less responsible, but how we determine accountability is going to be very interesting as we go forward with this. This goes back to the definitional challenges we have, and the absolute importance of conversations like this as we go forward. Yes, sir, on the far wall. We have about 10 minutes left.

MR. HARSHAW: Toby Harshaw from Bloomberg Opinion. I have a question relating, following up to that one. Let's say, hypothetically, that the rest of Silicon Valley follows Google's lead here. Who do we turn to? Is the traditional military industrial base capable of understanding this stuff? Could the IC and Pentagon take it on in house?

MR. ALLEN: Any thoughts?

MS. HENNESSEY: I mean, this is the cynical answer, but there are billions and billions of dollars here. And, I'm quite confident that the American system will produce a willing participate to want to design these things. I think one of the problems of potentially decoupling this into the events and industrial space, and separate from the public sector is one, we're going to have more distance from those public sector values. Two, we know that the data and the use of this stuff is comingled. These are likely going to be deployed in civilian spaces, or civilian military spaces. And so, I have no doubt that there is going to be someone, and then someone who is quite capable of developing these systems, but I do think they might be quite different in character and values, and the data sets and information that they can use to create their systems. And so, if that's going to be the path that we walk down here, we're going to have to think about, all right, how can we correct for, essentially this imbalance here? And, bring in some of those values and insights into this space.

MR. BAKER: I think what Google has done is actually a very good thing, which is to bring the discussion to the public about, are there limits? How should we even approach the limiting question early in the game? Their position may stay the same, it may change over time. Companies shift and adjust. Everybody is trying to figure out how to make use of this, everybody is trying to figure out how to help this drive fundamental underlying efficiencies, and gains, and everything else. It'll work its way out, I do believe. But, their point is a really good one. You can't hide from the ethical questions early in the consideration of how to use things now, because these are inherently ethical in some of the choices. And, part of me would want to see some legitimate experiments, pilots, demonstrations, to help understand them better, but you also can't go into it blindly. And so, I think it'll work its way out when you look at the companies generally, and Google as well, as the future unfolds.

MR. ALLEN: Yeah, great question Toby, thanks. Sure, microphone please because we have the webcast.

SPEAKER: I'm just wondering if the other three of you agree with Susan's comment that Google and most companies are missing a chance to actually help shape this in the way that they want it shaped by walking away.

MR. TOWSLEY: Yeah, I don't want to appear to condemn Google's, I think, very clear corporate position to take the moral high ground on an issue. But, I do believe that there will be companies believing that they also, are similarly armed with a set of values that will move forward with this. But, I also know, that we have competitors in this world that are not in the least constrained by the values that we as a nation embrace, as a matter of our DNA, frankly. While we've got problems from time to time, in the end, we are a nation of laws and a nation of people

committed to the human rights of our population, and the human rights of people around the world. That's not the case with all of our potential competitors. And so, that's going to be a challenge for us. We have to work our way through this. Again, the speed of government, and the speed of this conversation is lagging the potential for the technology. And, the technology, frankly, is fearsome in some applications. And, we have got to get a grip on this basically.

MR. BAKER: John, if I -- I'm sorry.

MS. HENNESSEY: And, just to be clear to the point before Jim responds, I don't intend to condemn Google for this. I think it is -- I think the fundamental choice is a do no harm principle. If you don't understand this fully, making the threshold decision of saying, we're not going to operate in this space. And then, figure out the ethical questions later, I think that's a reasonable choice.

MR. ALLEN: True.

MS. HENNESSEY: I think it's just necessary that we identify that that means the decisions are going to be made by others, and it's going to be incumbent on all of us, especially those of us in the policy and government space to really think about the character and nature of how those decisions are being made.

MR. ALLEN: Well said.

MR. BAKER: I was just going to add that I think your question raises an even more profound issue, which is where is the origin of that kind of thinking? And, the concerns that I have with respect to the relationship between the government and the people. And, how are the people thinking about the government, such that they would not want to participate? If the premise of your question is true. We've seen a lot of that, as Susan was alluding to earlier, in terms of over the last several years, the concerns

about government surveillance, that kind of thing. I mean, I think that is something that we have to spend a lot more time as a country working on --

MR. ALLEN: Right.

MR. BAKER: and reflecting on, and making progress on together. In terms of how we, as a people, relate to our government and our governmental institutions.

MR. ALLEN: Thank you Toby. Yes, ma'am, please. Microphone coming.

MS. QUINT: Good morning, and thank you all for being here. My name is Elaina Quint from Arizona State University, currently researching cybersecurity with the House of Representatives. And so, my question today is that a lot of our discussions about technology seem to be very reactive. And so, as someone interested in trying to start conversations for the future, how can we reorient our thinking, or our discussions, to make our discussions of policy and law more proactive regarding future technology?

MR. TOWSLEY: I think that's actually happening as we speak. To me, one of the most interesting parts of all this is the collision, the mash up, the combination of different machine learning and AI techniques with the way that they are percolating into just operating technology and management systems nationwide, infrastructure wide, et cetera. With the question of how do you educate people to use them, adapt them, fold them in, and that's a workforce education from the age of 50 to 65, and beyond. So, all of that is happening in different places around the country. Again, in different applied, experimental use cases. And, that I think is where we're going to get more anticipatory, more proactive, and less reactive, I think if you look at things.

MR. ALLEN: Anyone else?

MS. HENNESSEY: Yeah, so I'd make a plug for the reactive model here. So, we've -- our legislative bodies tend to not be great in terms of predicting technology. And so, whenever we think about the various levers we might have, in order to influence the actual development here, I'm not sure that those legislative levers are the appropriate ones. I think that there is a case to be made whenever we think about how the issues might emerge in the particular, and passing particular legislation that allows judges to decide in particular cases. So, obviously we need Congress to get up to speed on technology issues across the board, but I think the real risks of timing and evasion, focusing on the wrong issues --

MR. ALLEN: Right.

MS. HENNESSEY: having unintended consequences. To me, those seem like the more probable risks to be realized. And so, until we solve some of those issues, I do think that education mode really is the one that we want to see Congress in. Getting them to learn as much as possible, and to support education as much as possible. Funding these programs, funding initiatives, getting people to be focused on the questions, rather than deciding what are the legislative answers.

MR. BAKER: Can I --

MR. ALLEN: Please Jim.

MR. BAKER: To be proactive requires leadership. So, leaders need to drive change in organization -- in their organizations in order to accomplish what it is that you're talking about. Technology is hard to understand for everybody, and for leaders who didn't grow up with it in the same way that younger folks are. That's number one.

Number two is, they're busy and distracted by other things. They have other things they have to worry about with regard to their organizations. And, it's hard I

think, for them to really appreciate, and understand, and drive change through the organization. I think that's the reality of it. Another thing is, quite frankly, I've sat through a lot of bad briefings on technology issues, where technologists struggle to explain what's happening, and what it means to nontechnical folks in the organizations. And, I think that is something that technologists can work on, trying to figure out how to explain all that. I love this quote, it's been attributed to Einstein, saying that, "You don't really understand something, unless you can explain it to your grandmother." And, I think, keeping things simple and explaining them in a simple, but not simplistic way so that you can -- so that leaders can understand the nuances and so on, will help them. So, I think it's a two way street. Leaders need to drive this, and folks thinking about these problems need to figure out how to communicate upstream to make it effective.

MR. ALLEN: Elaina, we've got great confidence in your ability to help our elected representatives to figure this out. And, happily there is an AI caucus, now on the hill. Which I think is a very good start and gets to the point that you've made. And, it was actually my grandmother who explained many things to me as I was growing up, so I was very happy for that relationship.

Ladies and gentlemen, we've had, I think, a very stimulating panel. We have touched on some, I think, central issues that we're going to have to address as we move forward with the embrace of not just artificial intelligence, but emerging technologies of the 21st century. The speed of development, the speed of innovation, the speed of employment of these kind of systems is going to have require, or going to be aided in a very real way by public policy, research institutions, to help the technical organizations to bridge the gap with the government -- governed mental organizations so

that we can have laws and regulations, and policies that bring us along as a people, consistent with our values as we embrace this technology.

Let me ask you to help me thank this great panel this morning, and we'll move on quickly to the next. (Applause) Thank you. Thank you very much.

MR. WEST: Okay, that was a terrific panel. It was a great overview of how AI is affecting security, law enforcement, and intelligence gathering, and what some of the ethical and societal aspects of those areas are, as well. So I think we heard a number of provocative thoughts.

What our panel is going to do is to follow up on that conversation by seeing how AI is transforming a number of domestic fields. There have been important developments in transportation, healthcare, resource management just to name a few areas. AI is creating tremendous opportunities and offering a number of interesting innovations.

To help us understand this area we are pleased to be joined by four leading experts. Martin Fleming is the chief analytics officer and chief economist at IBM. In those positions he leads the company's efforts on AI, as well as cognitive analysis.

Amir Khosrowshahi is the chief technology officer for AI products at Intel. He works on creating hardware and software for AI solutions.

Carolyn Nguyen is director of technology policy at Microsoft, and in that position she looks at AI and digital governance. It's also nice to welcome her back to Brookings. Many years ago, she was a fellow here at the Institution.

And then finally, David Silberberg is director of large-scale analytics at the Johns Hopkins University Applied Physics Lab. And there he employs large-scale data systems and data science to improve analysis and decision-making.

And I do want to note that Intel and Microsoft support the work of Brookings and we are grateful for that support.

So I want to start with Martin. What do you see as the most promising AI applications in the domestic area?

MR. FLEMING: Well, certainly, the technology industry itself, a bit of bootstrap operation, is perhaps the industry where most applications have advanced the furthest to date. Then thinking about financial services, where there's a great deal of activity underway; financial services, the close cousin of the technology industry. But even in the large, well-known financial services firms that I speak to regularly, still exploring opportunities and potential and building capabilities, probably tied with financial services as healthcare. An enormous amount of work underway in the healthcare space.

IBM, for example, in our applications we have helped to provide care for about 55,000 patients at this point. It's a large number, but still a small percentage of the U.S. or the global population.

When we look at, for instance, the work that's been done at UNC to test and place some trials in the AI Watson capabilities, very interesting and promising results. The recent meeting of the American Society of Clinic Oncologists had a number of very interesting solutions being experimented with, as well.

Beyond those industries then, more broadly, I think of it as more in a functional space. The whole area of sales and marketing, which is data rich, both in the business-to-business and the business-to-consumer environment is one where there's an enormous number of applications that are beginning to emerge. And we all experience them to some degree as consumers of Netflix and Amazon's capability and others.

And the supply chain area, again, a data-rich, functional area where

there's been some significant progress made.

And then finally, I would say in the human resources space, of course, facing some significant challenges because of concerns around privacy and confidentiality, but still a place where there's been some pretty good progress. So that's the landscape as I see it today.

MR. WEST: Okay, thank you. So, Amir, I know you work a lot on transportation solutions and autonomous vehicles in particular. What initiatives to you have underway in those areas?

MR. KHOSROWSHAHI: So autonomous driving, driver's assist, entails lots and lots of interesting technology, all the way from building processors for cars, for other autonomous vehicles, and targeting them, making them robust, to work in as kind of adverse environment as your car has to sustain extremes of temperature and so forth. So beyond processors there is algorithms for doing the AI of these systems, doing mapping, doing computer vision, doing things like sensor fusion, route planning. These are all quite involved.

But it's not just in the car. The technology is also in the data center. If you're managing a fleet of 10,000 cars, there's a lot of systems-level machine learning in AI that's involved in that. Each car is recording on the order of 4 terabytes of data per day. And just managing the data, analyzing it, running machine-learning algorithms from this data and extracting knowledge is a really interesting engineering task; as well as the communication between cars and cars with a data center, using 5G technology, for example, is another thing we're investing in. That's also really interesting. How do you communicate between the edge and the data center?

MR. WEST: Okay. David, so Amir mentioned this extraordinary amount

of data that is being created. You study large-scale data analytics. How are they being deployed to improve decision-making?

MR. SILBERBERG: So there's a lot of advances coming from the university and also the labs from many of the outstanding companies that are producing in AI, so our job is really to deploy the analytics. And when we deploy analytics there's really two aspects of it that I consider. There's the engineering of analytics and there's the art of analytics.

So from the engineering perspective it's important to not understand just AI all on its own. It has to work within a large system and systems of systems where people are in the loop and there's a particular goal that needs to be achieved, so it has to be understood in the context of an end-to-end perspective.

Also, AI is not AI, is not AI, or the same thing for machine learning. If you open a machine learning textbook there are hundreds of algorithms. Understanding the right algorithms for the right job is very important and understanding how they need to be composed and how they need to be used is extremely critical within an organization or when you're laying out any kind of large data system. So to that end, understanding not only the technology of how to integrate a system, but also understanding the science of data analytics and how to pull the different algorithms together to achieve the goals you want to achieve.

There's also a level of explainability. So some systems need to be explainable, others do not. So there are various technologies that range from the broad spectrum of easily explainable, such as like expert systems, to deep learning, which is very inexplicable in many ways. So understanding the requirements of the human in the loop is very important.

MR. WEST: Carol, what are the AI applications that you think offer the greatest hope?

MS. NGUYEN: Thanks so much, Darrell, and thank you for enabling me to be a part of this panel. It's kind of interesting that we've had this discussion on AI and we haven't really defined what it is, so I'll just say what I think -- how we use it, which is AI helps to detect patterns which can then help to make predictions and recommendations. And looking at it from that perspective it has the ability to enhance any decision-making process in any sector. So as a tool I think it can be applied everywhere, and we think of it from that perspective as computational intelligence.

I'll just use three examples. One is in healthcare. So in terms of today's issues, an Institute of Medicine study that was released in 2016 said the third leading cause of death in the U.S. is misdiagnosis. And so one of the things that we're doing is actually working with Johns Hopkins to improve healthcare, patient care, in the ICU to identify anomalous treatments and also interoperability of systems, something very, very basic.

But in terms of going forward, in radiology it is estimated that half the people over 60 will develop cancer at some point during their lives, and half of those people will need radiotherapy. So one of the things is that our computer scientists are working with radiation oncologists, as well as surgeons and other experts, to try to figure out what's the best way to identify and delineate tumors from nearby organs in three-dimensional radiological X-rays.

I use that example a lot because I think that's a perfect example in terms of thinking about AI augmenting human abilities and capabilities. In other words, enabling subject matter experts to enable and create leapfrogs in each of their fields.

And that's how we're really thinking about this.

In terms of statistics, if you use AI alone in terms of radiology it's got a 92 percent accuracy. Radiologists have about a 94 percent accuracy. When you combine the two, you can get to something like a 99.5 percent. Again, these are the kinds of scenarios and applications that we think about as a tool's development.

The second area I want to talk about is really how AI addresses sustainability issues. So, for example, in precision farming we talk some of this about to use sensors, drones, et cetera, to enable data-driven farming. And so the notion is that with that data a farmer anywhere can understand what's the soil condition, what's the water, what's the landscape look like. It can improve farming productivity. The estimate is that food productivity could improve up to 67 percent. That's a major achievement and a step forward when you start to think about the fact that the human population will increase by about 2-1/2 billion over the next quarter century.

So these are some of the ways that we're looking at it. And in terms of that, as a company, we launched AI for Earth, which is a $50 million grant program over 5 years that addresses agriculture, water, biodiversity, and climate change. And thus far, the program launched last year, we've funded something like 110 grantees over 27 countries.

The third area I want to bring up is AI for accessibility and inclusivity. As a technology AI can empower people to be really more a part of their profession, their society, et cetera. So a very simple example, we developed an application called Seeing AI. It sits on my mobile phone and it describes to people kind of what's going on in a meeting, what's the reaction of the people around you. This is for visually impaired people. What's the scene on the street? It helps you to read menus and also identify

what are the products.

So these are some of the ways in which we really think about how AI can transform lives and improve societies overall.

MR. WEST: Terrific. So we've heard many innovations taking place in healthcare, in finance, transportation, and accessibility. So I'm curious, what do each of you see as the greatest barriers to making progress in AI in these various ways? And how can we think about overcoming those challenges?

Martin, we'll start with you.

MR. FLEMING: People. You know, in a business organization, changing behavior is the most challenging. We all show up for work every day and expect we're going to do the same thing the next day we did the previous day. Unfortunately, the world doesn't work that way.

So the challenge is to be able to create the tools that are necessary to help improve the productivity and the ability of workers to continue to grow their incomes, but allow them to adopt the tools and understand what's needed in terms of training and education, and being able to work in very different ways.

I can take you through a number of examples, if you'd like, but it's really the adoption and the deployment as much as it is the technology and the engineering itself.

MR. WEST: Amir, what do you see as the greatest obstacles?

MR. KHOSROWSHAHI: So some of the things we work on at Intel are making algorithms more explainable, transparent, developing algorithms that are privacy aware, that don't need to expose your data potentially to a nefarious actor.

Other issues we're working around are adoption. So the technology has

particular features that makes it very difficult to adopt. It's very computationally intensive, it requires infrastructure that's specialized for machine-learning AI, from storage to communication, to the compute requires new kinds of processor technologies, as well as helping companies get their heads around deploying robust, scalable, power-efficient AI systems is quite a challenge. So the theory and math behind neural networks is relatively simple, but to get a system deployed in an enterprise or in other situations is quite challenging. So those are some of the main things we work on: algorithms, systems-level AI, making it easily adoptable.

And also, my presence here, sometimes questioning some of the notions I hear about how the current version of AI is a black box. I don't think that it's actually true. And the research community has been a really good steward for this technology. So if you go to a machine learning conference where lots of academics are present, you see people talking about jobs and diversity and security and privacy. So I think we're very forward-looking as a community and we're becoming more and more involved in public policy settings, such as Brookings.

MR. WEST: David?

MR. SILBERBERG: So I'd say there's two obstacles. Number one, as data gets larger and as algorithms get more complex, so there's just an inherent limit to the size of the data and the machines that can process the data. So there's just a theoretical computation of complexity that needs to be overcome, and that really is overcome by increasing the system size and perhaps innovation in algorithms and heuristics.

But I think even probably the bigger obstacle might be is worrying about sort of the overhyping of AI and machine learning. So it seems to be a buzzword.

Everybody's looking for it today and I hear it more and more. Even over the last year the amount that I hear about AI and machine learning from potential users, potential people that are going to be employing these systems or want to employ these systems, it seems to be this magic word that's going to overcome everything. And it's very important to understand what all of these AI techniques or machine-learning techniques are, what they can achieve, and what's not achievable and what's achievable through a lot of work. And when we get a realistic perspective on it, then we understand what we're employing and we'll have realistic expectations.

The fear is that it'll become hyped to such an extent that it can solve everything. In reality, it'll solve many things, but it won't -- we just got to make sure to match expectations with real outcome.

MR. WEST: Carol?

MS. NGUYEN: I'll build upon the point that was just made by David, which is that there's not a lot of clear understanding on what the technology is, what it can do. At the end of the day, technology, it automates what we're already doing today and that's really the extent of the technology.

But to answer your question specifically, what are the barriers to AI, I think it is people from two different aspects. One is it needs to be trusted. It needs to be trustworthy in terms of the design, development, deployment, and adoption of this technology. Unless a technology is perceived to be trustworthy, it won't be able to be adopted to the extent that it can really achieve the potential of some of the applications that I mentioned earlier.

And from that perspective, the discussion this morning with respect to principles is very interesting, you know, from the perspective of there needs to be values.

As a global company we need to think about ethics, but from a very different perspective because ethics is a social-cultural construction. It is social-cultural norms, also. And so it needs to be timeless values that is applicable and can be applicable in multiple countries.

The second aspect of this is that we do need to make sure that we have the appropriate involved in the development of these applications in a way that is trustworthy. So that's capacity building, that's work skills. So there's a second conversation there about developing the ability of people to develop these kind of applications that will be relevant and can deliver trustworthy services.

MR. WEST: So David mentioned the risk of overhyping. Carolyn in her first comment talked about the need for inclusivity. So in thinking about the ramifications for workers and society in general people worry that AI is going to take jobs, increase inequality, and be biased in the way that it makes decisions, should we be worried about AI?

Martin?

MR. FLEMING: Sure, we should, yes. The whole issue of the future of work that you've written about quite eloquently and at great length is one that is certainly very pressing, a pressing issue. My view is that on the one hand are the broad societal attitudes have been very much shaped by the technology that we've seen deployed over the last several decades, largely in the manufacturing space around robotics, which is the old technology. It's a rules-based technology where the robot encounters a condition and reacts in some pre-specified way.

This is a very different technology that's being applied in very different spaces. We've talked about healthcare. Both Carolyn and I have used illustrations in that space. We've talked about financial services. We all as consumers use the

capabilities every day when we're typing a text message and the word comes up that you're trying to type, QuickType, that's an artificial intelligence application. So we see how the benefits are beginning to be apparent.

So the impact on employment will be fundamentally different from robotics technology, which is designed to replace employees, to a technology that's designed to enhance productivity. I would never suggest that there will be no jobs lost as a result the deployment of artificial intelligence solutions. That will be the case and it will differ significantly by geographies in the developing world versus the developed world, but it's a very different technology and will have very different implications for the future of work.

MR. WEST: Amir?

MR. KHOSROWSHAHI: So the promise of AI, I think, in the near term and potentially five years out is, as Carolyn and others have mentioned, is augmenting and working alongside humans. If you're immersed in this field like I am, building AI-based solutions, it's quite hard. Some of the simplest things like picking up a glass off a table is quite difficult for a robot to do, for example.

And even in areas such as radiology in the press you see a lot of hype around automated tumor detection systems and so forth. Is this going to replace radiologists? It won't. It will just augment. It'll be just another tool that they will get to use that'll improve their performance. And I think this will go on for the next three to five years.

Some of the tasks, the standard example in robotics is Amazon automated its data centers and what did it do employment? It increased -- Amazon has increased employment in its warehouse by 300,000 people. So automate the

warehouse, it did not eliminate jobs. Actually they have many more jobs in the warehouse. And this is true all across AI applications, in law and going through large corpora of text.

Basically the biggest problem of the latest neural networks in AI technology is to augment humans and work alongside them. So I'd like to act as a counterpoint to this belief that AI is going to replace jobs, but as you've written in your book there are certain parts of the population that are very susceptible to being replaced. And that's something that's a very big public policy question that we need to address.

MR. WEST: David?

MR. SILBERBERG: So I'll agree with both Martin and Amir, yes and no. So yes, you know, it is something to worry about. But again, you have to understand what you're building and what you're using. So if you're talking about automation in cars, you're subject to cyber-attacks on your cars or other types of equipment that you're enabling with AI.

On the other hands, it's an augmenting tool. If you use it correctly, it can actually -- just as Carolyn mentioned before, you can actually improve the accuracy of diagnoses of diseases. And ultimately, like any tool, any tool could be used for the better or for the worse. But if you use it correctly, you'll be able to improve productivity of people that are now doing -- perhaps taking many hours to achieve a task, can now achieve many more tasks in the same amount of time with augmentation from AI.

MR. WEST: Carol, your view on these issues?

MS. NGUYEN: So we very much think about AI from a human-centered perspective and on this question we think about it the same way, which is that AI will impact jobs, both the nature of the kinds of jobs as well as the nature of work itself. And

so what's really important is to be human-centered about this and how do we work with people who will be impacted, first of all, to make sure that they're trained appropriately.

So just to share with you some statistics, right? Something about the fact that 65 percent of children entering primary schools today will end up working in completely new job types that don't yet exist. About 50 percent of the subject knowledge acquired during the first year of a four-year technical degree is outdated by the time students graduate. So there are some fundamental changes that's happening both in terms of the types of jobs that's being available as well as the kind of work environment, for example, some of the crowd source work.

So from that perspective I think that's where we need to be paying a lot of attention, which is, you know, from the elementary and primary schools up to teach STEM skills. That doesn't mean just math and science, but the ability to think critically, the ability to have empathy, the ability to have collaborative work, those kinds of things, and the ability to adapt and have flexibility to change because we know that skills needed will change. So this also has implications, for example, in education programs. It's no longer just a four-year university degree, but it's about how can we use AI to identify the kind of skills that will be needed? And then how can we use AI to provide training? How can we use AI to look at different career pathways?

So a lot of the time we talk about AI as a problem, but I think AI really needs to be looked at as also part of the solution. So I wanted to put that out there, as well. But it's very important to be focused on the human. It's human-centered rather than, you know, we can argue about what's the net job loss or the net job gain. Let's focus on the human in this new AI-driven society.

MR. WEST: Okay, one more question and then we'll open the floor to

questions or comments from the audience. And the question is, who should decide on the future of AI? Right now America is pretty libertarian in its approach to emerging technologies. Companies have a lot of leeway to deploy new solutions. Should we stick with this general approach? Do we need new laws, new regulations, or new ways of thinking about it?

MR. FLEMING: So we heard a little bit in the previous panel the view that it's a bit too soon to understand specifically the legislative and legal changes that might be required. I think there's certainly some truth to that.

But I do think what's important is that each of our organizations, and I know we all are, have our own set of ethics and principles that we adhere to. From an IBM perspective, we're very much focused on three principles really that artificial intelligence is intended to augment human intelligence; number two, that the data and the insights that we have belong to the creators of the data, which is I know a controversial statement these days given the public discourse that's underway; and number three, the focus on continuing to build skills and the development of capabilities, much as Carolyn was alluding to.

So we have a very strong focus on the ethics and the principles that underlie the deployment of AI solutions and what that means in terms of their applications.

MR. WEST: Amir?

MR. KHOSROWSHAHI: So I agree with your statement. I would like to reinforce that what's really nice and why I'm so optimistic about this incredible explosion in the use and development of AI is that the academic and research community, which is largely driving this, has been very forward-looking. And this is clearly evident in

conferences you go to. At academic conferences you usually have talks by researchers about algorithms and innovations, but in the last two major conferences on AI that I've gone to there's been a lot of attention spent on how AI will influence work. How do you address privacy issues? How do you make your models more transparent? How do you make them more robust to adversarial attacks? And it's quite surprising how forward-looking the -- how good a steward the academic and research community is in this area.

And many of the large mind shareholders in the research community are actually at places like Microsoft, Intel, Google, and others. And again, at these companies there is a strong impetus driven by the researchers to be really good stewards of the technology and be self-regulating.

So I'm actually very optimistic. And I think, again, the people who created the technology are also really cognizant of public policy issues. So that's somewhat unusual, I think, in research.

MR. WEST: David, should we continue the current approach/

MR. SILBERBERG: Yeah. I think ultimately it'll be the public that decides how it gets implemented. We have great stewards, as you say, from some of the top organizations, top research organizations, also top academics. People want to do the right thing and people want to help society for 99 percent of the people that work in this area.

It'll be a matter of understanding what's accepted by the public, what's usable by the public, how it enhances their life. And if there are abuses, there will be policy recriminations for that and people will come back and start with legislation to address those abuses. But I think for now, people are doing the right thing and they're achieving great goals.

MR. WEST: Carolyn?

MS. NGUYEN: So this morning there was a lot of conversation around shared dialogues. As a company we strongly believe in that, that there needs to be dialogues between policy stakeholders, the academic community, business, civil society together because each of us bring a particular perspective to the issue.

Civil society can bring up and raise issues with regards to human rights, for example. The academic community can help us think about what's the way in which technology can be a part of the solution and we work together very closely with the academic community. And then government can identify what are the policy issues.

And I think there was an earlier question today that said is it too late? I think in AI we're actually doing this at the right time. The technology is still developing. There is huge opportunities to shape the way that it's developed further. And we all really need to be at the table and contribute to this conversation, so it needs to be a multi-stakeholder conversation. It also needs to be an interdisciplinary conversation. And that's where we can start to identify what are some of those unintended consequences as the system is being designed, architected, and deployed.

There also needs to be a lot of sharing of best practices. And that's why we formed the organization such as Partnership on AI. And the notion is how can we share practices on these very, very difficult issues, such as safety and reliability, transparency and accountability, inclusiveness, security and privacy?

And also, how do we address the issue of bias? Fairness is sort of what do you do once you've identified bias? And is that bias inherent within society or is that bias a part of, as Susan pointed out earlier, a function of the data set that you've chosen? So I think this really needs to be a multi-stakeholder conversation and a wide-ranging

dialogue.

But I think that, at the same time, the U.S. is also not as active with respect to AI policy discussions as other countries in the world. And I think that's something where we really need to have a strong conversation with respect to how do we establish competitiveness in this area and, furthermore, longer term research on some of the issues. There are reports and recommendations on this that I think really needs to be acted upon.

MR. WEST: Okay, let's open the floor to questions and comments from you. There's a gentleman right here who has a question.

MR. WINTERS: Thank you.

MR. WEST: And give us your name and organization.

MR. WINTERS: I'm Steve Winters, independent consultant. I just wanted to -- I'm not an expert on AI, but I do try to follow the discussion. So, for example, I wonder if you're being too hopeful as a whole on the panel, the issue of keeping the humans in the loop. So I'd like to get the reaction to the other argument that's made.

For example, the radiologist case that you mentioned. Probably today that's absolutely true, the radiologist plus the automated reading of the X-ray or whatever is better than either one alone. But in other cases things have moved along.

For example, in chess-playing computers, there was a time when the chess-playing computer plus a chess expert was better than just the chess-playing computer. But now that the algorithms for the chess-playing computer have improved, if the human gets involved in the current chess-playing computer, he actually makes the result worse.

Same thing with Go. The Go was originally based on the machine

putting in all the human experience with Go as part of the training. The current version of the machine finds that if you put in all human experience on Go it actually makes the end result worse than the machine they have.

So the tendency --

MR. WEST: Okay, can we have your question?

MR. WINTERS: There's a lot of evidence that says human -- that the humans are going to be out of the loop as things develop.

MR. FLEMING: Can I try?

MR. WEST: Sure.

MR. FLEMING: I don't know how many Go players there are in the world, but let me share with you the little I know about the radiology profession. There, first of all, are a very, very large number of images being produced on a daily basis globally, to the extent when I talk to my colleagues in the radiology profession the concern is the ability of radiologists to keep pace not just with reading the images that are being produced, but to provide the appropriate clinical diagnosis for patient care. So the ability to provide greater productivity to the radiologist is enhancing the care delivered to the patient as a result of being able to focus on those images which provide the greatest risk. Carolyn put it well talking about patent recognition, recommendations, and prediction. And that's what the tools of radiology are intended to do.

The second aspect around radiology is the demographics of the profession. Demographically the world is challenged generally. We're getting older. The labor forces are growing more slowly and it's impacting the medical profession just as it is every other profession. Some of my radiologist friends will say it's not just the total number, but it's the geographic distribution. There are more radiologists in the street

where the Dana Farber Cancer Institute is in Boston than in all of the country of Tanzania. So being able to provide the care globally and clinically appears to have a significant probability of being enhanced with the tools of radiology.

MR. KHOSROWSHAHI: There's a really excellent article, following up on the radiologist thread, by Erik Brynjolfsson in the February issue of *Science*. I don't know if you're familiar with it. And what he and his co-author do in this report is they go through a wide variety of use cases of AI and how much the machine learning technology will be able to replace the human. And it was quite surprising to me that even in the area of radiology, I study computer vision and I work on volume metric data sets and MRI images and all sorts of things, it's quite unintuitive that the machine learning is actually a small part of the task of a radiologist; that some of the things that are really difficult are communicating with the patient, just the commonsense aspects in addition to the things that you mentioned that AI cannot replace.

And I think in cases where there's fear of AI replacing a person, I think it's important to go and look at actually all of the tasks that are involved. In the case of a radiologist, not just looking at the images and detecting a tumor, but all the things that it entails being a radiologist is surprising and that it actually cannot be replaced by an AI.

MR. WEST: Right here's a question. There's a microphone coming over to you.

SPEAKER: Good morning. My name is Nicholas. I lead the Future Society. Thank you so much for a very insightful conversation.

I'd like to build upon your last point, which is that when this relationship between substitution and enhancement is engaged, and it is engaged, how do we look at the fact that what we may be replacing in terms of tasks within an occupation is a highly

productive task which generates a lot of value, which get transferred?

The case of the radiologist is a very interesting case in point because what remains which the machines have not been able to replace is something that could be in the current economic paradigm judged as low value. And, therefore, in terms of value, you can translate that into wage and, therefore, income.

I know it's not a question -- you know, I'm asking this because it's a big question. How do we, from a policy perspective and from a corporate social responsibility perspective -- that, too, at a scale which seems to be a more global than it is local, as you have pointed out; Microsoft serves global consumers and not U.S. citizens -- how do you see that problem arising? And how would you address it from a CSR perspective and from a broader governance perspective?

MR. WEST: Good question. Carol?

MS. NGUYEN: So, I mean, I think that there is no one answer to that question because a lot of what you're -- so there are two points that you are making, so let me just make sure that I repeat it. One is that you're saying that AI can replace tasks that are meant for automation, which would then increase the value of more the human aspect of the task. And that I completely agree with you.

Now, I think in terms of being able to ensure that those tasks get highly valued and that it's deployed in such ways and that these professions really get the value that they deserve worldwide, I think these are conversations that we need to have, you know, in the different countries that we are involved in. But we're completely in agreement with you that AI automates tasks and not jobs at this point in time.

And that's why in terms of education, it's going to be really, really important to emphasize what are the human qualities? What's the way in which people

can collaborate better, can look at alternative solutions, et cetera?

And then also to answer the gentleman's question earlier, these are systems and there needs to be -- especially when they're deployed in sensitive applications, such as radiology, financial services, employment decisions, et cetera, there needs to be an appropriate governance level involved to ensure that we really do truly understand what is it that the system delivers. What is its value of false positive as well as false negative? And all of those really need to be taken into consideration as part of the governance of deploying these systems.

There's a tendency that says, you know, it's a technology, so it knows it all and it's better than human beings. It's not. It is just a tool. It's a computational tool that needs to be a part of I think you used the term ecosystem.

MR. WEST: David?

MR. SILBERBERG: So, yeah, I'll agree with the panelists here. I think it's ultimately comes down to accountability and responsibility. So, for example, a program like AlphaGo or Deep Blue or something like that, there are very little consequences to that machine losing a game of Go or chess. However, if you go to an oncologist and they come up with a -- using machine learning entirely and they make a false prediction because there are always false positives and true negatives, and they decide not to insert themselves in the loop, they are ultimately responsible. So ultimately, you know, it really depends on who you go to and ultimately somebody taking responsibility.

And as Amir said, it's an end-to-end system. AI is placed in different parts of the end-to-end system, but people need to control the system. And at this point, there's not an end-to-end AI system that controls everything.

MR. FLEMING: So for the rest of the audience you're referencing two pieces of research that I'm sure you know well. One is the work that David Autor and his collaborators have started actually many years ago distinguishing between occupations, which a relatively stable structure over time, and tasks within those occupations, which tend to change at some given rate and pace. Recent work by Daron Acemoglu has begun to look at how those tasks get expanded or contracted over time.

The other body of work is Jim Bessen's work at Boston University where he talks about the remainder principle, that there are certain tasks that are automated as each technology epoch comes along, but there are certain tasks which cannot be automated either because of the technology itself or because of the business case, the incremental value of the last bit of automation.

And so the debate is, to frame the debate, is what is the value of those last un-automatable tasks which require the human effort? Some would assert that that's where the human effort achieves its greatest value in terms of reward.

Jim Bessen's work has shown historically it has taken time for the labor market to adjust and provide the higher levels of compensation. But we're certainly funding a lot of research in this exact space with David and Erik Brynjolfsson and Jim, as well, to understand these labor market dynamics and how they're beginning to roll out over time.

MR. WEST: Other questions. In the very back. Actually there's a microphone coming over to you.

SPEAKER: Hi. You had mentioned something about robots being unable to pick up a cup. And I was wondering if you're familiar with Hanson Robotics and Sophia and other companies, such as SoftBank and Italia. I think that that may be a

misunderstanding. I think that robots are there, and we're talking about humanoid robots. And I'm wondering if there's a way to fit humanoid robots into the conversation as well as augmentation, human augmentation, and the incorporation of neurotechnologies or nanotechnologies into the body that would or could augment the human mind or destroy the human mind; that would be artificially unintelligent, something that could make us -- something that could block firing between signals and, therefore, be used to depress the human mind. Thank you.

MR. KHOSROWSHAHI: Is that addressed to me? So on the question of picking up a glass of water, my point there was that it's non-intuitive how difficult that task is. There are robots that can do things like pick and place, but, again, we're still very early on in these settings are really difficult.

Again, robotics has come along quite a ways, but if you go on YouTube and look at the latest robotics competition where many of the best academic labs come representing their robots and their robots have to do simple tasks, like get out of a car and open a door, just look at the YouTube videos. It's lots of hilarity ensues when a robot tries to do that. I'm not deriding it. I like to point out that these tasks are incredibly difficult and we take them for granted. We don't know -- we know it's Pollyanna's paradox.

On the questions of incorporating robotics into the mind, I'm a neuroscientist by training and I specialized in computer vision. And we did a lot of work in trying to figure out how the brain does processing and vision and motor cortex and other areas that could be relevant to enhancement by robotics. And I would say in neuroscience we're even earlier on than in the AI space. It's one of the reasons I switched fields because it was so hard.

We don't have enough understanding of how the brain works to actually do things like what Elon Musk's potentially doing, like sticking something into your carotid artery and it goes into your brain and something incredible happens. We don't even have a basic understanding of how early vision works. How I detect my hand moving in front of my eye, even that is largely unknown.

So I think it's just too early on to address these questions. I know you disagree, but I've been there. I studied neuroscience for eight years.

SPEAKER: (off) because AI is (inaudible).

MR. KHOSROWSHAHI: Absolutely, I agree with that.

SPEAKER: (off mic) we are very libertarian, unfortunately.

MR. WEST: Actually, can you use the microphone? Just so our webcast audience can hear your question.

SPEAKER: We are very libertarian, unfortunately, in this area. We know that if you're a capitalist, you want to have your laboratory, you can and you can do research and you don't have to share it with anyone. You can go overseas, you can develop whatever you'd like in Hong Kong. Maybe you're in Taiwan, maybe you're somewhere in Finland, but we know that we are behind in this country and we know that we're not hearing what we should be hearing.

And you're in a huge multinational company. You have a lot of information and it's not being shared. YouTube is not the source for educated minds. We know we're not the only -- you know, we have a Silicon Valley and so does Russia and so do many other nation states. We need to hear that information. We need to know where we are. We need to be able to protect our biologies and all of the technologies that we are required to interact with on a day-to-day basis.

We were just hearing earlier how vulnerable we are to cyber-attack. Why would we invite AI into our industries at the level that we will be and have been considering how subject we are to attack?

MR. WEST: Okay. Any responses to that? People who are skeptical of what you're saying, what would you say to them?

MR. SILBERBERG: So I think we're not as advanced as you may think we are, so, you know, it ultimately comes down to fundamentals, really fundamentals of math and computer science. There's improvement. There's constant improvement and there's constant refinement and constant new approaches, but we're just not there yet.

MR. WEST: Carol?

MS. NGUYEN: I want to come back to the need to have a lot of these dialogues. Right? In many ways, people say, well, you know, what happens if superintelligence is here? The way I look at it is that we're part of shaping that future. We're part of creating that future. So the more that we can talk, the more that we can create solutions that can counter whatever are the issues that are being seen.

So I just want to come back to that because if technology can create -- can have unintended consequences, technology can also be created to detect those unintended consequences and mitigate them and address them. And that's one part of the conversation. That's why I do want to go back to the importance of having those dialogues at this point in time with everyone -- with all of the different stakeholders at the table.

MR. FLEMING: I just wanted to repeat the comment I made earlier on the commitment that we have as an organization to ethics, privacy, confidentiality, and skill development.

MR. WEST: Okay. Right here, this gentleman.

SPEAKER: My name is Kumar and I was in research and development at DuPont till I retired. And I can see AI applications in applied research. Do you think AI can ever do any creative work, like basic research?

MR. KHOSROWSHAHI: So in the area of AI there's an area called generative models. So the machine learning today is taking lots of data, understanding the statistical properties of this data, and being able to do certain things with this data, doing inferences, telling whether a cat or a dog is in an image. But one of the things you can do is you can actually sample from these distributions and you can hallucinate. So if you have a very good understanding of the visual world, if you have a good model for the visual world, you can actually ask your model to hallucinate the scene, a face of a celebrity, even voices in different languages and dialects. And then there's also artists who are getting involved and using generative models they're called to create art, to sample from these distributions, and it's quite remarkable what you can generate.

And it can actually be applied to engineering. Someone made a heat transformer using a generative model that had this really intricate and non-intuitive structure, how to dissipate heat efficiently, so a combination of engineering and art.

MR. SILBERBERG: So I'll just say, just to add to Amir's comments, there's a whole area of reinforcement learning and it goes back to games like AlphaGo where they played themselves and they learned strategy and they develop strategy beyond humans, what humans had thought of previously. So computers are learning and they're learning how to learn and they're learning to be creative.

MR. WEST: In the very back there's a gentleman with his hand up. There's a microphone coming up from behind you.

MR. FRIEDMAN: Thanks. Josh Friedman from AAAS. Amir, I have a question for you in your space. There's basically been a lot of conversation about the AI competition between the U.S. and China. And today, both on this panel and the previous one, there's also been a lot of conversation about differing levels of responsibility and accountability in AI. Do you have any concerns that the way we attribute responsibility and accountability here in the U.S. might actually slow the progress from semiautonomous and sensor-aided vehicles towards full autonomy in a way that it might not in China, in a way that actually enables China to gain the learnings around autonomous vehicles much faster than we will here?

MR. KHOSROWSHAHI: I'm going to actually defer that to someone else on the panel and they can fill it in. I mean, I can make an answer to that. It's an excellent question. So are companies in China, for example startups in China, less hindered than companies in the U.S.? I'm not sure that's really the bottleneck for AI progressing. It's quite a challenge, again, I talked about picking up a glass or driving a car. There's quite a lot of challenges that we face as engineers and systems developers and solutions developers that don't have to do with limitations imposed on us by regulatory bodies and so forth. I'd like to just answer that part of it, but does anyone else have comments?

MR. WEST: Well, maybe I can address that part because we've done papers on driverless cars in the United States and China, and interviewed people in China on this. And it's interesting in the sense that when you think about the policy and regulatory challenges here on autonomous vehicles, the problem for the manufacturers is much of the transportation space is regulated at the local and state levels in terms of how you define drivers and what the rules are. And so American federalism creates a complication in terms of states having very different kinds of rules.

In China, the issue is not so much federalism, but they have about a dozen different national agencies that regulate different parts of the autonomous driving space. And the people there complain about these agencies and the government oversight, and it's limiting innovation and they have to get permission from so many different people. Many of the Chinese companies actually are now doing their road testing in California because they cannot get permission to do the road testing in Beijing and Shanghai. There are off-road testing that's going on there, but not here.

So there are challenges in different places that are going to complicate the path going forward.

I think we have time for one more question. There's a gentleman right near the back there.

MR. KYSTREVEV: Hi. My name is Kulov Kystrevev and I'm from the 21st Century Wilburforce Initiative.

MR. WEST: Can you speak up just a little bit so I can hear you?

MR. KYSTREVEV: Yeah. And my question's actually related to China issues. It's been mentioned a number of times using AI tech for privacy. And in China, obviously, there's a lot of censorship going on. And recently they made it illegal to use VPNs. How are technologies being created and developed to sort of circumvent the human rights and censorship kind of opportunities that are existing in some of these more authoritarian states?

MR. WEST: Well, I make, again, one quick comment on that. China's certainly moving forward with a number of emerging technologies, but one in particular is the use of facial recognition software combined with AI systems and combined with video cameras. So there's a fascinating example just more than a month ago of a guy who the

police were looking for, he knew the police was looking for him, so he's kind of laying low, not really leaving his house too much. But one weekend in his hometown there was a concert with 75,000 people. He assumed he could go to this concert, not recognizing that the combination of the cameras, the AI, and the facial recognition software, they could find him out of the crowd of 75,000 people, which they did and they arrested him. So that's kind of a very vivid demonstration of how they are pushing the envelope, employing AI into law enforcement.

Here we use it, but we often use it after the fact. Like, you know, if there's a terrorist attack, then we go back, look at the cameras, find the suspect, and arrest that person. We're not so much doing it before the fact. There is controversy over the use of predictive analytics, but kind of our approach is still pretty different from how they're doing it.

I think we are out of time, but I want to thank your panelists for a terrific set of insights. I want to thank Martin, Amir, Carolyn, and David. Thank you very much for sharing your comments with us. (Applause)

MS. NICOL TURNER-LEE: All right. We're going to get started with the next panel. Hello, everybody. You know, the Caps are about to celebrate a big parade here. I think we can be a little bit more excited, right? I told people I'm not dressed for the occasion today as I got out of the Metro.

We want to thank you again for spending your time here at Brookings and this very provocative conversation that we've had all day around artificial intelligence. My name is Nicol Turner-Lee. I'm a Fellow in the Center for Technology Innovation here at Brookings. My particular research portfolio, digital inclusion and I also work on regulatory legislative issues related to AI algorithmic bias, as well as automation. So very

happy to actually have this conversation on the governance side because that's a big part of my portfolio which is regulatory and legislative policy.

We are joined today by three very distinguished people, and I will just do a brief introduction of their name and who they are so we can jump right into the conversation, I think. As we become the tail end of the entire day we've got a lot to sort of unpack from the other panels that actually went on today.

The Honorable John Delaney is seated right to my left who is a democrat in the Maryland area at the U.S. House of Representatives. Thank you, Congressman, for being here. Nicolas Miailhe. Did I say that right? I tried. I'm from New York. I have a very bad R, but I was trying Nicolas, I tried. Who is the co-founder and president of the Future Society and a senior visiting research fellow at Harvard's Kennedy School of Government. And Julia Powles who is a research fellow for the Information Law Institution at New York University. So let's actually give them a round of applause for joining us today.

So I've asked all of you to sort of start this conversation with just some general remarks to sort of frame where we're going when we look at the legal and policy implications of artificial intelligence. And for those of us that have followed technology issues over the past this is sort of the new trend, the new emerging technology that in my ways, Congressman, reminds me of when we started talking about privacy, when we started talking about even the evolution of the internet.

It's this new discussions and when we have new things we then have to look at the governance question. So I want everybody to sort of start with is it too early? Do we need a legal and policy framework when we're looking at AI? Congressman, start with you.

MR. DELANEY: Well, I think it's not too early. I think one of the problems that our government has had here it the United States is we have not been particular good at managing change. In other words, change happens. It's driven by the private market, innovation is extraordinarily positive, but the job of policy makers is to kind of look at how the world is changing and then update the basic institutions in society for that change which doesn't mean making government bigger or smaller. It just means making it smarter and responsive to how change has occurred.

Obviously, technological innovation has been an extraordinary blessing in all of our lives, but it's also created a lot of challenges for specific individuals, it's created additional demands on our education system and our workforce training system. It's created issues around privacy which we're, obviously, going to talk about significantly in this panel. And the role of policymakers is to try to understand these things and then update these institutions in society.

One of the reasons I found the AI Caucus in the House of Representatives was to create a forum for us to actually have these conversations. Our first bill which is bipartisan, the Future of AI Act, basically has the Department of Commerce do an evaluation of how artificial intelligence impacts our society. And, you know, the reason we did this is because it was our view that if you go outside of government, if you go to business, academia, the non-profit world they are appropriately obsessed with how this change is affecting everything, and they're doing things to plan for it.

The federal government has largely been ignoring change and continues to kind of re-litigate battles of the past instead of focusing on the most important thing which is the future. Which is why I think it's time for us to start, you know, putting in place

the framework for this stuff to continue to be a blessing, but make sure it unfolds in a way that make society more just.

MS. TURNER-LEE: That's right. We'll come back to the AI Act.

MR. DELANEY: Sure.

MS. TURNER-LEE: Because I want to unpack that a little bit when we look at the various aspects of. Nicolas, what about you?

MR. MIAILHE: Well, building upon exactly that I would like to, again, reinstate the fact that the AI revolution inextricably intertwines opportunities and challenges, number one, and that's very important to understand because as a result the question which is asked to us and we come back to the question of the us, the we which is changing. It used to be very local. It's a global one.

The previous panels that we've been listening to, you know, have brilliantly exemplified how the question of the we is changing from the we of the citizen to the we of a consumer which is not only national, which is global. With interests that are not only frictioning, but at times, clashing. That's the first point I'd like to make.

And the second point I'd like to make too is so, indeed, it's never too early to start thinking and working on the governance framework of this revolution. Why? Let me paint the picture for you.

This revolution has been framed by some, especially in Germany from the World Economic Forum, I mean, Switzerland and Germany as nothing less but the forced industrial revolution powered by the rise of artificial intelligence. And the ways in which it defers from previously revolutions, industrial revolutions is that it's more global. It's more interconnected. So the ways in which we are interdependent is very important.

And as a result, from my perspective, what happened in Canada

yesterday is problematic. The fact that President Macron, for example, is demanding and putting on the table proposals for more collaboration in the governance of AI. Not regulation now, collaboration, proposing the rise of what we call an IPCC for AI, and inter government panel for artificial intelligence so that we agree on a strong base of fact, base of matter of fact over what do we mean by artificial intelligence.

We've seen this morning how options, definitions diverge, and what are the dynamics and the consequences? And those dynamics and consequences are a new economic paradigm. The velocity and magnitude towards changing it seems that the time space at which these revolutions are speculating into society's compressing.

And the last point I would make and that's a question through which we can frame the quest for this governance framework. It's not exclusive. It's not a silver bullet, but one of the things that we're working on at the Future Society with IEEE is asking the question of what kind of decisions and how should we delegate to machines? Mind you, this remains a social technical system, a complex social technical systems, but there is this relationship between humans and machines and delegations.

What are the principles? What are the values that should drive these choices over what we delegate? And I come back and finish my point where it became which is that if the priority of, let's say, (inaudible) is to expedite the cost of development and provide access to credit, micro insurance to a billion people, and the rise of black box algorithm creates enormous productivity gains to provide access to capital, but at the cost of sacrificing privacy then we have a question to solve. And that's not an easy one to solve, but that's imperative for us to solve it.

MS. TURNER-LEE: Thanks, Nicolas, and we're going to come back to all this. My head is spinning and my notes are writing. Julia, what about you?

MS. POWLES: So I wanted to reflect a little from the two panels we had before because, you know, one position I have is that I think we're in somewhat of a state of exception about AI. Both about the science, I mean, I appreciated Carolyn's fairly sober definition of what we're talking about here which is systems that are very good at recognize patents, very good at classification. In a way it's statistics with a slant.

And I think we're affording it this huge scope that we, you know, it's going to solve all of our problems. It's excellent at matching, you know, a particular query to a particular response, but I think that sort of across the realm of human endeavor there's a lot of other tools and techniques in addition to statistics that we may want to apply.

So I think a bit of a caution about the science itself, and also about the governance. This idea that AI, you know, the question even this idea should we ask, you know, should we govern AI. I feel like well, why shouldn't we govern AI? Like, why should it be exceptional in the realm of science that it doesn't need to be touched by, you know, ordinary rules.

And I think that there's already a baseline of rules that apply to artificial intelligence around discrimination, around tort liability and so on. And I think that the reason we sort of have some of the debates we do is because there's some bigger dynamics at play that actually are much harder to solve. So there's big questions, I think, about shifts in power. And it's quite difficult to have conversations, I think, about AI without acknowledging that there's huge capital and, you know, new entrance major technology companies that, in many ways, are more powerful than states, and how you deal with that in a world without boundaries.

So I think I, you know, coming from the academic community I think there's some conversations that sort of are the problems that we can grasp, and then

there are bigger challenges that are much more difficult to grasp. So the ones that we can grasp are things around bias which actually is endemic to systems that learn from the past, run a loop on it and call it the future. And so maybe we need to say sometimes that is not the right solution to a particular problem.

And just that ability to sometimes question the technology's application and what mechanisms we have when we have entities that are developing these systems, can deploy them in the wild which unlike in the domain of medical ethics and food and drugs and automobiles doesn't have any precursor, external sort of third party accountability mechanism. I think that sort of provokes really profound questions of governance that are about what sort of preconditions to we want to have to deploying these system.

And maybe reconsidering, I think, say this conversation about bias is that actually a way of saying, well, when we think these systems are inevitable the only thing we can solve is let's make them a little bit more computationally fair as opposed to saying, well, maybe the inevitability is unfair itself. So I think some of the levers that we would want to think about are much more profound thinking.

Sort of where is the value in AI and where it is coming from, and could we somehow create different incentives. So it's a combination of massive datasets, computer power, and I think that technology, for example, has never been more realizable by public interest kind of sources. Governments have access to the data which, at the moment, in many cases they give away to those that come with computer power. So thinking about the ways that, at the moment, there's no real costs on hoarding data at the time and whether we want to have different ways of sort of responding to that with levies, exclusivity periods, radical sharing practices.

So those are some ideas. I think they're outside the kind of usual you want transparency, you want trustworthiness, we want, you know, non-biased system.

MS. TURNER-LEE: So I want to pick up on that, so I want to share something that I once heard, and I won't reveal the source, but it was interesting about the evolution of technology, and then just sort of unpack what aspect we should be paying attention to because I think you've laid out, Julia, some of those that sort of streams this conversation.

Some would say with technology's evolution that a lot of the design in technology products were between the consumer and the pixel, right. So video games, I'm not gonna say my age, by Atari, Sega Genesis systems, very static, right, way to actually develop technologies. Then over time we saw the pixel, the individual, and then the ecology shift, right. Where we actually now see changes in the marketplace. Amazon, companies changing the way we do business.

Now, with AI we're actually seeing societal shifts. So what you talked about in terms of power structures, bias, you know, just evolutionary shifts that are probably more drastic and dramatic that have a global ramification. This is not an easy place to put governance, right. And Congressman, I'll go back to you and this AI bill.

You know, when we talked about privacy there were some statutes that were off the books that we could actually say, well, with online privacy, you know, years ago when the Obama Administration, for example, took it there's no fair credit report act, the fair housing act, there were things that we could actually look to define it. With AI, as Julia's point is, we can look at governance of bias. We can look at governance in terms of full deployment. We look at governments in terms of technical architecture, data sharing. It's so many layers. Where should we be spending our time because policy

often means prescriptive application?

MR. DELANEY: Well, first of all, I tend to think I mean, you know, I'm fairly focused on this topic AI, as the leader in the Congress on it, but I also don't want to make it seem like this is the only issue we have to deal with in society. So I think we have to put this in perspective, and we have to think of artificial intelligence, in my judgement, as just the next evolution of dramatic technological innovation that has changed every aspect of our world.

So I tend to think of it as across all the aspects and platforms of government we have to be doing basic updates. And privacy is probably where I go to first. Now, part of the reasons I care so much about privacy is, like most people in the room, is I have children. I have four daughters, and I see what happens to them in the online world and I see that we haven't done things to protect them and their privacy in the online world and that's very concerning to me.

And there's some many obvious examples. If you look at this last election, and not to be political about it, but the notion of Russia interfering in our election using social media. The reason they decided to do it using social media is not because they thought traditional media was not effective. Like, when I run a political campaign I put ads up on television. I put them on radio and I put them on the digital platform.

The difference is when I put them on radio and television I have to disclose that I paid for them. When I put them on the digital platform I don't have to disclose that. So the paid for by John Delaney doesn't have to appear. So the Russians did it on the digital world not because they thought it was better, but because they didn't have to say who was doing it. And that's such a simple example of government failing to update the basic institutions of society.

In other words, a couple decades ago we decided as a society that it was important for you, as voters, to understand who paid for political ads so we required disclosures. But we haven't done that in the digital world which is such an obvious thing we should do. But it's such a simple example.

You know, we look at our iPhones and they turn on automatically now when they see us which is great. But also, when we see a movie that we like and we smile it knows that. When our parents call us and we answer the phone and the sound of their voice makes us respond in a certain way it knows that. When it sees a color we don't like it can see that. And that can all become kind of instantaneous messaging to get us to vote a certain way or buy certain things.

And to me, society has a role in that process. Right. That doesn't mean we should be putting the toothpaste back in the tube, but we should be saying to ourselves as government which is, okay, we represent the people at it relates to these platforms. What role do we have in making sure they understand what's happening to them, and what's happening with their data, and that they have some basic structures which give them an opportunity to protect that.

And right now the way it's structured they don't really have that opportunity. So I tend to go there first. That's the area. You know, then there's a military application. It's a whole other discussion that I care a lot about. But that's kind of where I probably prioritize my thought process.

MS. TURNER-LEE: Yes. So starting with the updating. So I want to stay on this governance question in terms of what do we focus on and maybe jump right in to the privacy piece, GDPR, right. Some of you know that the EU went ahead and passed general data protection privacy rules, you know, in the European context all that

we're talking about with AI is not necessarily something that they think they have to have. But at the core of it is, and it goes back to Congressman, you've triggered that, right, is privacy is the first step.

Julia, I want to point to you first and then Nicolas, jump in. Should the United States be looking at a governance structure like GDPR when it comes to AI versus, you know, general data protection when it comes to -- those of you that are not familiar, the GDPR is basically giving consumers back the ownership of their data.

MR. MIAILHE: Among others.

MS. TURNER-LEE: Yes. Exactly, right.

MR. MIAILHE: Among many other things.

MS. TURNER-LEE: Well, yes, other things putting in governance structures, etcetera. But I always say with AI, as we've spoken about, it's a little bit more difficult, right. Because human intelligence, the neuro reaction how do you govern that. So I want to start with Julia then Nicholas jump in.

MS. POWLES: Yes. So I think that what the GDPR is a bit of a response to this kind of (inaudible) issue of we're facing a future where there are going to be systems that we don't really understand that will have increasing consequences for life options for different people. So what it provides, I think the challenging aspect of the GDPR and the 25 year framework that it builds on is a very strict regulation and control of all flows of data.

And that, in many ways, and anyone who's looked at copyright it's a similar thing, like a foundation it doesn't really work for the internet age and that sort of level of control is difficult. In practice, it's enforced in a kind of well, somewhat ad hoc fashion, but it tries to focus on where there's more harm and you can trace then what the

implication should be.

So I think that the level of -- I think most people have some instincts that align with what data protection offers which is that when information about you is processed that you should know about. That you should have some ability to see how it's used. You should have opportunities to contest it if it's wrong or if it's out of date and it doesn't meaningfully reflect you. So those sorts of rights, I think, are ones that are common.

And, in fact, here the U.S. is the exception. There's over 100 countries around the world that have a system like the European system. And what it particularly offers in the case of AI, I think, is strong prohibitions on sort of data hoarding, and also on purpose limitation. So that you can't say well, we have this massive stack of data which is what a lot of companies are doing. We have this information, maybe we can throw some different AI systems at it and we can get some value.

So from a data protection perspective that's very problematic. And what it translates down to is that the individual level that this sort of rights to contest. I think what's difficult is privacy is something that is more of a collective value than an individual one, and I think that it puts a lot of weight on individual shoulders to understand, agitate for how they should be protected and so on. So I think, perhaps, more -- what the opportunity in the U.S. is to think more in terms of what values we want more widely.

And, for example, the situation that the Congressman stated about sort of facial recognition systems that are just appearing. I don't know that if we polled 100 people in the street that they would all like the fact that those systems are collecting that and could be used for any number of purposes. And the kind of complete absence of prohibitions in that sort of space is really, really problematic.

MS. TURNER-LEE: Nicolas, jump in on there because you're right, there's so many other things, but AI and GDPR, just as we have to look at governance and sort of combine that with the U.S. context.

MR. MIAILHE: Well, there's so much to say, but I'll start there maybe. The implication of looking at GDPR as a way to govern the rise of AI is the fact which I think is right. To look at it from a technical perspective, to look at the governance of AI through the data maker.

As you said, and as you have emphasized, the rise of AI does not exist in a vacuum, does not happen in a vacuum. It is part and it is the manifestation of the wider digital revolution which is delivered through new economic models of the online platform of the data accumulating, increasingly the attention economy. Whereby, our attention wingspan becomes the product. You know, we are the product, but when we dig into what is the we in the product these are functions which are behaviors or transaction. Our ability to point our attention and increasingly productive factors of our attention.

When we educate facial recognition, deep global networks of Facebook by tagging those pictures what is bought from us is a bit more productivity than what it used to be. So in that context I think that the right angle to approach is, indeed, the data. And the key hope and bet, let's be clear, it's a bet.

MS. TURNER-LEE: Right.

MR. MIAILHE: And it's a bet with risks implied because the Europeans are regulating from a position of extreme industrial weakness. Extreme industrial weakness. And so they're creating the conditions whereby leading actors in Europe were not very much digitized, are not acquainted with those new responders, and growing the

giants in the U.S., for example, will have the financial well-withers, and the, I would say, organizational strength to adapt, and to adapt and comply with those regulations.

Those who could suffer are small innovators. A bit like (inaudible) those who complain, because that's the value, that's a payment, that's a fee to pay at the end of the day. So we are, as Europeans, because I'm French, we are aware of that. The big bet that we're making is that we want to plant a stake to create a digital market which is based on trust. Trust that in that framework which I described before over what kind of delegations we delegate to machines, and the ways in which those delegations are based on data. The ways in which we entrust data for certain uses to those companies is regulated in terms of consent, in terms of formability or data, and so many other things.

The implications are the following. Europeans want to leverage their 500 million consumers integrated, not sufficiently, but integrated digital market to send a message to the multinationals. And it's no surprise that Facebook, Microsoft, IBM have said and declared, all publicly, and you'll correct me if I'm wrong, that they consider the extra territorial impact of GDPRs potentially something beneficial. That GDPR could become a global gold standard.

And because we have so much in common in terms of values across the Atlantic, the Trans-Atlantic partnership around these values can be enormously, enormously constructive in how we define the global gold standards.

MS. TURNER-LEE: So, I mean, Congressman, I don't know if you want to jump on in this because this part and then we move on, but what do you think? I mean, in the U.S. it was Clinton and Gore that decided in the U.S. to sort of, you know, make the internet much more of a capital exchange. We give our data in exchange to getting something free. We believe in the U.S. in a two-tiered marketplace, right. That

changes. The GDPR came into a perfect storm which is why I think it has so much attention.

MR. DELANEY: Well, but the world changes.

MS. TURNER-LEE: Right.

MR. DELANEY: Right. So, I mean, look, I tend to think it's incredibly important that we not bring too much ideology to this debate. Right, so if you listen carefully you'll hear kind of two arguments around this discussion. One group of people saying don't stifle innovation. Anything the government does stifles innovation. Well, that's ridiculous. Right. I mean, obviously, I believe in a free market capitalistic system.

We want to make sure the innovation is based here in the United States of America, and that we are the leaders in the world. That's incredibly important to our competitive. No disrespect to your country, but as a representative of the United States I want to win in the technology of the future, and I want it to be in the United States of America.

So I don't want to hamper innovation, but that doesn't mean we can't put in place certain protections for our consumers. Similarly, some people see anything that moves and they want to regulate it, and that's a bad outcome. So I think we've got to be very balanced about this. Again, I keep coming back. The world changes and part of government's job is to update the basic institutions of society for that change. Change is generally very positive.

I think the other thing that's dangerous in these discussions are all these, you know, Doomsayers. You know, the Elon Musks of the world were predicting the end of the world based on this stuff. First of all, they have no ability to predict that. Just because he's been successful at building electric cars, and I applaud him. That doesn't

mean he has any better insight into how the future of this is going to unfold than anyone else.

Generally speaking, history teaches us that innovation is extraordinarily positive for the condition of human kind. I think this will be that way as well, but that doesn't mean there's not a role for government to kind of update institutions to protect our citizens, ensure that our country wins in this next age of innovation, and importantly, that we prepare our workforce that they have the skills they need to be able to get jobs and succeed in the world as it will change based on these systems

MS. TURNER-LEE: So I want to go back then and we'll soon take a couple of questions from the audience, but I want to go back to this conversation. Where should government come in? And I want to sort of reflect back on Julia's question of bias in the work that I'm doing here at Brookings and Darrell and I sort of kick the can on which is, you know, to many respects facial recognition does have disparate impact. It has different disparate treatment, and it contributes to inequity. In many effects it has disparity effects we call it.

You know, where the facial recognition or let's just go with the algorithms in the AI that's used for predicting bail and sentencing and incarceration has baked in bias where African Americans, for example, regardless of who smart the science is they still tend to be incarcerated longer because the training data, and you said it earlier, is not necessarily academic. It's sort of rooted at the bottom line.

Countless cases where we've seen face app, photo shopping apps based on European models that basically oppress or credit score stacking, etcetera. Is that the place where government should start? Looking at protected classes?

Nicholas, you said something, in many respects if you're not online

you're actually online because those investments that are driven by AI are not coming to your community. When we look at that I'd just like to ask all of you is that a place where we actually can get some consensus that governance is probably well-needed to ensure that we don't create a massive divide that we've worked really hard to have technology not do which is to help people solve problems, not help people become poorer and unhealthier, and under educated, you know, as a result of their lack of access to it. Anybody?

MR. DELANEY: Well, I would just say three words, privacy, transparency, disclosure. Right. Government has a role in making sure that privacy is protected. That there's disclosure in how things are programed, recognizing you've got to protect certain intellectual property. The people understand, and kind of transparency around actually what the user experience is really all about.

MS. POWLES: Yes, so I think those different examples you said of facial recognition are really interesting themselves. As an outsider to the U.S. system I can look at the criminal justice system and see all sorts of problems, but I think most -- for any of these sort of algorithmic systems that build on top of what we've already done in criminal justice the key challenge is we don't really have very good or any data about crime. We have a lot of data about policing. And so the more that policing which we know to have all of these endemic issues is refined to keep doing what we've been doing it's going to perpetuate, I think, a very unequal state of affairs.

With solving systems this sort of idea that we don't want facial recognition systems that can't capture minorities and other groups I think the challenge there for those who work on these technologies in industry and in academia where a lot of the policing work happens is that there can be really perverse outcomes in making the

systems equal and fair. And I think what's very striking to me is that this sort of whole conversation about bias and fairness takes this very formalistic idea that, like, if we all treat everybody the same then it will somehow be fair.

But, I mean, I actually would celebrate systems that don't capture a proportion of society and maybe we should say, therefore, they're not very good and we don't want to use them for this particular application. Because in the process of making, you know, solving this great fight of computational fairness we create these systems of, I think, ubiquitous surveillance which have all sorts of other consequences. And it's just a sort of very problematic direction.

I think what's challenging is that because we don't have very good systems for regulating when a particular application of technology is desirable, like we don't want people to be subject to, you know, have some metrics around credit that are transparent and applied equally, but around policing it may be different.

And so an ability to actually regulate use which we haven't really proven I think until we can prove that we can regulate that I think we do need to do more of the collection level of data. And so a lot of the systems there's a real question about whether we should be using them at all. And, yeah, I'm just a bit wary about some of them for solving bias as a way of just entrenching systems that then have later consequences for transparency and accountability.

And I just wanted to say one things about transparency which hasn't really come up. There's a sort of real clash where there's corporate secrecy around automated systems and AI really has sort of narrowed the scope for regulation to actually even understand. I think we had comments on both this morning's panels about how important it is to understand what systems are doing. So I think there's an opportunity for

regulation that restricts in the same way as we have under Freedom of Information laws the proper scope of defenses of trade secrecy in response to -- and you can have partial transparency and all sorts of options in order to allow those who are elected representatives to actually understand the systems that they use.

MS. TURNER-LEE: Nicholas, did you want to jump in?

MR. MIAILHE: Yes. I think one thing which is very important. I think the case of algorithmic bias is a great case and point to approach and attack the governance of AI. Articulating the very long term super intelligence versus the (inaudible). In a way, we're asking the same questions. In a way, in solving that problem right, including globally or trans-nationally. We are laying the foundation for solving the next problems.

And it's not, in my view, never too early to think about the bigger problem. I don't think that thinking and preparing for super intelligence which is an act of conviction, not an act of science, is worrying about overpopulation on Mars. I don't believe that because if the velocity of magnitude of the rise of AI is such that the current trend continues we might, for the first time in human history, have to worry vis-à-vis this kind of magnitude of problems.

But I think that the best way to do that to appease the short term very legitimate concerns is to look at what we have now and the algorithmic accountability and governance is a great case and point. To address that I think that one way we need to go about that is try and be very smart. What does it mean by that?

One way in which we are generally not too smart and the we in that case are communities seen at large and societies is to look at sequencing of regulation. What is it that we need to shift from a laissez faire position to a forward guidance position to a hardcore regulation, number one. Number two, how is the fact that, and that's my

personal view, of the view that to develop artificial society that the rise of AI, because of the global dissymmetric oligopoly that is unfolding it cause, in a way, corporate governance, public governance, and technical governance to merge.

So in many ways the work that engineering communities are doing right now to standardize and to define standards and design principle measurability of competence, of accountability, of transparency, and so on and so froth represent sides of governance. And it's very important that they are, and those sides of governance of enhances, recognized, and supported.

And as the same ways as the corporate governance. The ways in which big multinationals are asking the question. In most ways, in very sincere terms in trying to look at this problem initially from a corporate responsibility, and now increasingly from a corporate governance perspective. I think it's a very good thing. And one thing which I heard this morning which is that we need more and more of these kind of dialogues. I totally agree with.

I would qualify a bit more what we mean by dialogue. Let's not be afraid of it. We're talking, in a way, in the most noble way we are talking politics. And we're talking politics with the right kind of stakeholders, and it's very important to not be afraid to approach that question, and not find, you know, fall into the trap of this, which is ongoing, which is this paradigm of a global race for AI. It's happening and therefore, it's very important to be able to upgrade the quality and the volume of these conversations at the global level without crushing very local identities and problems involved in that.

Because the question of AI ethics in this country, in the case of the Lumos case, for example, in access to justice is not at all the same of the case of, as I said before, an Indian follower demanding access to micro insurance.

MS. TURNER-LEE: That's right. Did you want to respond, Congressman, or any others before? I think just to kind of stay on the three points that you all made, I mean, I think that's the biggest challenge with AI when it does come to governance. The paper that we're working on, and I sort of like, Nicholas, the way you framed it. We've done conversations here in Washington D.C. where it's mostly policy people who are like, we don't like the output, you know, it's because it creates this disparate impact, this disparate treatment. It's not enough of a sample.

We go out to Bay Area and they say, but we like the formula, the computation works. This is what people are telling us that they're doing online through their tags, and we're using that natural resource of big data to come up with these assumptions, not realizing that it's the inferences that come from this activity on the web that creates, you know, what the policymakers are saying.

And so I think you're right, corporations are coming up with their own governance, data engineers are coming up with their own governance, policymakers are coming up with their own governance. And at some point, and I'll go back to you Congressman, policymakers are all about protecting consumer trust, you know, the public interest.

I'll ask the question. I always ask this. Since you're standing here I feel like I've got all these people as my witnesses that you won't throw an apple at me, but are legislatures really ready to deal with this topic?

MR. DELANEY: No. I think it's a big problem. I think we saw in the Facebook testimony with the Senate that there wasn't a lot of technological literacy represented. So that's a core problem, but that's manageable because we've had that problem before. And, ultimately, policymakers guided by smart people who are

interested in good public policy helped them get there.

But it has to come -- see, I think there is a little bit of a top down approach that's needed here which is what this country needs, the United States of American needs is a national strategy around artificial intelligence. And it should have kind of four components to it.

The first and most important component to it is what we do to protect our citizens and our consumers. And we've talked a lot about that with respect to privacy and data. There's a basic level of consumer protections, a bill of rights, if you will, for our consumers as it relates to what they should expect their government to do to kind of intermediate between themselves and the technology companies so that they are protected. That's the first thing.

The second thing that the country needs to do is basically look at kind of the business opportunity available to our nation from a competitiveness standpoint, and make sure we're making the right investments in basic research so that we continue to develop the cutting edge technology here in this country and it becomes commercialized in ways that create jobs here. So there needs to be kind of a competiveness angle.

The third aspect to a national artificial intelligence strategy would look at the future of work and look at how these technologies will disrupt the workforce. They'll create jobs. They'll disrupt jobs. Are we actually educating people and training people so that they have the skills they need to get jobs in the future.

And then the fourth aspect would be as it relates to our security, but our homeland security and our foreign policy defense strategy which is the conventional advantages the United States of American enjoys militarily can be equalized very quickly with, kind of, powerful technological systems that rouge actors and terrorist organizations

can use. Have we, in fact, hardened our military and our national security for these systems?

So a national artificial intelligence strategy, in my judgement, would have those four components to it. And if we articulated that without specific regulations, but articulated goals, what we should be seeking as a country. Then it seems to be it would be a lot easier for the legislative branch to actually do its job and work with experts, etcetera, and go through the legislative process to put in place things to make that strategy kind of come into being.

But we don't have that. We don't have that. In part, because of ideology. Right. Some people say, no, no, no. There's no role for government in this. And other people's like, yeah, the government's got to be doing everything. Right. And that's, like a lot of issues we have in this country. Instead of solutions we get gridlock, and that's a problem as it relates to the future because unless you prepare for the future you don't benefit from it as much as you could.

MS. TURNER-LEE: That's right. Congressman, I hate to do this shameless plug, but Darrell West has a book that talks a little bit about ideology. Just came out. If you haven't read this book, you have to read this book.

MR. DELANEY: I've got to read the book. But John F. Kennedy in 1958, four weeks after Sputnik was launched when the country was terrified about us losing our leadership position gave a speech in Baltimore, Maryland where he said we shouldn’t seek the democratic answer. We shouldn't seek the republican answer. We should seek the right answer, and we should own our responsibility for the future. That's what we need as it relates to technology. This isn't a democrat or republican issue.

MS. TURNER-LEE: That's right.

MR. DELANEY: This is an issue for all Americans and we ought to be doing the right thing to prepare ourselves for the future.

MS. TURNER-LEE: Darrell, you were forecasting on that one. I want to give the last two panelists just an opportunity to speak on, you know, again, we've heard the production of a national strategy, particularly that applies to the U.S. Nicholas, you've talked about global. Do you see something more global in terms of a framework and where we go with this?

MR. MIAILHE: I certainly see an ongoing race for artificial intelligence for very legitimate and good reasons which is to capture the upsides, productivity gains, power. So it's a question of power and sovereignty, and therefore, the fact that there are very legitimate national techno strategies which compete with each other because they correspond to communities of interests, communities of values, communities and practice which are not yet harmonized, creates the condition for destabilization.

Not only from a military perspective, but also because, like we've said before, I keep on coming back at this example of the Indian farmers, vis-à-vis the -- let's say the American or the European consumer. These frictions, this lack of harmonization creates tension and probable destabilization or ongoing destabilization. Our work and one of the things that we do is we work with several organizations, including, for example, the government of the EU which has appointed a very young minister, state minister for artificial intelligence which wants to work on laying the foundation for a global governance framework, basically.

And that starts, and we should not shy away from that, and that starts at the point of discussing where do we have common grounds in terms of values. And more often than we think because we are going through a wave of convergence. We are going

through a wave of globalization we can find common grounds. It's about finding those common grounds in terms of those values, and translating those common grounds in terms of design principles, norms, codes of conducts, codes of practice, and so on and so forth.

And every effort that go in that direction, in my view, are very constructive. They all some of them, and that's why I come back to what, as an example, the French president suggested two months ago which is to start by creating an IPCC for it. To come together as a global community to start agreeing on what do we mean by I, what are the dynamics, and what are the consequence?

MS. TURNER-LEE: And I think we have several presidents, right, when it comes to international governance, you know, cross border data flows, all of the data portability. We've been around this conversation before, you know, in many respect I think you're right that there is this local governance that is very much pertinent to the country. And then there is this opinion to do more collaborative work and sharing which comes up with best practices or repository values.

Julie? And then I'm going to open it up for questions.

MS. POWLES: I want to hear from people, but just one. I think it's a very compelling sort of comprehensive strategy. I think it'll all depend on the interrelationship between the first and second part. And often what happens in the piece about how you get the innovation is that all of the parts about protecting the public sort of falls by the wayside and --

MR. MIAILHE: Right.

MS. POWLES: In my view, a sort of real rethinking of the data economy and the opportunities that exist for. To me, it's not that innovative to let companies that

are sitting on hordes of data and are incumbents to keep monetizing it however they can, and there's ways of thinking about those assets that could really spur a lot more innovation and competition. I think that demanding the innovation proceed in a principled manner isn't to stop it. It's to save it.

MS. TURNER-LEE: This have been a valuable conversation. I'm going to open it up for questions. I will recognize you. Why don't we start this way? We'll go here to this young lady and then we'll come over to you.

QUESTIONER: My name is Melissa Cataldo. I'm a student at California State University Long Beach, currently working with Storm King Analytics. So my question is we've talked about how AI is used to detect patterns, and therefore, make decisions. So with the extensive future applications of the technology, especially with automation how do we decide or program ethically debatable decisions within the new advances? Are we capable of determining which decisions should be systemically programmed without bias? And do we establish these determinations through governance or through what methods would we use?

MS. TURNER-LEE: Anybody want to take that question? Go ahead, Nicholas.

MR. MIAILHE: I can take a first crack at that. One way to look at that is really to understand what is this big data-driven machine learning centric algorithmic centric tool system that is I today? Today when we talk about AI we talk about, essentially, not only that, but essentially that.

It means that there is a convergence between big data, growing computing capabilities, and those old, but now high performing, let's say, machine learning techniques, including (inaudible). So looking at how we can extract more

accountability and explainability from these, I would say, system, is not only a question of open data.

Of course, we need to be able to see the kind of data and data sets which are used to train these algorithms. But increasingly, because the computing is done at the core of the hardware we need to also have more open hardware. So, for example, when large multinationals like Google talk about terms of flow as an open architecture which I think is great. I think it's not only a question of understanding the ways in which the algorithm operate. If we want to govern well we need to better understand that type of data that have gone into that.

So it's a question of what kind of data, what kind of computing algorithm has been used, and what kind of algorithmic architecture has been used. And moving from there into a conversation where we look at what are the values that we have? What are the tensions between access and protecting privacy, protecting dignity, due process? These tensions and the ways in which communities and countries look at them are important to go towards the right kind of solutions. But there is no, and there won't be any silver bullet.

MR. DELANEY: And the private sector should understand that unless there's transparency around how these things are done that it won't, ultimately, play out well for them. Right. Citizens will reject it. And let me just give you one example.

Warren Buffet tells a good story. He owns a company called GEICO which is the largest auto insurance company in the world. And he was asked, well, people aren't going need auto insurance anymore because we're going to have driverless cars and they'll be no accidents. So how's that going to be for GEICO? And he said, well, let me tell you the issue with that question. And he said, it'll happen. We have the

technology. But he said imagine a driverless car's driving down the road and approaching it is a car driven by a human being with two passengers in it and the person driving that car has a heart attack and that car swerves towards the driverless car.

On the side of the road, on the sidewalk is a 5 year old girl riding her bicycle. So the driverless car has to make a decision. Does it hit the car that's coming towards it which is the person had a heart attack and it has two passengers, or does it veer and run over the little girl on her bicycle. And someone's going to program that car to make that decision. And his point is society cares a lot about that decision. And unless society understands completely how that decision was made and who programmed it, it will never be comfortable with it.

And that's why when we talk about transparency and the programming of this stuff it's not only something that we should care about as citizens, but I tell people in the private sector all the time you should care about this. Because unless people ultimately feel comfortable with this stuff they may, you know, not realize it's happening for a while, but once they realize the implication of some of these decisions they're going to want to know who made them and they're going to freeze everything until they get to the answer of that.

MS. TURNER-LEE: That's right. So just if I can chime in on your question. They need to hire more sociologists, these companies, because they clearly don't have enough people that understand the world context to actually help with some of that.

We'll go here and then we'll go here.

QUESTIONER: I wanted to thank the panel for a very good discussion. My name is Elliott Horowitz. I used to work at the World Bank, the State Department, and

in the intelligence community. Congressman, I thought I heard you say that the U.S. government has largely been ignoring change. Would you include in that the Department of Defense and the intelligence community?

MR. DELANEY: Well, look, I think the Department of Defense has, obviously, been making very significant technological investments. Right, because that's what it does. But in general, largely because of our preoccupation with a lot of wars in the Middle East I don't think we have been, kind of, resetting our military from a technological standpoint as fast as we could have.

QUESTIONER: What about the intelligence community? They have not been ignoring -- it's hard to say, it's not been ignoring change.

MR. DELANEY: No. I mean, look, I didn't say every single person within every department. The U.S. Government's, obviously, a big enterprise. I think, in general, we have not been good at managing change as a nation, and our policymakers have not been forward looking at where the world is going and preparing our country for that.

MS. TURNER-LEE: Yes. And I would say on that, sir, too, you know, you look at the military and their use and deployment of artificial intelligence and the internet has been much longer than what we're talking about in terms of this commercial market. I think the challenge is it goes back to election piece. That we're used to sort of looking at people playing by the books.

So when you look at the Russian election interference, you know, it almost looks like the worst case of voter suppression because no one was going to Supreme Court to say, hey, wait a minute. They just target all these ads to vulnerable populations.

MR. DELANEY: Right.

MS. TURNER-LEE: And so there's a different strategy.

MR. DELANEY: We haven't hardened our electric grid.

MS. TURNER-LEE: Yes.

MR. DELANEY: And that's a Homeland Security issue. That, to me, is a country not planning for the future because if I was a rouge actor those are the kind of things I would be focused on.

MS. TURNER-LEE: That's right.

MR. DELANEY: And have we done that? No.

MS. TURNER-LEE: That's right.

MR. DELANEY: And that would actually cost about $6 or $10 billion to harden the grid in this country. That's actually not that big of an investment relative to the cost of something happening.

MS. TURNER-LEE: Sir, right here?

MR. MIAILHE: I would like to add something to this point in terms of the relationship between the markets and governments in fostering the rise of new and fresh techno-scientific cycles. In the history of the digital, governments have been the main purveyor of the kind of long term, (inaudible), high risk, capital that has enabled the rise of the internet, the rise of GPS, and we could continue on and on and on and on.

So citizens have had, have and will have a key role to play in driving those techno-scientific cycles. But the difference is that the ways in which those techno-scientific revolutions percolate into society through innovation is, at this point, led by private companies which innovate on the basis of taxpayer money delivered to foster the rise of new techno-scientific cycles. And thereafter, when those innovations percolate

through the market at scale in all societies then it creates challenges of adaptation.

MS. TURNER-LEE: But to the defense of the private sector, I think what we actually saw with the growth of the internet becoming more transactional versus static are these opportunities which is very much part of how the internet ecology has grown for these new startups. Right. So I think your question is right, it's the extent -- I mean, even if you look at the telecommunications act of 1934 we weren't anticipating the growth of these types of companies. There was nobody thinking that information was going to be a transaction -- a commodity.

MR. DELANEY: Wouldn't it be nice if it said 2018 after that?

MS. TURNER-LEE: Right, exactly. Exactly. And that's the point, right, and so I think to your point I think we have to sit back and say all of society has been impacted by some type of industrialization. This is the next wave of it. I think this conversation is very relevant and timely because then we have to figure out what's the proper foundation to actually make it work, and that's with the updating of laws.

MR. MIAILHE: My point is in funding highly disruptive early techno-scientific innovation the government which plays its role, in my view, should pay much higher attention to what we call second and third order consequences.

MS. TURNER-LEE: Yes, that's true. That's true.

MR. MIAILHE: The case of Darfur is a great case. Immense talents, immense long term vision, and a true and certain demand to go slightly beyond national security as what drives us and look at second order and third order consequences so that when self-driving cars percolate into society and deliver major revolution these consequences have been anticipated because the (inaudible) all along.

MS. TURNER-LEE: That's right.

MR. MIAILHE: At least ten years, if not 20 to 25 years.

MS. TURNER-LEE: I see another panel coming out on this. So we're not done here yet at Brookings in this conversation, but you're completely right. So we've got to invite you all back. Now, we can take one more question. Sir, please ask your question.

MR. DELANEY: We should let Julia answer it because she's the smartest person on the stage.

MS. TURNER-LEE: Somebody? Did you want to ask it? We have one more question in the back. If you can, there's a gentleman. Raise your hand. We'll go to the gentleman in the way back and then we'll come to the gentleman a little bit forward, and I think the last question will be this question over here. Okay.

QUESTIONER: Hi. Thank you. This is a very interesting panel. I actually worked for Delaney Campaign 2012, so it's a pleasant surprise. I was going to ask about larger -- about a question of a large monopoly. That Amazon owns not only owns a large part of the web services that drive a lot of websites, but also owns -- but, I mean, also has fingers in Whole Foods and the Washington Post. And that's just one example. I mean, Google has a whole host of companies, or rather Apple has a whole host under it as well.

And you have these huge data silos and they -- and even if one were to have sensible legislation that would allow portable data where would it go? Can you address that issue a little more? Thank you.

MS. TURNER-LEE: Do you all understand the question? I think the question is would you raise -- I heard the competition word come up here on the panel. Sort of like looking at the competition. I mean, Amazon actually just was reported was

selling some of their algorithms. I don't know if some of you follow that. But if you could answer that question in terms of market competition, concentration, and how this actually sort of plays into the data silo stuff.

MS. POWLES: Well, I think it's very telling that actually the most progressive thinking in how to deal with tech is in competition which has traditionally been kind of a backstop when you have to reach for anti-trust. But anti-trust has a few issues that I think haven't really adapted well.

One is just when you don't discriminate on price, but you have massive datasets and data hoarding that you then can use to offer greater advantages that are free. It's really not a very easy thing for ant-trust to grip on. There's some excellent work, I'd refer you to Alan Greeners, Maurice Stuckey, Frank Pasqual have written a lot about the implications. Lean Kahn here in D.C. on Amazon.

So this is, I think, where a real opportunity I think here the U.S. can really lead. There's been a lightened feeling about Google and so on, but what we do about Amazon and there sort of AI rise. And some of the acquisitions that have been problematic in retrospect around, like, that WhatsApp acquisition by Facebook, and so on. I think will be crucial in the AI age. So, yeah, I think this is a really important area of policy.

MS. TURNER-LEE: So what I want to do is I want to take this question, the second question. If you both will hear both and then if you all can sort of answer that with a closing comment. So this one and then the gentleman back there.

QUESTIONER: I'm Steve Winters, independent consultant. I think I'll direct this to Julia. Actually, just around the corner last night General Hayden said this existing systems, AI systems understand you now better than you understand yourself.

And that's now. We don't have to wait for super intelligence, and those existing systems are getting better.

So the problem is -- and, by the way, it's not just because I click on certain things on the internet that it understand me better. It's because it has big data on the whole population and it can compare me to people who are similar to me and come to conclusions. So it's the big data plus the algorithms. So how do you propose to address the danger that when you have systems that understand me and everybody else in the population better than we understand ourselves that opens a possibility of manipulation of the populations on a scale that's never been conceived of before? So, you know, how would one prevent that? Would it be a legal issue or how?

MS. TURNER-LEE: And so that question, Julia, and we'll just get to the last gentleman there. We'll have you all summarize your response.

QUESTIONER: Hello, Jessie Wu Aledo Consulting. So in 2014, Professor Ryan Kaylo published in Brookings an essay calling for a federal robotics commission. This would just be an advisory group. It wouldn't have rule-making authority, but it would situation expertise on AI and robotics in the federal government. And so I'm curious what you think about that? That was, you know, four years ago. Are we sort of beyond the point where that kind of light touch, just having an advisory committee is useful or is that a useful thing still?

MS. TURNER-LEE: Okay. So, Julia, we'll go back to you answering that first question.

MS. POWLES: Yes. Well, I think it's really important to disentangle, and a lot of the stories we tell about AI dictate, I think, what future it will have. I'm sure if you believe as -- you know, I don't know you and a system may know an approximation, a

derivative version of you based on your activities. And if we, I think, build systems that define how we navigate the world and how decisions about us our made that depend on all the information about everybody else then we will leave that sort of future, and it will be, I think, a pretty dystopic one.

But if we understand what is truly the case that I think that human autonomy is a real thing and that systems that -- but the architecture of the world around us we have this interplay. And so I think that this is exactly why we're at a point, and I think there's a tremendous opportunity with, sort of, connection of AI with the internet of things, more animated objects in our environment that do dictate our physical behaviors as much as our digital ones to say I don't want these systems that I can't see that are run by, you know, just trying to serve me more advertising and enable greater transactions and consumer surplus to be actually having a fundamental impact on my autonomy.

So I think that is the challenge. There's some excellent research I can send you on this sort of manipulation scale problem. But I think that there's still this opportunity for us to say, well, that is the derivative version of me based on everyone else. It's not me and I don't want the world that is defined by it.

MS. TURNER-LEE: So I'll pose that last question to Nicholas and the Congressman. You have the last word which is around light touch. The gentleman's question, should we go back to light touch? Multi stakeholder process. Are we seeing a pattern here that we should maybe, from this conversation, avoiding, very prescriptive and really start with the conversation to get to an end point on the policy and legal implications.

MR. MIAILHE: That's still one because they are connected. Which is that that's why I'm talking about a new social contract. These systems do not know you

better than you do. They are reconstituting a new you. You lay down digital traces, only traces, and they do not reflect the complexity, the intensity, the granularity of your true self.

Those digital traces then get algorithmically projected to create new solutions and that's why, indeed, the risk of AI and algorithms inextricably connects opportunities and challenges because the ways in which this new self appears to you and society poses new challenges, and the asymmetry of power through which this new self-emerge is potential problematic.

So it's not yourself, it's a new self, in my view, and connecting with the other question. Well, from a U.S. centric perspective I personally miss a lot the Office of Technological Assessment which is this office that is supposed to create a bipartisan strong base on matter of fact based on which legitimate political discussions can happen. And I'm a bit wary of, in a way, trying to find a fix, meaning and administrative independent authority where we need to get to the meat of a very important conversation. That's where I'm a bit -- I think we need that, but I would rather see first the right kind of conversation brought back where democracy's to be played in this country. You know, in Congress. But that's my view.

MS. TURNER-LEE: Congressman?

MR. DELANEY: Well, I think it depends on the issue. I think on privacy we need to be doing some things right now. I don't think we need advisory commissions anymore. I mean, I think the toothpaste is out of the tube on some of this stuff, and there's some real stuff we should be doing.

I talked about one simple example which is requiring disclosure on political advertising. I think doing things to give consumers more protection on their data.

This is real stuff we could do now, updating the Telecommunications Act. Right. These are real things we could be doing now.

On things like robotics, I still think on that issue, I don't think there's any legislative solutions for robotics right now. Right. But I do think it'd be important for the Congress of the United States, where I serve, to be thinking about the impact that these things are going to have on the future of work, and making sure then we are designing our educational and workforce training systems, etcetera, so the people can get the skills they need to have jobs in the future economy.

So I do think it cuts across, you know, what we should do. Again this stuff effects every aspect of our lives and some aspects of government we're woefully behind and we should ask now. Others, we're probably still in the phase of trying to figure out where the world is going, and doing some policy things that are somewhat indirect. I mean, robotics, there's not, like, laws you pass to limit the number of robots that can be in factories, but you do think about how you educate your kids and what kind of career and technical training people should be able to get and how they pay for it, and what's part of the basic social compact. I use compact, not contract. In society so that people get the skills they need to get a job.

I mean, right now we're graduating a lot of our kids from high school and they don't have either the ability to continue their education or the ability to get a job. I mean, two-thirds of the kids that graduate high school in the United States of American are not eligible for our military because of deficiencies in hard and soft skills. There's an example of clearly a public education system that's not preparing people for the future of work as it will change with robotics.

I think having commissions there to actually make us smarter to make

some of those changes I think is a good idea.

MS. TURNER-LEE: So I wanted to say this. Thank you for your panel. Let's give them a round of applause. I want to continue to also stress, you know, here at Brookings, and Darrell, I see with your book if I can actually just -- we're looking at this stuff, and I think in particular we're looking at this intersection that came out most profoundly in this panel which is, you know, the good of AI, precision medicine, education, other decision making, along with the balance of its effect on the economy and competition, but also on people.

And so keep following us. We've got papers. We've got books coming out. And, Congressman, we thank you. Nicholas, we thank you. And, Julia, we thank you, and we thank all of you for giving us your time.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020