THE BROOKINGS INSTITUTION

THE ECONOMIC, POLITICAL, AND SECURITY IMPLICATIONS OF TECHNOLOGY TRANSFER

Washington, D.C.
Thursday, April 5, 2018

**Innovation and Technology Transfer:**

JOHN ALLEN, Moderator
President
The Brookings Institution

RICHARD ANTCLIFF
Special Assistant to the Associate Administrator for Space Technology
National Aeronautics and Space Administration

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

ANTHONY VINCI
Chief Technology Officer
National Geospatial-Intelligence Agency

**Security and Technology Transfer:**

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

CHRIS MESEROLE
Fellow, Foreign Policy, Center for Middle East Policy

MICHAEL O'HANLON
Senior Fellow, Foreign Policy
The Brookings Institution

HEATHER ROFF
Associate Fellow, Leverhulme Centre for the Future of Intelligence
University of Cambridge

PAUL TRIOLO
Practice Head, Geo-technology
Eurasia Group

* * * * *

P R O C E E D I N G S

GENERAL ALLEN: Well, ladies and gentlemen, good morning and welcome to Brookings. I'm John Allen and this morning's panel is about economic, political, and security aspects of technology transfer. I want to welcome CSPAN to this panel. They'll be covering us and our panel will be broadcast later today. And at the very conclusion of this panel we will be followed immediately by the next panel. There's no break in the process. I just wanted to make sure you're aware of that.

Also wanted to announce that if you are unaware and if you haven't muted your cellphone, I would ask you to do that because sometime between 10:00 and 11:00 Washington, D.C., is going to test its cellphone and remote device emergency broadcasting system, which means at some point everyone will look down at their phones. That happens to me frequently in meetings. (Laughter) But let's today anticipate that and not have it be too much of an interruption.

I really have the honor this morning as the president of Brookings of hosting this first panel of three terrific panelists: Dr. Anthony Vinci, Richard Antcliff, and Nicol Turner-Lee. Anthony Vinci is currently the chief technology officer at the National Geospatial-Intelligence Agency, or NGA. And I never miss the opportunity to thank your agency for the terrific support that they have provided to us in places like Afghanistan and Iraq and many other places. So thank you very much for that.

Anthony has a long track record of success at the NGA, serving as the associate director for capabilities and the director of plans and programs

prior to his current role, and has been central to developing the agency's vital public-private partnership efforts. And I think he'll talk a bit about that as we go on.

Rich Antcliff is a special assistant to the associate administrator of space technology at the National Aeronautics and Space Administration, or NASA. Prior to his current role, Rich served in a variety of top positions at NASA and most recently was NASA Langley Research Center's Office of Strategic Analysis, Communications, and Business Development leader, as well as a chief technologist at the entire center.

And Nicol Turner-Lee is a fellow here at Brookings in the Center for Technology Innovation within the Governance Studies Research Program. And Nicol's research at Brookings focuses on public policy designed to enable equitable access to technology cross the United States. She's also an expert at the intersection of race, wealth, and technology, and comes to Brookings after most recently servicing as the vice president and chief research and policy officer of the Multicultural Media, Telecom, and Internet Council and vice president and first director of the Media and Technology Institute at the Joint Center for Political and Economic Studies.

We have three terrific panelists here this morning, ladies and gentlemen. I'm very, very honored to introduce them and to guide this discussion.

We'll be here for about an hour. For the first 30 minutes I will offer some questions to the panelists and for the second 30 minutes we'll go out to you. I don't normally ask our panelists to do introductory remarks, but, of course,

in the first question that I'll ask, which will go to all three of the panelists, if they choose to make an introductory remark they are most welcome to do so.

So with that, let me go to the first question, which is about technology transfer. Starting first with our overall topic of discussion today, technology transfers, be they public good technologies emerging from U.S. Government projects or university research, this has enormous potential ramifications when thinking of the growing tech race that we see as nations compete against each other in areas of big data and artificial intelligence. In particular what comes to mind is the United States and China, for example.

Let's go down the line of our panelists this morning and present the opportunity they get some opening thoughts about do we need a new definition of public good technologies? And what's the U.S. Government's obligations here? This is an important topic and I think it's a good way to begin this overall conversation.

So with that, Anthony, would you like to offer some comments?

MR. VINCI: Yes, thank you. Thank you for having me. Thank you for having the panel, which I think is extremely important at this particular moment in time for the country.

I think looking at technology transfer, I put in the larger context of what is the appropriate role of government working with commercial industry and nonprofits and the wider economic and civil society. And within that, from my role at NGA, I think about national security and strategic kind of consequences. And over history, and in particular since World War II, we've kind of gone through some phases of working differently with industry and working with the public.

And we've invented new approaches to doing that and the entire idea of tech transfer as an approach, uses of FFRDCs, uses of contracts, approaches like CRADAs and OTAs and things like this.

And I think right now we're watching a kind of geopolitical shift, and if you look at the national security strategy and the national defense strategy, we're seeing this shift from kind of the post 9-11 world into a new era of near-peer/peer competition with China and Russia. And so I think what that demands is a new approach to public-private partnerships and within that to tech transfer and seeing tech transfer as a means of strategic competition.

And within that I would include not just transferring technology, but more broadly transferring, sharing, investing data and other intellectual property. And, you know, I look at the last sort of 40 or 50 or 60 years of government activity and I've noticed that we've built up a massive asset and resource, really. And whereas we used to think of natural resources as something maybe the government owned and then leased out, you know, say to the energy industry, now we've created this IP and data and technology kind of national asset. And I think we need to come up with new ways to invest that asset and use it for strategic national security and economic purposes.

And so one of the things I've been working on at NGA is to do that, which is strange for an intelligence agency to think that way. Normally we are consumers of data and information, not providers to industry, but I think that's what we're going to have to do to strategically compete and start looking at it not necessarily just as something we open source you brought up as this sort of a public good. I think there's still definitely a role for that and for open sourcing

things. For example, the corona imagery was open sourced for kind of historical and archival reasons, but I do think there are other aspects where we might want to not open source it, but still provide it and maybe treat it more like proprietary information, you know, unclassified, of course, so we could provide to partners out there, to universities, to companies, to create technology.

And you brought up AI. I think that's the major technology to sort of consider in this aspect where you need historical data to train some of these algorithms. And so, all of a sudden, this asset that we've developed over the last 50 years of historical data is extremely important in that economy. So we have to find ways to share it, you know, strategically with certain companies, not with everyone, and I would suggest primarily with American companies or potentially allied. I started thinking about Five Eyes, for example. And that's what I think we're developing at NGA and the Department of Defense and the intelligence community, and some other agencies are also starting to work on.

So, again, perfect timing on the topic matter and very important to what we're all trying to do.

GENERAL ALLEN: Thank you, Anthony. Let me turn to Rich. From your position at NASA, what are your thoughts on this?

MR. ANTCLIFF: So one thing I want to just mention is that we need to make sure we think about tech transfer in both directions. As an agency that has a mission to do something technologically pretty difficult, it's really important for us to tap into the technological activities that are going on outside of our own development. And so, you know, we have traditionally used tools like SBIR to tap into small companies to get their technologies, to take advantage of

those within the NASA mission. But recently, we were also doing a lot more with prizes and challenges. And with those we actually now can reach into a much broader community outside of just the U.S. and tap into technologists who may be in a garage somewhere across the globe.

This is really important as we look at technologies that now 70 percent of the research is done offshore, right, outside of the U.S. For us not to tap into that is a big mistake. We have got to tap into that and we've got to develop the partnerships in order to get that kind of technology in order to accomplish the kinds of things that we are working on. So I think we need to make sure we have a balanced discussion with regard to tech transfer.

The other side of that with regard to the tech transfer itself, it is something that is in our original mission statement. It's something that we do a lot of. It's something -- you know, we have this spinoff magazine that goes out that people look at all the time for the amount of things that have come out of the space program. So it's kind of part of our culture to do tech transfer.

I think the thing that we're recognizing, however, is that this broad dissemination of the technologies is not as effective as perhaps doing it in a more focused way. So we've recently begun some programs around working with individual companies, with individual organizations, and particularly looking at startup organizations, to try to see how they can take advantage of some of the technologies that have been developed within NASA; not only the technologies, but take advantage of some of the expertise, some of the subject matter experts within NASA, to help their companies actually move forward.

So we find that we can actually leverage then those technologies

a lot quicker and a lot faster and try to help that economic ecosystem be more robust, actually transfers the technologies in a way that is much more effective to help businesses grow, to create jobs, et cetera. So that's something we're experimenting with and we think is going to be something very important as we go into the future. I'll leave it there for now.

GENERAL ALLEN: That's great. Thank you very much. That's a particularly important point about helping the startups to accelerate a process that might have otherwise taken quite a long time.

Nicol, please.

MS. TURNER-LEE: Thank you, John. And I feel so honored, I'm sitting next to two scientists from the federal agencies here.

I'm actually going to talk about tech transfer from the perspective of civil society. And what we're seeing to a certain extent is sort of creating I think some difficulties and challenges with tech transfer because the Internet and the way it's been commercialized has sort of accelerated the private sector's engagement, right, and taxed the government sector when it comes to R&D.

So we all know that the first tech transfer was probably the Internet and GPS systems. And if we look at the way that those systems have been leveraged, as well as U.S. regulatory decisions to make the Internet more commercial, we are seeing these plays, I think, which is a lot different today if we were to look back, where the Internet's growth is sort of outpacing what governments can do. And I think that's what we're sort of referencing, how do you create different types of models and partnerships.

But I want to address this question of then what do we look at

when we see public good technology, and just sort of reflect on that for just a minute. Obviously, this competition has created, I think, a good firewall where companies that have newly been created in this disruptive age are essentially sort of not necessarily doing things for the public good. And so we had that first challenge, right, where we're seeing the marketplace develop products in the commercial market that may not translate back into the public sector, which is something that I work on here at Brookings, or vice versa, we're seeing the government not able to keep pace with what the private sector's actually doing. And I think that's somewhat problematic when we start to look at government funding toward R&D, something that traditionally supported public technology.

I also think that public good technologies require some level of architecture that protests citizens. I think the second panel will talk a little bit more about that in terms of civil society, but there's a challenge, right, if a public good technology that's designed for healthcare, that's designed for transportation, environmental systems, et cetera, military, do not have those protections in place, which I think, John, goes back to your question. It creates a different type of definition of what we should be looking at when we look at public good technology.

I also think, and many of us in this room have been watching the news, when you have private sector companies that are sort of etching into the public domain and suggesting in many respects that they're doing public good, there are problems and challenges associated with that, most recently with a breach that I think all of us are very familiar with, that has now toppled about over 80 million people. With respect to that, I think what we're seeing in terms of

public good technology, where we're seeing private companies like Google, Twitter, Facebook, et cetera, actually doing public purpose things that do not necessarily translate with what federal agencies have in terms of strict scrutiny around design, intent, and the benefits of that product outward.

So I'm always again reminded of having worked and interfaced with federal agencies, you know, things like precision medicine and some of the technologies that we're seeing advance through R&D. You know, the question then becomes when you actually negotiate that or when universities -- I've had the opportunity to go to MIT during their Tech Day where students are essentially putting out patents for new products. You know, it's a little different to have seen the two-screen television and think, okay, that's an interesting patent on that product coming out of a university. But when you start talking about drone technology or interference with national security systems or healthcare precision medicine that sort of finds itself in conflict on the private sector with public sector goals, then I think it's problematic.

So, John, to your question, I do think we need to revisit a public technology definition, particularly in the U.S., as we see the framework in which we started the Internet from this commercial -- our decision to make the Internet commercial has implications on how that actually affects civil society.

GENERAL ALLEN: So your thoughts are then that there has to be some semblance of transference.

MS. TURNER-LEE: Yes, yes.

GENERAL ALLEN: In the context of public good, being of use to the broader civil society.

MS. TURNER-LEE: Exactly, exactly, or the private sector will sort of drive that and we'll have to sort of catch up.

GENERAL ALLEN: Terrific. Anthony, back to you. In the world that you've lived in and currently do at NGA, and thinking about America's use every day of GPS and entities like Google Maps and Uber is currently doing in terms of using big data collection, significantly enhancing these technologies, but as we watch that unfold we don't necessarily always know that it's for the public good. So thinking less about the data itself and more about the technology that collects that data, should there be limits on U.S. companies that are allowed to sell this information abroad or even disseminate it to third or fourth parties in that context?

MR. VINCI: Yeah, I mean, this is a particularly important question when I, again, going back to think about this as a strategic issue and a national security issue for the country. But I would say even in terms of economic competitiveness outside of the national security realm it's important.

Clearly, there should be some limit on technology transfer abroad and I think we're all fairly comfortable with that. And nuclear weapons, for example, come to mind as something that very clearly should be limited in how it goes. So I think there's some things do best when they are fully open sourced and available to everyone. So GPS, for example, I think revolutionized not just one industry, multiple industries globally and definitely helped the United States economy, the government, and everything we do essentially and every day. And you can't necessarily always predict when you're looking at a particular technology what the ramifications are going to be when you do open it up.

So my personal bias, as somebody who actually came from commercial industry, is that there is a bias towards opening up, but, at the same time, putting on my national security hat I realize that there are some competitive advantages that we want to keep within the country to support some of the industries here and then support the national security community. And I think that is creeping from, again, if we have nuclear weapons all the way at the extreme, I think it is creeping left as more and more issues do become particularly important for national security.

And you've brought up algorithms and data and hardware. I think we are creeping towards the algorithm side and where, you know, intellectual property should be protected. But I think the primary issue to think there is that as you kind of creep left and you get from hardware into software into algorithms, the shelf life, the half-life, of these technologies become shorter and shorter. And the shelf life of an algorithm might be months and sometimes even weeks. And so how do you even protect something like that? And is it worth -- is the juice worth the squeeze in even trying to protect it? So we have to kind of factor that in, as well, and, in particular, where much of that happens in the open source and academic realm anyway.

So those are the kinds of points that we have to start kind of considering. And I would suggest what it means is taking a much more sophisticated approach to how we secure and how we think about securing intellectual property and technology in the country and thinking about multiple factors. And then figuring out where in that spectrum of transference we should allow it to exist.

GENERAL ALLEN: Let me make a comment. I'd ask for your thoughts on this.

Obviously, the speed of government is woefully behind the advances in technology across the board, whether it's the production of data or the collection of data or the processing of data, the emergence of algorithms, sophisticated algorithms To your point about public-private partnerships, is there some hope that that concept of public-private partnerships can create a regulatory process that is faster than the speed of government to create the regulations, but demonstrates a level of responsibility in the private sector to do what we ultimately hope, which is doing good and protecting privacy and that sort of thing? Your thoughts would be helpful on that.

MR. VINCI: Yeah, it's an excellent question and something I'm intimately involved with at the agency. We do have a discrepancy and asymmetry between the speed at which technology is developed and commercial companies move, and then the speed at which the government develops technology or, really importantly here, adopts it and integrates it into our operations. And who do we kind of shrink that asymmetry?

I do think there will have to be some new regulatory policies, statutory approaches to this. And, you know, as kind of where I started, I think in our history we have adopted those new approaches when we have determined that we need them. And so In-Q-Tel is an example. We, you know, realized in the late '90s and early 2000s that we needed to be able to communicate with Silicon Valley and early startups better, and that required new authorities. And more recently, changes in how OTAs are able to be used within the Department

of Defense.

So I do think we're going to need some new approaches that kind of take this speed issue -- and I would call it the speed of adoption. It's not really the invention because I think that we're actually reasonably good at R&D and inventing new technologies. And commercial industry is great at inventing it and we're great at buying it. It's how do we adopt it faster? And that's what I'm sort of seeing within the government now. And if you look at things like Project Maven, for example, that's really what they're focused on and I'm involved in Project Maven for that reason.

And so I think that we right now can muddle through, but I think that it's incumbent upon Congress to come up with new approaches that are going to support faster adoption.

GENERAL ALLEN: And I think we're going to find that I believe it's the 12th or the 11th, the testimony on the Hill of the three tech giants, we're going to see some of that worried out into the public domain, where we'll have some excellent commentary on it.

Nicol, would you like to comment?

MS. TURNER-LEE: Yeah, can I add to that, too? I mean, I think you're completely right that we're actually going to -- we do see some of the public-private sector cooperation when it comes to big data analytics, et cetera. But I do think we're in this stage where much of the U.S. regulatory framework has been focused on consumer privacy. Right? And I think the area when we talk about privacy in terms of tech transfer has been more limited to the IP space and I think those conversations do need to happen, right.

But I think what's scarier about this particular area and the rate of technology's pace is the algorithmic piece. I mean, some of the research that I do here at Brookings is on algorithmic bias. And it's clear that what happens in terms of the commercial sector with data scientists there are not many government agencies that have data scientists on staff that understand algorithms and how to unpack that. And there are not many companies that actually want to give away the algorithm, which is why we talk about bias because you can't really see what's under the hood, particularly when it's disproportionately affecting people.

But I was just going to say on that, I mean, I think, John, we've made progress. I mean, in the GDPR, last week was Privacy Week here in D.C. We're going to see data protection, privacy policies sort of come through the pipe. I think the U.S., and I wrote this in the blog, after April 11th, probably April 11th in the afternoon when he leaves the Capitol Hill testimony room, we'll probably see privacy legislation begin to be debated.

But the question becomes with tech transfer what we've seen in the last few months is the manipulation of what is available to sort of innovate new types of practices and procedures. For example, where the algorithm has manipulated democratic institutions, that's a different type of regulation where the data flows are not easily identified and not necessarily understood by all actors and I would even say in some cases the private sector outside of Silicon Valley. I would say companies who are experiencing these breaches every day don't even understand what that means.

So I do believe going forward we will have to look at this

implication that distinguishes between consumer control or consumer access to their own data, business or enterprise access to data, and then the government transfer of data as three different verticals that at some point have to be reconciled to create a much safer and resilient system.

MR. ANTCLIFF: Can I just --

GENERAL ALLEN: Please, Rich.

MR. ANTCLIFF: Let me just add, I guess maybe it's a little bit of balancing, and in the little pre-conversation we had we talked there's a balance issue here between these issues.

You know, there may be ramifications of some of these new technologies, but there's also opportunities of these new technologies. And we've got to be careful not to over-restrict to miss the opportunity. Right? So that's the balance that we've got to find that right place in the middle.

And I think that, you know, as was stated, this idea of public-private partnership is a really good one. And we have done that with the airline industry before to try to move like composites out into the industry. And that serves -- they have the speed that we don't have in order to move those technologies forward. And taking advantage of that speed is very, very important.

You know, NASA's a bureaucracy just like the rest of the government. Us trying to move things forward is difficult. But when we can have these public-private partnerships they bring the speed in. They make it happen a lot quicker and that's very important for us to move it forward and within the opportunity space that's important for the future.

GENERAL ALLEN: Rich, thanks for that contribution. And let me just shift over to you with respect to your NASA background.

We've seen the growing success of companies like SpaceX combined with the resurgence of interest of human travel into outer space and in particular towards Mars. What are your thoughts on the private sector's role in that? And are there risks associated with the technologies obviously being developed in the private sector in the context of technology transfer?

MR. ANTCLIFF: So let me make sure we've got the right perspective on this opportunity, frankly, with regard to organizations like SpaceX, Blue Origin, et cetera. Let's take us back a few years, back to NASA actually was formed out of an organization called NACA, right, the aeronautics committee. That organization was really put in the position to try to help the fledgling aeronautics industry move forward, right. So they had a lot of research, they had a lot of policy discussions about how do we have a -- how do we open up the airspace to these crazy companies that are flying airplanes around? And oh, my gosh, don't we have to have some kind of restrictions on those, et cetera? So that has been a job that NASA in its history has been a part of for all of its lifetime, really, is trying to help industry grow such that it can commercialize and become something very valuable for our country and, frankly, for the world.

And so we're in a new era of that now with regard to the space economy, where we're seeing organizations like SpaceX, like Blue Origin, et cetera, et cetera, right, who are taking some of the technological developments that NASA has done over the years, they're taking them on and they're figuring out how to do them cheaply. Right? Again, this is not something NASA is good

at. We're good at the technological stuff. We're not good at figuring out how to do it cheaply. The SpaceX's and those can figure it out how to do it cheaply such that we can then have a commercial market that's valuable.

So this is very positive from our point. We think this is the way it should go and we are very much working to support those industries. They're using a lot of our facilities and capabilities, subject matter experts. You know, we are actually trying to become a customer of theirs to try to get, obviously, provisions up to the Space Station and eventually humans into space.

So we see that as a very positive benefit. It is the public-private partnership that we've been talking about and in kind of a big, mega economic way.

GENERAL ALLEN: Sure, please.

MR. VINCI: If I can come back, actually. And you bring up a great point, which is relative advantage and relative competitive advantage, and what is private industry good at and what is the government good at. And that really gets to the heart of why you would even have public-private partnerships.

When I look at the government, and particular I look at agencies like NASA or NGA or the Department of Defense, it's very good at doing certain sort of more or less impossible tasks; I mean, putting people on the moon. I think of the Corona program, putting satellites up in the air, literally dropping film canisters over an ocean, sending an airplane to pick it up in midair, and then getting it back to the U.S. to be processed and analyzed. That's a nearly impossible feat and it's incredible that they did it with the technology they had.

Whereas when you start to look at private industry, it's very good

at something very, very different. Being inexpensive is a big part of it, but also being creative in a way that the government isn't. An example I like to use is Waze. And I feel like the government approach, for example, to global traffic monitoring, if we had come up with it 10 or 15 years ago, would have been to go out and buy helicopters because we looked at how do you monitor traffic? Well, the local news stations, they use helicopters and they film the traffic and they radio it down, so we should just buy a lot of helicopters and be doing ellipses around every city in the nation and sort of radio it down and let's go global with that. Whereas Waze, with almost no money and without even that in mind, created a community of people to kind of -- well, for mapping purposes actually to start, but then for monitoring traffic and sharing that. And they use cellphones and they use GPS, and now they give it away for free.

And so that is just a very, very different approach to problem-solving that lends itself to solving very, very different problems. And so when we start to think about these public-private partnerships, we should look at it from that lens of, you know, what is the relative competitive advantage of each side and where should they play?

And I think even within that example we see an example of that is GPS. Right? Waze couldn't have been possible without GPS. And GPS would not have been possible from a commercial perspective. It's a money loser, I suspect, and it's really big and expensive and complicated and just difficult to do. And it has to last forever, for decades and decades, which not all companies do. So there's a clear role for government, but then there's a clear role with something like Waze for creative new uses for it.

So, again, it's that relative advantage and it's a new way to think about how government partners with private industry.

MS. TURNER-LEE: And, John, just so I don't sound like Debbie Downer, I do agree with the panelists that there are positive ways to actually deploy technology. And I do agree with you, I mean, SpaceX, for example, is now being looked at to provide broadband services to rural communities. So there's this repurposing of technology that's going on every day.

I just think with the panelists it's a responsible not necessarily standards-driven, but some type of input-output where the commercial and the public sector partnership is defined by what that output is. So that it doesn't become something where you do have geolocation and then later the government is kicking themselves because the geolocation had some unintended impact or consequence that was not thought of by the commercial sector.

So I wanted to make sure, John, everybody knows that I do support it.

MR. VINCI: It's a balance issue.

MS. TURNER-LEE: It is a balance. It is a balance.

GENERAL ALLEN: It is. And I think that the common thread, and I'll go to the audience here in just a moment, the common thread is that the public-private partnership is really the way ahead here. It is something that can reinforce the public good. It can probably minimize the deleterious or negative effects. You know, Waze has the capacity, as Anthony says, of producing enormous amounts of useful data with respect to metropolitan planning, infrastructure planning, and that sort of thing. But it also will tell members of my

family if I stopped off at the Dubliner on the way home and I worry slightly about that. (Laughter)

And with respect to commercial involvement in the space program, I absolutely agree with Rich. This has been an accelerant. It's also very cost-effective. It's a quick integrator of technologies. The one Tesla I had my eye on is on its way to Mars now, so I'm out of the business for a while. (Laughter)

MS. TURNER-LEE: That's all right.

GENERAL ALLEN: But I think this is a real opportunity for us in terms of technology transfer both in the context of national security, but even more so internally towards the good of civil society and the transference to civil society that is the real opportunity. And, Rich, you've touched that a number of times in terms of opportunities.

So let me go to the audience now. We have a rich array of attendees this morning from a number of different organizations and from many different countries. And so we welcome you here today. We'll go for about a half-hour. I'm busted another five minutes and I will end straight on the hour at 11:00, so I apologize for taking up five minutes of your time.

When you stand if you could give us your name, please, where you are from, and if you could get to a question relatively quickly I would be most grateful. If not, I'll find a question in what you're saying.

So, please, yes, sir, right third row back and we'll come to the second row after that.

MR. HURWITZ: Gentlemen, thank you for a very good

presentation. My name's Elliott Hurwitz. I'm from Rockville, Maryland. I used to work for the World Bank and the intelligence community. Could people please define the public-private partnership a little bit more clearly?

GENERAL ALLEN: Why don't we start with you?

MR. VINCI: Yeah. It's a loose term and it's used in a lot of different ways historically, everything from building toll highways together to NIH investments in healthcare and so forth. But the way I would use it is to see it as what are mutually beneficial things that the government, the public side, and the private side -- primarily commercial industry, but I would also include universities, nonprofits, civil society within that -- what are mutually beneficial things that they can do with specific projects? And those benefits might be very different from one side and the other or they might be the same.

So the example that I would use is the co-creation of technology, what I was saying before, the government's good at creating certain technologies, the commercial sector's good at creating different kinds of technologies. How can they work together in a mutually beneficial way to come up with technologies that they both want? And so, therefore, chipping in different things at different times.

And I see it as a partnership in the sense that it's not a one-way street. So it's separate from contracting, for example, where the government provides money and, in return, gets a service or a product. So that's really more of a one-way street.

This is a partnership in the sense that both sides need to chip something in, whether that's money or time or effort or capability. And both sides

should receive something in return, again, whether that's technology or data or some competitive advantage.

GENERAL ALLEN: Anyone else?

MR. ANTCLIFF: I just wanted to add I absolutely agree, a lot of our public-private partnerships are in that vein where we both contribute something to the mix. I think the other kind is, what we do a lot, is precompetitive work where we'll have several companies that'll come together that we will partner with as a team to work on the maturation of technologies to a certain level that's precompetitive. And then those companies can take it off and actually do something with it competitively. So I think both of those are models that we are used.

MS. TURNER-LEE: And I would say with public-private partnerships, an area that I do a lot with in the telecom space, you have to have common goals, right, between the private sector and the public sector and what you want to accomplish and a fundamental interest in public interest, honestly. A public-private partnership is really not a public-private partnership if the public interest or civil society is sort of not at the core of what that partnership looks like.

And I would agree with Rich in the sense that the public-private partnership has to be done in a way where it does not stifle innovation. And so we've seen different arrangements where you kind of go into the public sector-private sector partnership and then there's concerns on whether or not you can have the ideation process happen, innovation can happen, because of the constraints of either the public sector or the private sector's unwillingness to invest the resources, et cetera.

I was just going to say a good example in terms of public interest are electronic health records. Over the years we've seen electronic health records become much more resilient because the public interest, sort of guided by HIPAA and other sort of regulatory prescribed rules, have helped the private sector innovate in a way that that's more readily available.

And I would just end by saying it's the scalability of that partnership that has to generate the output. And we often deal with that in my particular work where we're asked to see, well, is this a benefit to civil society? If it's only benefiting one part or a block and it's not really scaling and you're taking all this R&D money for a competitive advantage, it really hasn't met the criteria.

GENERAL ALLEN: Thank you for that question, Mr. Hurwitz. There was a question in the second row, please. And I'll come to you in a moment. The left side of the room seems extraordinarily inquisitive this morning. (Laughter) We invite anyone to take questions from the right side of the room -- or offer questions. Please.

MS. FAZEL: Thank you very much. I'm Marina Fazel, an Afghan-American journalist. And this is really exciting to be at the dawn of the digital era and watch all the differences that it will bring for our societies.

Could you please put into context how this relates to future of government? Up until this point, really, the societies worked on a global system of opening economies and coordinating the economies and governments. Right now we're in the midst of such populist movements and with technology being at its earlier stages, although we're seeing some of its fruit, we're still also seeing it being used, and you've just all described processes where it's going to take time

to introduce regulations and perfect techniques to ensure that they still serve the public good and government can have its jobs.

Could you please put in context? This is going to take a long time and yet we are on the brink of what looks like maybe a new Cold War with so many conflicts brewing, both in the private sector and global. Thank you.

GENERAL ALLEN: Who would like to take a crack at that?

MS. TURNER-LEE: So I think your question is spot-on. I mean, I kind of describe this as the myopic tendencies of creators who want to see a product go to market quickly, a lot of the tensions that we've discussed, and the broader goals of what that technology's impact is on society.

And you're correct that we're so much more global. I would actually argue that tech transfer become much more protected by people in terms of what they want to share. Because the vulnerabilities that it sort of created by having the technology be so much more widespread is not generating the outcomes that we all thought it would generate. It's different from a government or a smart city, you know, leveraging technology and practices to be more efficient, et cetera, to actually cutting into your democratic institutions.

I really do think we'll go into an age where those regulations actually happen before the innovation catches up, which will be a flip-flop model of what we've actually seen where the innovation has outpaced government. I actually think government's going to come in and sort of put a plug in some of this stuff before the innovation comes out, which might also create its own set of problems.

But I think generally your question is correct, that we have to

figure out ways to harmonize these systems so that since we are moving into more of a digital economy, the Bureau of Labor Statistics just put out a report about the percentage of the GDP that is now driven by digital. You know, this is certainly something that has taken up a huge proportion of our attention not only in terms of the innovative side, but economically. So this is going to be a problem. It's a good problem to have, but it also has consequences.

GENERAL ALLEN: Let me also add a couple points. In terms of Afghanistan, there is enormous capacity for the community of nations using the digital environment to accelerate civil society, economic productivity, and even improve governance in many ways, apart completely from the security side of it. And here's where I think the community of entities, which is bigger than the community of nations -- when we talk about "entities," I'm talking about Facebook and Google, some of the most significant sovereign entities when you think about sovereignty -- have the capacity to help to slingshot many countries that are in the developing world that would not otherwise be able to do it on their own, through public-private international partnerships have the capacity to be quite helpful, I think, in that regard.

Also, you mentioned the potentially emerging Cold War. Quite apart from the dust-up we're having right now with the Chinese, I think that there are enormous opportunities, again, for us to share and to cooperate, the U.S. and China, on a number of issues. The Cold War, you might have mentioned this with respect to Russia and I have great concerns about where all of that is heading, frankly. But I see China in a very different mode.

And I think beyond the reflex for protectionism, which can chill

this, it can chill the opportunity to cooperate in these very important areas, the capacity for the United States, and China in this regard to find common ground in the digital future I think is extraordinarily important to both countries and to the community. And I would hope that we don't confuse the activities right now that appear to be protectionist that could lead us down the road towards a trade war, as being helpful over the long term towards a U.S.-China relationship.

MR. VINCI: If I can add in there, I completely agree with your point and the point that's come up here on the value for developing countries. And I'm a technology optimist. I used to work for Alvin Toffler, who wrote quite a bit about this subject and talked about how you can skip a generation of technology and this can have a profound effect on countries. So if you skip from landlines to cellphones, for example, much more resilient, much less expensive technology. I've done a lot of -- my Ph.D. fieldwork was actually in Africa and I watched this happen in real time what mobile phones did to an entire continent. And that really is the promise of the use of technology.

And I think we all know there are downsides, obviously. There's also a negative consequence for lots of technologies. But the net gain to me is massive.

And I think when we talk about the public-private partnerships there's an unsaid assumption which is really important, which I see in my government role more and more, which is an acceptance by government at the working level that commercial industry, commercial technology has a lot to contribute to governance and government in general, and that we should adopt it. This is a very real factor within government, the not-invented-here mentality,

within any large organization. And I think we're starting to get over that and realize that there are a lot of these technologies that we can use that allow us to govern and to enact our government duties and responsibilities significantly better, cheaper, with a wider scale.

And what came up before, for example, broadband, whereas government again, and the Waze example, maybe we don't buy helicopters, but maybe we do dig a hole in the ground for every house in the country no matter how far off. And I think that is valid and everyone in the nation should have broadband. But all of a sudden, maybe there's this game-changing technology if we can do broadband from space because a company like SpaceX and even some other ones than that have come up with a new, much cheaper solution. And that's really the promise here and we need to be open-minded as a government and government employees in thinking about that.

GENERAL ALLEN: We're not cycling very quickly through these questions. The gentleman I think just next to the camera, please. Yes, sir.

MR. PESTRONK: Bobby Pestronk from Pestronk Glass. I would be interested in your thoughts about the wealth that has been created through digital technology. That wealth is unequally distributed currently and the digital industry is becoming increasingly sophisticated at the creation of rules, as other industries have in the past once wealth has been created. Do you think we have the right balance in the public-private partnership with the financial wealth that's returned to government for public purposes that public governance can make decisions about?

MS. TURNER-LEE: No. (Laughter) Just leave it at that.

No, I completely agree with you. I mean, if we go historically and we look at the evolution of technology in general and something that I always have to remind myself, you know, we really started with IT and very basic principles of what "tech" meant, even with government, right, going back. That's morphed into an economy that has not just been a static economy. You know, the Internet is no longer this composite of websites that people go to. It's actually layers that create in and of itself its own wealth. So the sharing economy outside of the digital economy, which is sort of ruled by the Internet of Things and other types of really cool technology that you can touch, Cloud computing, each of those layers actually generate its own sense of output, economic output that does create this unequal distribution of wealth and access.

All of us in this room if we don't own a patent or a technology company, what we all should be -- I don't know if we should be proud to say this, but we're all passive consumers in this digital economy right now. Startups and other incubators, you know, government is really trying to break through, and this is a case where I think government is behind on that, too. VCs that were government-driven or VCs that were supporting public technology applications are now just coming around to see that, hey, we've got to fulfill this role.

I tell people all the time Facebook wasn't designed for what it's being used for today. It was designed just to be a social network and now it's in the middle of a conversation around algorithms. I mean, it was an ad-supported model that has morphed into something else.

Uber found a spot in there and it's creating its own generation of wealth, own generation of workers, which is why we're sort of wrapped into this

conversation which is so much more sophisticated.

Who are the people on the end that will become the fatalities of this digital economy? It is the 11 percent of Americans that are not online. They're poor, they're disproportionately people of color, they're disabled, they're in rural communities. They will always be involved because their big data is what drives the new economy, even if they're not online. Their lack and absence of data actually drives companies to know where they need to deliver food or what kind of investments they need to make in smart grid systems. They're still part of it, but they run the risk of becoming deeper and deeper in poverty and eventually becoming digitally invisible.

And so to your point, I think the way -- the BLS report I think was the latest case to sort of debunk and unpack what the digital economy looks like. But I think your question is really critical, particularly when government invests resources in R&D and they don't get a return back on investment or that technology which was designed to solve the social problem actually creates the problem. And that's where I think, again, a lot of us are sort of stuck in the middle, and I know the next panel will talk about security.

You know, how do you begin to resolve and reconcile and create harmonious legislation or regulation that allows one part of the technology sector, again, to focus on civil society while another part of it continues to do what they do, but perhaps in a regulated context? Because again, the Communications Act of 1934 was designed for the telegraph, later picked up ISPs and broadband. It didn't anticipate the companies that we see today.

So I think your question is spot-on that the wealth equity index will

continue to widen based on where you are within the topology of the digital economy.

GENERAL ALLEN: That's a great question, Mr. Pestronk. Let me just offer a couple of thoughts.

Sovereignty throughout much of modern history has been shaped by the concept of Westphalian sovereignty, which is a line on the ground that circumscribes terrain and some number of people, often with a homogenous identification, all who provide their loyalty ultimately to the sovereign. That's a relatively modern view of the concept, the Westphalian concept of sovereignty. Sovereignty really is about the capacity of a sovereign to influence. That's the traditional sense all the way back to Aristotle.

I think we need to think differently. And I believe that the public-private partnership concept may be some of the nascent thinking about how in a world where tech giants, digital giants control the modern version of the power of ancient sovereigns, which is wealth and data and algorithms, in ways that traditional Westphalian governments don't necessarily control them, I think we need to think a bit differently now about public-private partnerships ultimately morphing into what might be public-private alliances.

Because when you think about some of the large tech giants with GDPs, if you will, that surpass many of the countries on the planet, that can reach out and touch people in the numbers of billions and influence their thinking for voting purposes, et cetera, that's a whole different way of thinking about influence and sovereignty in the modern digital era. Because where it was in the past about terrain and numbers of population, today it's much more about the

information that you control, the way you will wield that information in terms of algorithms, and the outcomes that will flow from that, which will be prosperity and wealth.

It's a different way of thinking and I think we need to begin to expand our view about -- I used the term a moment ago, the "community of entities." We often talk about the community of nations. It's much bigger now than the community of nations. If the community of entities join forces in a public-private partnership or an international-private partnership, we have real capacity. And I'm not sure that we're thinking about it properly. I'll leave it at that.

MR. VINCI: Do you mind if I kind of build upon that?

GENERAL ALLEN: Sure, please.

MR. VINCI: Because I think what you've done is place this concept of public-private partnerships within the wider spectrum of how we understand geopolitics and how we understand history. And I think we can go further with that thinking in terms of how different nations have different government systems. And that difference will apply to how they use public-private partnerships and the nature of those relationships.

So I think that China will have a very -- it already does have a very, very different approach to public-private partnerships, say, when the Chinese government deals with a company like Baidu than we do and how our government and the U.S. Government deals with a company like Google. And I think both of those types of relationships are going to shift over time and I think that's what we're starting to see now and what we're kind of talking about here.

But what makes it even more complicated is these companies, as has been brought up here, aren't necessarily just within a single governance system. And so Google may have a very different relationship with the EU than it may have with the U.S. than it may have with China. And it makes it very complicated to think about how all these relationships are going to interact and evolve over time. And that's going to be the sophistication for us on the government side is what do we actually want from the public-private partnerships and partnerships with these other entities? And then how will we get it? And that's what we're all starting to think about right now.

GENERAL ALLEN: Well, this is an important outcome for this panel. I think very importantly my digital network-capable device tells me that we have four minutes left in this panel. I've been very disappointed in the right side of the room to this point. (Laughter) Is there anyone -- yes, sir, please. We have just a couple of minutes. I'd like to get quickly to a question and we'll get quickly to an answer. This gentleman in the third row.

MR. JING: Thank you so much. I'm Fu Jing from China Daily. I have two questions.

The first one is in terms of the cooperation between China and the U.S., could you elaborate more areas, specifically where U.S. can improve their cooperation to improve the simple wellbeing of all countries?

And the second one is you just talked about the areas where the government on the one hand needs to set the regulations of the different industries. But in the meantime, it needs to provide sufficient funds for different industries to develop. How does the government strike a balance in terms of the

U.S. side? Thank you.

GENERAL ALLEN: That's a very long question -- a very short question, a very long answer. There comes to mind immediately where the U.S. and China in the context of the digital environment can cooperate would be in medical diagnoses, the capacity to harvest enormous amounts of information on medical research, and using the right kinds of algorithms help us to get more quickly to diagnoses now that we're beginning to see can be harvested and rendered with high levels of confidence relatively quickly.

And the other is in the area of security, of course, and the whole business of countering terror. There are lots of reasons why China and the United States need to cooperate in this regard. And there's real capacity in that regard, as well.

And I would simply say that we haven't seen it play out yet, but we're all very interested in seeing how President Xi's objectives with respect to the outcomes of the 19th Party Congress and China's intent ultimately to surpass the United States by 2030 in terms of emerging technologies, how that will ultimately play out. China has, in some cases, advantages; some people would say disadvantages in that it has at its core the capacity to create great cohesion between the objectives of the government and the objectives of Chinese companies. There is much more capacity there than perhaps in our system. And I don't call that a strength or a weakness, it's just different and we need to acknowledge that that will be different for us.

Anyone else?

MS. TURNER-LEE: I just, also, in the same area of AI, I mean,

clearly the artificial intelligence side of what we're seeing the Chinese do I think is really interesting and sort of outpacing some of the things that we have here in the U.S. But when it comes to global decision-making or problem-solving, I think some of the applications there should warrant some cooperation because -- particularly when the U.S. takes on big issues like a couple years ago, when the White House was trying to solve the Ebola crisis, for example. Some of the new applications and emerging technologies could have actually been more helpful if there was more cooperation.

And we're starting to see the U.N. do more of that kind of cooperation as an international entity when it comes to human rights and digital civil rights. I think they should actually be moving into this conversation around that.

But I was going to also say to your second question around who funds that, I think the interesting conversation that we've had at this table that's even enlightened me is how do you incentivize? So you regulate, but you also incentivize this type of digital development. And hopefully, we'll begin to see more models like that. Where are there cases where we can incentivize governments to have more cooperation around products and services that fit sort of the core verticals of the public interest, which I think will help with the allocation of funds? Because, unfortunately, I don't think any government has enough money to support the local GDP of a company that's surpassed the GDP of a small country. And so I think having more of that.

I also understand, like, for example, in Africa, with mobile there's some lessons that were there that we didn't pick up on in terms of the wireless boost that you were talking about. So, again, you've got to incentivize those

types of experimentation or projects to sort of balance the regulatory framework.

GENERAL ALLEN: Nicol, Rich, and Anthony, I want to thank you very much for participating. Ladies and gentlemen, thank you for joining us this morning at Brookings. And would you help me to thank the panelists.

(Applause)

(Recess)

MR. WEST: Okay I will introduce our topic as well as the panelists. I'm Darrell West, Vice President of Governance Studies here at Brookings and also the Director of our center for Technology Innovation. So we are going to continue the discussion started by John and his panelists on technology transfer. I do have to say, the first panel set a very high bar in terms of both substance as well as humor. I'm not sure we're going to be competitive, at least, on the latter part of that. They also were able to work in references to Aristotle and Wes Faille and Systems. We may or may not meet that threshold as well. But we will try to get into some equally important issues. I do want to remind the audience, both our C-SPAN audience as well as the people in our auditorium. We have set up a Twitter hashtag. That is #TechTransfer. So if you wish to make any comments or pose any questions, feel free to do that. That's #TechTransfer.

So our panel is going to focus on the security angle regarding technology transfer. We'll be getting into questions such as, when should technology be transferred and when do sensitive products need to be protected and where should we draw the line between national security issues versus free trade and the free exchange of information. To help us understand these issues,

we are joined by a set of distinguished experts.

To my immediate right is Heather Roff. She works on the ethical aspects of artificial intelligence. She has published several articles on autonomous weapons and also is the author of a book entitled, “Global Justice, Kant, and the Responsibility to Protect.” So if they had Aristotle, we have Kant here. Mike O'Hanlon is a senior fellow of foreign policy at Brookings where he holds the Sydney Stein, Jr. chair. He is the author of numerous books and works on U.S. defense strategy and American national security policy. He also serves as director of research in the Foreign Policy program. Paul Triolo is the head of Geo-technology at the Eurasia Group. He works on global technology policy, cyber security, and emerging areas such as AI and big data. Prior to joining that firm, he served in several senior policy positions within the U.S. Government over more than 25 years. Chris Meserole is a fellow in the Center for Middle East Policy at Brookings. He's an expert on religious and sectarian conflict and the impact of technology on foreign policy. He also is using machine learning to study violent extremism.

So why don't I start with Heather. You have argued that many emerging technologies are what you call, dual use in nature, meaning they can be used both for good or bad purposes. How should we think about technology transfer and expert control with dual use technologies?

MS. ROFF: Thank you, Darrell. Thank you for having me here today. So I think to answer your question there are two ways to think about this. One is to talk about Kant, one is to talk about Hobbs. We're going to throw down. We're going to double down on some philosophers. The primary purpose of the

state, job one of the state from a security purposes to secures the rights and lives and protections of its citizens. This is very Hobbesian. The leviathan's whole job is to actually protect the body politic.

So when we want to start talking about dual use technologies and the regulation of dual use technology, what we're really talking about is the regulation between civil society, civil applications of a technology that is for peaceful purposes, something in the economy and something that is used for military purposes. The flip side of that is that same technology could be militarized in a way and used for security purposes or for weaponization. So we have to be very careful about how we draw lines around these technologies. One way to think about this is through a series of arrangements that we already have in place. We have international treaties in place like the missile control regime, so the MCTR.

We also have things like the Vashon Arrangement which is a voluntary arrangement of likeminded states that want to ensure that the technology developed and exported. When a dual use technology actually starts to become so precise in what it can do, it becomes more conducive to military applications. So thinking about things like hardened systems against electronic magnetic pulse, so those systems that can withstand a nuclear attack or those systems that might be able to withstand extreme temperatures. When those things start to happen, those begin to become what we would consider dual use in need of expert control.

So the good and the bad purpose is one way to think about the hook but the other side to think about this is military versus civil. And then it depends on which side you think is good or bad. What I would say about tech

transfer and expert control is that the new emerging technologies are not very amenable to the current structures that we have for expert control and dual use. So if you look at something like the Vashon arrangement, for example, you have within about a 198 pages, all sorts of discussions about what needs to be regulated, at what rate, when it is here and if it is this type of technology. If it's nuclear, if it's a software, if it's an enabler, if it's a sensor, if it's a frequency hopper, all sorts of different types of technologies that are enumerated throughout that 198 page document.

Within three lines of that document, I found something very anomalous and I think is very interesting. That is, voice encoding. So if you can voice encode, so you can take continuous speech and then you can make it into zeros and ones and then you can encode it into a digital frame and then you can compress it and then you can compress it and transfer it at a very slow rate, 700 kbs. That's a very slow transmission rate. For some reason, Vashon finds this a dual use good that needs to be regulated for export control. I don't know when they decided this was the case and I don't know exactly why. But what I do know is that about six months ago, an academic decided that he figured out how to do voice encoding at 700 kbs. And he dropped an open source on the internet. That kind of move really pushes us to think about how we do our regulations and how we can have more foresight about our regulations when it comes to military applications for security purposes.

Another thing that I would just really briefly draw attention to is not only do we need new governance structures and new ways of thinking about these types of security and military technologies. Or technologies that hey, I want

to regulate this algorithm, by the way, that's the same algorithm that's on your phone running Siri. Then you're going to stifle innovation and you're going to stifle the ability of other states, particularly developing countries, to gain that technology to boost up their civil society's well-being as well as their economies. You have to be very careful about where you draw those lines.

But there is another question that is equally at play. You have, where do we draw the lines, how do we do new normative governance and forward thinking on really hard questions about these dual use goods. But another one comes when these public private partnerships happen in the security realm. I think one of the things that we can look at now, it has been in the news quite recently, is the potential for a cloud computing contract for a single company to take all of the DOD's data and host it on the cloud for the next ten years. A single company contract, ten year span. That's a lot of money. And right now in the news, what we've been seeing is Amazon is up for that contract. We don't really know if they're going to get it but there has been lots of discussion about Amazon cloud and Amazon's web services hosting that.

And then we have questions about that public private partnership and what that does from the civilian side of things and the security side of things when a public global company like Amazon starts making bets that it is going to host a state's military data. And what that does to where Amazon operates in other countries that they say, maybe I don't want Amazon to have my data if they're going to be feeding it to the U.S. government or those types of things. How are we going to partition that, how are we going to keep that export, how are we going to keep that dual use goods, how are we going to make sure that the

public private partnership is for the good of everybody, particularly if those states or those entities are global in nature. So I think we have some really hard questions when we start thinking about technology, civil, military and the securitization of all of this when they're running together in really difficult and complicated ways. Thank you.

MR. WEST: Thank you, Heather. So Mike, you work on great power competition, particularly with regard to Russia and China. What are your thoughts on when sensitive products need to be protected?

MR. O'HANLON: Thanks Darrell, and good morning everyone. I certainly won't try to rival John Allen, our boss, on humor or anything else. I maybe will try to rival him on saying something surprising from a Brookings podium which is, I think, much of what President Trump is trying to do towards China right now is actually justifiable. Not necessarily in every detail but the general thrust of pushing back on China in particular. Let me try to have a historical perspective on this as well, not quite as far back as Aristotle necessarily.

If we think about the last 500 years and Paul Kennedy, the Yale historian, wrote about this. We've seen European powers, in particular, rise, and then fall fairly fast, partly because they couldn't protect their advantages. Because they were living in an economy that didn't have barriers to technology transfer or theft of intellectual property which is an age old phenomenon that we've seen long before the internet. Just in the last 100 to 150 years, Britain lost its advantage in industry and advanced technology to Japan, Germany and the United States, among others, but those three in particular. Luckily, one of the

three was us and we ultimately therefore were in a position to help bail out the west of the western world in World War I and World War II which resulted partly because of this technology transfer happening pretty fast and Germany, in particular, catching up faster than it might have otherwise.

So I put all this in perspective because, of course, our more recent historical reference point is the Cold War. We had very little economic interaction with the Soviet Union during the Cold War and we were very comfortable putting up a lot of the barriers, some of which Heather just talked about, some of which were done for non-proliferation purposes to prevent nuclear weapons from getting to other countries. But many of which were designed to keep high technology conventional weaponry out of Soviet and Warsaw packed hands. Now we're living in a world in which I think our most likely competitor over the medium to long term is China which is, of course, so fully integrated into the world economy. And we made a gamble, not just in economics but in strategic terms, 10 to 20 to 30 years ago. We decided to try to bring China into the western economic world as fast as we could, including membership in the World Trade Organization. And the gamble was on both economic and security fronts, this would help China liberalize fast enough that the risks of seeing China grow fast would be outweighed by the liberalization of China and that it would become a more rules oriented participant in the national order.

This sounds like China bashing, I'm really not a China basher. Jim Steinburg and I wrote a book a few years ago about a strategic vision for how we could try to get along better with China and do some things even on the U.S. side that would promote that process and recognizing China's impressive

historical rise. But in some ways, it has become a little too fast for comfort and especially because of the means that China has been using.

Darrell, you and I talked about the idea for this panel and I want to thank you for the whole concept of this event. But we talked about this originally a few months ago when we met with Brown and Padme Singh who were from the DIUX unit in Silicon Valley. They wrote a paper, which is very compelling, called China's Technology Transfer Strategy. How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of American Technology. They went so far as to actually suggest we rethink how many visas we give to Chinese students studying in the United States. They had some pretty drastic ideas in their paper. I'm not sure I support all of them but their analysis is pretty compelling. It is recommended reading for all of you.

I'm going to begin to wrap up here by saying that at least some of the ideas that have been put forth to try to force China to comply with the rules based order for technology transfer, I think, are actually appropriate. Specifically, trying to make sure that until China will allow equal access to their economy and their country for western firms, we should slow down their ability to acquire and access American high tech giants and jewels. That's not enough of a strategy but it is certainly a viable beginning and that's why I support much of what President Trump is doing.

What I'll finally say is, I'm just going to tick off, I know I'm throwing out a lot as a fire hose methodology here for presentation. But I want to just tick off a few of the technologies beyond the AI, big data and cyber worlds where, I think, my co-panelists are stronger than I am. Where we have to really keep our

eye on trends. Because these are going to be the areas where much of the other parts of key military competition occur over the next one to three decades. And first of all, anything having to do with nuclear proliferation remains important, not so much for China but for other countries. So advanced metals, advanced machinery, precision machinery, advanced timing devices, the sorts of things that are needed to make centrifuges to make bombs themselves, we have to keep a very close eye on these things and not lose sight of that as we try to hasten technology transfer in other domains for good and positive reasons.

And then within the areas that I do think are important regarding China in particular, we have to keep our eye on a few things such as submarine quieting technology, which has been a traditional American strength that we've got to try to keep. Stealth technology for aircraft, same thing. Many aerodynamic and aerospace capabilities and advanced engines in hypersonics where in China, in some ways, is getting ahead of us but where we, I think, have other advantages that we can reinforce and preserve. Directed energy including lasers. And then finally Nano materials, microscopic materials which are very important for everything from batteries to the strength of various composite, structural materials that we build systems out of.

These are among the areas where I want to just interject a note of caution in a conversation that very appropriately is thinking about how do we share more, how do we, especially in terms of the first panel, how do we promote economic growth through technology transfer between government and private sector. I also want to remind of some of the areas where we have to be particularly cautious, in my judgement. Thanks.

MR. WEST: Okay, thank you Mike. So I think we have the headline on the event now. Mike O'Hanlon endorses Donald Trump on some topics, not necessarily on every topic. Paul, I want to come to you. So Mike mentioned the China connection and one issue there involves the so-called force tech transfer where companies claim they have to share their core intellectual property. So I know you work with many companies. Could you provide a perspective from the commercial world on how companies view the intellectual property issue?

MR. TRIOLO: Thank you. This is a huge question and I think the other panelists have outlined a lot of the themes that I'd like to touch on briefly. I think I agree with Michael in general on the thrust of some of the actions that have been taken recently. I think it is really important to understand, for example, that the 301 action which we're in the middle of now, is really not about trade as much as it is about tech transfer. So I recommend reading the USTR report. It is 215 pages but I think the section on tech transfer is very important. Tech transfer is mentioned 227 times in that report.

So really, I think we're in the midst of a reassessment in the U.S. of how we do both export controls and how we handle things like technology transfer. Because China has, for a variety of reasons, has become the poster boy of industrial policy, overreach in the view of many including the U.S. government. And terms like mercantilism are used and again, force tech transfer then has become a key issue that is really driving, in part, this so-called trade action.

So there are two important parts to that. One is this issue of, how

do you deal with a country that has a very elaborate set of measures that are designed to compel, in some cases, legally involved tech transfer. There are a whole host of other gray areas, things that are unwritten rules or unwritten documents and cajoling of companies to do tech transfer. Also things like cyber espionage which has been a longstanding issue in terms of gaining access to technology. In part, the process that we have embarked in now is an effort to really try to roll back some of China's policies. It is a very complex edifice that the 301 report calls essentially China's technology transfer regime. I think it is going to be a very difficult thing to do because some of these issues are structural. Industrial policies like, made in China 2025, things like the National Integrated Circuit Fund which is a huge fund which was once described by a U.S. government official as an effort to appropriate the global supply chain for semi-conductors.

So there is a whole host of very critical structural issues. What happens is, U.S. companies are in the middle of this issue because U.S. companies are trying to do business in China, trying to negotiate a very difficult regulatory environment to do business there. So a lot of our clients, for example, are multinational companies that are involved in China and want to include China in their global operations but have to be very careful how they operate in China. I think the companies we work with by enlarge, view the situation that they can control the amount of tech transfer that happens and their operations in China and can protect the secret sauce, if you will, of a company. As you read in the USTR report, you realize how complicated that issue is because each company is going to have a different kind of problem to deal with, a different kind of

pressure to do tech transfer. So it becomes very difficult for companies to figure out how to navigate in that market.

So in part, there is sort of mixed feelings about this whole action that the 301 investigation has started. Because some companies have been very successful in navigating that and protecting their core intellectual property and others, of course, have not. So the business community is very split on this, I think.

The other piece of this process that will be really important is the investment restrictions. So there is a major effort in the U.S., of course, to revamp the CFIUS legislation, this is the Committee for Foreign Investment in the U.S. and that is a process that's happening now. And another piece of this whole action against China will be some sort of a proposal of an investment reciprocity regime which potentially has much bigger implications even than the tariff piece. Because this would restrict Chinese investment in key sectors in the U.S., for example, cloud services, which has become a huge issue in terms of this idea of reciprocity. Alibaba and Tencent built data centers in the U.S., for example, but Oracle and Microsoft and Google and Amazon all have to have a joint venture partner. That usually involves some level of tech transfer as part of that deal, for example.

So we're embarking on a really difficult period, I think, in U.S. China relations which encapsulates all of these issues. At Eurasia Group, one of our top risks this year, the third top risk was global tech cold war. I think the U.S. tech cold war is a big piece of that. Again, as we look forward to things like fifth generation mobile, China is going to be a big player in that. Countries in

developing markets are going to be looking for the technology leaders, for example, for 5G and the U.S. is looking at how, for example, build a whole 5G network, what we call China minimized or China free which is a whole other topic we can talk about.

With advanced technologies like 5G and particularly AI which can also talk about, there is a lot of sense that we're moving into a world where there is going to be more competition in these areas than collaboration. I am also a technology optimist but I'm a little worried that rhetoric, for example, in the media has tended to focus on the competition and not so much on the collaboration. For example, in AI there is a tremendous amount of collaboration right now between China and the U.S. That also could be jeopardized by some of these actions coming up.

In any case, I think, the bottom line is the regulatory system is sort of behind on this. The WTO hasn't worked and that is one of the reasons we're embarked on this U.S. government actions as focused on 301. But we're in for a really rough period, I think, here and hopefully at the end of the tunnel there will be some better sense of how this system can deal with U.S. system and the Chinese system and the global system can deal with these really complex issues related to tech transfers. I'll stop there.

MR. WEST: Okay, great, thank you Paul. So Chris, I know you work on social media usage by extremists groups. Now until recently, people did not think of social media as a sensitive technology but you show how terrorists have used it to recruit members. There is a similar issue in terms of off the shelf drones. They can be used by hobbyists or terrorists. Do we need to broaden our

definition of sensitive technology and if so, how.

MR. MESEROLE: Thank you, Darrell, for the question and for including me on the panel. I think a lot of tech transfer debates tend to assume that it's between states. One thing we've discovered over the last decade is really that a lot of big geopolitical conflicts and events that we've seen have been driven in part by tech transfer to non-state actors. So extremists and terrorists groups and their ability to use new technologies for ways their authors and originators never really considered.

I want to just situate a bit. Social media and off the shelf drones are really uses of commercial technologies. I'm going to mention briefly in a bit, get back to the point about dual use technologies which is really what the core issue is with these. I want to situation a little bit how tech transfer even happens to non-state actors and terrorists groups in the first place. Because they don't have the resources to have a big research and development budget, they don't have the resources to acquire cutting edge technology. So they're really left with three options for getting decent technology. One is the open source movement. They can go get on just like the rest of us and download tensor flow and build out their own sophisticated machine learning models. Another option is just leaked code. The one thing that I'm pretty worried about is what happens when some of the leaked cyber weapons that the United States had built get into the hands of some pretty bad actors. The third is commercial applications and in particular as the costs curve on many of these technologies decreases, more and more of them become acceptable or accessible to non-state actors.

The challenge for a non-state actor is that even though some of

them do have some pretty advanced technical capabilities, it is still very hard for them to incorporate new technologies in the same way a state would because they just don't have the same level of technical expertise or technical resources. I was just presenting at the UN a few weeks ago on attack and terrorism conference. The question was, our terrorists groups can go down and download tensor flow and build up their own models for AI and effectively target U.S. soldiers, for example, in Syria. I would be very skeptical of that because of the way AI works. You need to couple the algorithm with data and if you don't have access to massive data and massive compute as well, it is going to be hard to build your own model.

What they can do is take the post train algorithms that Google and others have started releasing for image recognition and incorporate into, say an off the shelf drone. I suspect we're going to start to see this over the next couple of years. I think it is something that we're going to have to pay more and more attention to. The advantage that commercial products have is that they tend to abstract away the complexity of the underlying technology. So if you think about the big app, social media, we all know about Twitter and Facebook and their use of social media a few years ago. Currently, most of it is happening on apps like Telegram are end to end encrypted. What the real breakthrough there is, we've had end to end encryption for a while now. What is new is that you can now have access to it through the smartphone app store. I think people forget that what the app store is really doing is abstracting away a lot of the complexity of the underlying technology so that is really just two taps on y our phone. Suddenly, you have access to a secure encrypted device that previously really

only the Pentagon or some other places would have had a decade ago.

So when we talk about the use by non-state actors of these new technologies, the sensitive technology question, I'm not a lawyer so I don't want to get into the fine details of that. I do think we need to start thinking very hard about the use of new communications technologies, new robotics, new drones that are commercially available, very cheap and easy to use and think about the dual use nature of them in advance of their product release. I think if you talk to developers at Facebook or Google today, they would probably admit that they made a mistake over ten years ago when they set up their platforms. They didn't really architect them in a way that would make it difficult for abuse. I would say that going forward for a lot of the commercial technologies like off the shelf drones, there is a lot we can do to make sure that they are no abused in the same way that ISIS and other groups abuse Twitter and social media. I have more to say but I'll leave that there.

MR. WEST: Thank you, Chris. I never thought about the app store as a means of technology transfer but you're right, that is an important point. So I have a question for all of you and then after this question we'll open the floor to questions from the audience. So some of you have suggested the need for additional limits on technology transfer. On the first panel, Richard mentioned that 70 percent of NASA research now is taking place outside of the United States. So the question I want to pose is, if we put new limits on technology transfer, is this going to encourage other countries to do exactly the same thing and with a lot of the RND taking place outside the United States, won't this end up harming our ability to innovate. Whoever wants to jump in, feel

free to do so.

MR. O'HANLON: I'll start and maybe create the down the row dynamic. I'll be brief to say, I think that's a valid concern which is why I want to target the technology areas that we're most concerned about into roughly the kinds of groups that I mentioned earlier plus maybe a couple others but not generalize more than we have to. Recognizing that if we were to try to do so, we wouldn't be successful in the first instance, we would slow down economic development and growth and ultimately it is just not realistic. If you try to limit everything you're going to limit nothing because China is too interwoven with the world economy. So if we're going to try to slow China down, it is going to have to be in a number of specific areas. And even there, I don't want to slow them down as a matter of permanent policy, I just want to try to force them to play by the rules a little bit and maybe buy us a little more time so their political system matures more before they truly reach our level of superpower.

MR. TRIOLO: Yeah that's a really good question. Again, AI provides a good example which we're just sort of grappling with. So, for example, Microsoft and Google both have hundreds of engineers in China developing AI algorithms. So is that a U.S. company, is that a Chinese company, how do we look at these types of arrangements. And then, of course, Chinese companies like Baidu and Tencent and Alibaba have research institutes in the U.S. They are hiring U.S. engineers and software developers in the U.S. And then AI is inherently dual use. I think we're just coming to grips with that. I think what Michael mentioned focused in particular on AI. There is a sense now that AI and other things like automation, robotics, biotechnology are all now becoming part in

the U.S. of the so-called national security innovation base. In part, that's what things like the new CFIUS legislation is designed to better protect.

I think it is going to get complicated because of these issues of the interactions between communities. I think, again, AI, I've done a lot of work on that and looked at the collaboration between China and The Valley. It goes very deep. Most of China's AI engineers and software developers at their leading companies came through Microsoft Beijing, have close ties to The Valley and are very plugged in. There is a lot of Chinese investment as the DIO report points out in startups in The Valley that are driving innovation.

So we have to be very careful in developing new ways to protect real national security concerns and assets that we don't stifle innovation inadvertently, particularly in an area like AI which is still very new in some manner. The idea of the U.S. government, for example, jumping in and determining through CFIUS what investments a Chinese company can or can't do or a VC fund can do in a company in The Valley, gives a lot of people heartburn, to say the least. These are really valid issues to be grappling with but I think the danger in extending out and revamping U.S. legal and other measures to control technology is that we end up stifling innovation in key areas.

MS. ROFF: I'll kind of maybe be the Debbie Downer. It's a good role, I play it often. I think there is a couple of things to think about. Most of my concerns are about artificial intelligence and related and enabling technologies. I think one, we really have to think clearly, not just about AI as a data compute and algorithms but also the backbone on which AI runs. If we're thinking about GPU's, if we're thinking about various types of glitches at the colonel level. If you

think about Specter in Meltdown as indicative of ways of siphoning technology in other types of secrets and encryptions or whatever you want. These are going to affect worldwide the way in which we can keep secrets and keep things that we want to keep secret, secret.

So just thinking about the stacks, just thinking about everything from the chip to the instruction base to the software to the firmware to the hardware to everything right. So I think that's something that we need to take into consideration quite heavily. And then when we think about artificial intelligence, the sensitive technology thing, I'm looking at this from an application base and maybe not an investment base. So thinking about applications that are maybe just not really good ideas. For instance, we have the ability right now to generate fake audio. So going back to my voice and coding example, I can take any person's voice in this room and get about 20 hours of data of you talking and I can create an artificial intelligent agent. I can make it say anything and no one can tell the difference between if it's your voice or the computers. So those AI agents can say anything. I can make it say anything and no one could tell if it's really you or if it's the computer.

Not only do we have artificial audio generation, we have artificial video generation using GAN's, General Adversarial Nets. I think that when we start seeing the coupling of things like fake video and fake audio of somebody anywhere in the world saying things that could be escalatory or inflammatory and no one can tell the difference if that's actually the person saying it, that's an application that in view is a weaponization of information. If we want to talk about information operations as an area of armed conflict, as something that we have

engaged in for decades, more than that really, like millennia, we've called it information operations for decades.

We have to be careful about those types of technologies that enable those types of military campaigns that are based solely on information. And information in this new era is really the heart of it. When you can weaponize information, when you can use information to get ahead of your near peer, when you can think about ways of using information communication technologies to do this, we have to be very clear about what we're regulating, how we're regulating it and when we think it has crossed a line into weaponization that needs regulation.

So again, I would just kind of walk back a little bit from questions of the structural things about where you can go to school and where you can invest to, just think about the application base and where you would use that application for any good reason. It might be a fancy little new toggle on my Android phone but is it really necessary and what are the risks associated with that proliferating to non-state actors to state actors to just your angry neighbor down the road.

MR. WEST: Okay why don't we open the floor to questions from the audience. So if you have a question, raise your hand. We have microphones. Just give us your name and organization. Right up here near the front.

MS. LEHMAN: My name is Jessica Lehman. I recently was working on CFIUS with Department of Defense. My question is protecting U.S. government investments. Especially startups in emerging technology and AI where there is foreign acquisition, particularly from China, for startups that

receive government funding initially. So how do we address issues of basically U.S. tax payers funding foreign countries or companies taking over or acquiring these technologies?

MR. WEST: Okay who would like to answer that.

MR. TRIOLO: I'll take a stab at it. I think on any of these issues like that, the devil is going to be in the details. For example, what sort of government oversight or CFIUS oversight would be adequate in looking at something as complex as ten VC companies all having minority investments in a startup that may not have developed a technology that is viable yet but it looks promising. So I think part of the challenge, and one of the challenges of the DOX report and its recommendations is converting that into useful legislation and then actually enabling a process like CFIUS to actually make intelligent decisions on this without balancing the security and the commercial concerns.

My concern is that as structured right now, CFIUS is heavily on the national security side, obviously. And it may not have the right personnel or resources to really evaluate some of these more complex challenges that involve earlier stage investment in companies that are doing some cutting edge technologies. So I think there has to be a lot of thought given into how that process works. I think we'll know when we have an example of that. I think the first time that we hear of CFIUS reviewing early stage investment in an AI company that involves a Chinese minority investor, we'll have a better sense of that. Of course, what the reality is, and it is mentioned in the DOX report is that just raising this issue has already served as a deterrent and potentially discouraged partners or people looking to put together a consortium to invest in a

particular company from having a Chinese partner. That's already, I think, probably happened, and could happen going forward. But yeah, these are very difficult questions and I think part of the problem is resourcing properly, organizations like CFIUS to help deal with it.

MS. ROFF: I would also say that the devil is in the details as well. It really depends on how far back you want to go. So if we're talking about early stage technologies and early stage companies or companies formed right out of university. So if you look at a lot of engineering labs, right, they're going to come up with some sort of new great widget and they're going to patent it and then they're going to form a company. Probably much of the money that they got to do the research on the widget came from the U.S. government.

I mean, we look back at Google. When you look at the founders of Google, they took money from the U.S. government through various types of grants. So if you're thinking about SVIR's, if you're thinking about getting money from DARPA, IARPA, ONR, AFRL, the Army Research Lab. I mean, there is so much money from these labs going into university labs that prop up the colonels of these ideas. And then they get to a patentable technology and they patent it and they form a really small startup with the lab manager and the guy who invented it and then they go out and they seek VC support to do their startups. So if you're going all the way from the generation of the idea which was funded by the United States government all the way down to VC's investing in a series A, then you have to say, okay maybe that go over to a series A and a series B and a series C. All of the sudden by the time you get down to C, you've got external investors that you didn't even plan on having in your portfolio to prop up your

technology that you don't want to have (inaudible) about. You start being maybe a little bit more open to other types of investors.

That entire kind of patchwork of how an idea gets funded and generated all the way to where it gets IPO'd and then thinking about, now it's IPO'd and I need a market. Now I need to go into a space that has more market like China or Asia, then I have to have force tech transfer. This is such a bad situation. It is so complex. And the incentive structure, I think, that Nicol was talking about, if you're a PhD student in a lab, you need grants. The grants that you're going to get that are going to fund you for serious types of, you know, if I need to build a reactor, I'm not going to get that from the National Endowment of Humanities or something right. I'm going to get that from DARPA, I'm going to get that from ONR.

MR. MESEROLE: The one thing I would add to that, building on one of Heather's points is it is fundamentally different, I think, when the tech investment is for a product versus for the talent. I think if you look at AI in particular, which you can kind of map out as a function of again, kind of algorithms, data, compute resources and talent, algorithms are a wash because most of them are open source. China and the U.S., neither of us is really going to have an advantage. China probably has an advantage in data for a whole host of reasons that I won't get into. They also are at parody or maybe pulling ahead in terms of their compute resources. The only advantage that the U.S. really has in this game right now is talent. So, to the extent that they're funding our companies to acquire or absorb talent is something that we need to think really hard about.

The one example that immediately comes to mind is Andrew Ng and kind of going from Stanford to Google to Baidu. I would imagine that he got a fair amount of U.S. government funding through various means while he was at Stanford. To complicate it further, we need to not just focus on the technology but the talent itself.

MR. WEST: And on the talent side with our current interest in cracking down on immigration, it could drive the talent further abroad which will make this problem much worse. Other questions. Right here, the gentleman on the aisle.

MR. SU: Anfu Su from China Daily. As you may know, the iCloud service in Chinese has already been transferred to a cloud company in a province in far south China. This company will be responsible for the operations starting from February this year. I'm just quite curious about your thoughts and opinions on the risk behind it and what is the consideration of such a deal. Thank you.

MR. TRIOLO: Yeah. That's a complicated set of business decisions on the part of Apple that this involved. There are two pieces of this. One is the JV requirement in China, Apple is essentially operating a cloud service there with iCloud. They were forced to enhance their local partnership arrangement. In this case, they chose the Guizhou company that is associated with the Guizhou provincial government.

I think also, Apple is also anticipating some of the provisions under the new cyber security law in China which are still not finalized but may require certain companies that are involved in critical information infrastructure

provision to localized data. That would include some foreign companies although it is still not clear that Apple would fall under that definition.

I think from a commercial point of view, Apple made the decision also because it made sense in terms of customer service and other issues. So I think it was a complicated decision to do that. I think the media has portrayed this as a security issue. Apple will be keeping control of the encryption keys for users there and has said that it will be very judicious and will respond to, for example, legal requests. But I think there is a general sense that this is a problem but I think we haven't really seen an example yet of the Chinese government requesting data from Apple that is inappropriate.

I think the broader issue of law enforcement access to data is part of the whole picture here. So the Cloud Act was just recently passed in the U.S. which is an attempt to provide a mechanism for law enforcement to gain access to data in the cloud globally. It's going to be very tricky though for countries to be approved by Congress as part of the Cloud Act and have a bilateral executive relationship so that law enforcement data can be smoothly passed.

But your point is well taken and the earlier panel talked about issues like data localization and how that's become a big issue globally. In Apple's specific case, there was a number of considerations that led to that decision to move to Guizhou.

MR. WEST: I'm curious how other countries are handling technology transfer. Like are there good examples out there? Are there lessons we can learn, good or bad examples.

MR. O'HANLON: I want to get back to the topic a minute ago on

our standing in the world competitively. Just to add a broader perspective, in addition to the points that were already made and this is not in any way to encourage complacency. But Chris made a very important point that what we have perhaps over China and other countries now is talent. By which I interpret, the entrepreneurial spirit and the people in Silicon Valley and Boston and elsewhere who are designing new concepts, new applications, new software. I agree but it's not just those people, of course, it's the fact that first of all, they live in the richest country on earth which also is the center of the western community of more than a billion wealthy consumers. By the way, other people who speak English on this planet include another billion Indian's who are increasingly wealthy and much of Africa, much of the rest of the world speaks English as a second language.

The Chinese are a long ways away from being able to compete in these kinds of terms. Also, if you had an idea to make $10 billion, you would probably prefer to make it in the United States rather than in China because you have more confidence in being able to hold onto your money. Which gets to Nicol's earlier point, maybe we can let these people hold onto their money a little too much in the United States in some sense, or maybe we're concentrating wealth too much. But nonetheless, that's an advantage of strong legal environment. The competitive advantages of the American economy are pretty profound and even as we try to erode them through huge budget deficits in a dysfunctional Washington, there is still some pretty strong foundations that are in place. So this is again, not to encourage complacency but just to build on Chris's and Paul's points and put them in a little broader context.

MS. ROFF: Also just to get away from maybe this like consistent discussion of U.S. and China doing this. I think we should also think about, what I think about in artificial intelligence is really the global spread of talent. When you're looking at where you have major sources of investment as well as major sources of talent, there is going to be a giant sucking noise going to France. With Macron's new AI initiative with the fact that France is going to be giving lots of incentives for companies to go. You're looking at Deep Mind just opened an office there. You're looking at London as well. The mayor of London has said things like he wants to make London the center of artificial intelligence. You're looking at Silicon Valley, of course, but that doesn't necessarily have to be the place. Canada right?

I mean Canada is putting so much investment in artificial intelligence. You're looking at Montreal, Waterloo, which Waterloo is one of the best universities in Canada for engineering. It is where Rim initiated with Blackberry which, of course, we can talk about later. But you also have Toronto being a major hub. And then if you really want to say, okay let's get out of this kind of five eyes or western world or EU side of things, no one in this room has talked about Israel. If you want to talk about major types of investments in artificial intelligence, cloud computing and robotics, you should look at Israel. They have massive advances in autonomy and AI.

So if you want to think about security applications in particular, I think again, we need to expand our view outwards from this very narrow western conception as well as this very narrow western conception of it's just going to be a powerplay between Russia and China. Because then all you've done is set the

frame and you're going to get blindsided and you're going to be like what, Iran has really good computer scientists? Yes, they do. So I think this is something that we really need to take into consideration.

MR. WEST: Okay thank you, that's a good point that we need to broaden the discussion. We're just about out of time but we'll give Nicol the last question.

MS. TURNER-LEE: Nicol Turner Lee, Brookings. I actually want to bring this conversation and get all of your feedback on the Cambridge Analytica Facebook scandal. I'm sorry, I'm listening to you all and Chris talking about ISIS won't develop algorithms, I'm not so sure about that. The question I have is universities have typically been under strict scrutiny when it comes to the development of products and services. A lot of them are governed under IRB, there are certain stipulations when it comes to taking government money. The Cambridge Analytica scandal, it was essentially laid out that it was done with the intention of research. Even though it got passed the Alexander guy it really went to Cambridge Analytica but it was sort of repurposed along the way which has then put up this conversation around guard rails. When it comes to the commercial sector engaging in research around, they may not have access to -- they do have access to concealed algorithms which was demonstrated in this Cambridge Analytica piece.

I'm just really curious from all of you. Should we start thinking about when we look at tech transfer putting in stricter scrutiny for the commercial sector that is engaging in more RND on its own terms who sort of feel like permission is forgiveness. We're sorry this happened, we'll come back, and we'll

try to revisit this. Again, I think places, universities and other actors outside of this realm of being much more innovative in the things that they do but it also puts an additional security risk.

MR. WEST: That's a great closing question. Any thoughts from our panel?

MR. MESEROLE: We need another panel for this one. This is such a great question. The way that I think about it is I think about it is that I think we do need to push the tech sector to think much harder about the negative externalities of what it is doing. I think the risk with Facebook, I view that, let me back up. When we're in D.C., we tend to think of policy and policymaking as kind of this higher level thing that happens in rooms like this because we're oriented to view governance in terms of political institutions. But as soon as you go into digital governance, policy is really baked in at the level of code. It is baked into the very architecture of how these technologies work.

So Facebook make a decision ten years ago to effectively growth hack its platform by how they allowed its API to be used. Basically, they allowed your friends to have consent over whether or not your data was going to be shared with a third party. They did that because they knew they would grow faster. They were afraid that if they didn't do that, somebody else would come along and do it and then they would outperform them.

What we need to be able to do in conversations like this is begin to communicate to a lot of the tech companies as they are building the products themselves, not ten years down the road when they already have massive networks affects and two billion people. But early on in their product development

cycle to think about what could go wrong here. We can come up with legislation to target things like what Cambridge Analytica did. My fear with that is that this technology moves so fast that we always end up, we're going to just end up a couple of years behind, always, perennially.

So I think the bigger issue is that folks like yourself, we need to be going out to Silicon Valley and having conversations with them early in the product development cycle. I think you probably would have flagged that maybe that API choice was a bad idea. It doesn't seem like it was flagged internally.

MR. TRIOLO: Just to expand on that, I think if we don't legislate, I think the Europeans will. I think the EU with GDPR coming up, a lot of people were of the opinion that if this had happened after May 25th, that Facebook and Facebook still might be facing some action under GDPR which is going to set the standard for data privacy which may or may not become a global standard. But it will certainly drive regulatory change in Europe and will influence regulatory change elsewhere.

MS. ROFF: Just to follow up on that, Nicol. So when as a fellow at the University of Cambridge, I have to make the disclaimer that the University of Cambridge was not involved in this whatsoever. So just because they co-opted the name Cambridge does not mean that anybody, so let's just make sure my peeps at Cambridge are like, no, no, we didn't do that.

So one, I think also Cambridge Analytica, they knew what they were doing. They knowingly broke the law. So there is one side of the equation, right. If you want to think of this as Cambridge Analytica was shady enough that they knew they were breaking the law. Facebook, on the other hand, was just so

negligent in thinking about oh whatever, I don't know what you're doing, fine here have some data. So I think there was a confluence of gross negligence and probably some gross misconduct from other types of things from the platform and then just knowingly breaking the law. So that is something that we really have to keep in mind.

The other thing too is that I would like to flag the work of a friend of mine, Ryan Calo, who is a professor at the University of Washington. He said things like, look maybe we really do need an FDA for algorithms. Maybe we do really need to set up some sort of institutional structures that when commercial sectors and when, if we need to start thinking also about whether or not it rises to a dual use or expert controls or things like that. We need to have some sort of federal institution. So I think Ryan's work is really amazing on this.

And then finally, to again put my hat on as Debbie Downer. GDPR in the EU is already making everybody a little bit crazy of how they're going to comply with all this stuff, Cambridge Analytica aside. But even in the case of, we might be able to prosecute Cambridge Analytica under GDPR but what we're not going to be able to do is actually have any sort of arbitration institutions for the average person. So GDPR says things like you have a right to your data and you have a right to look at these things and you have a right to bring basically arbitrate if things become wrong. But they've actually not set up any institutions for a right of recourse. So you say well, it's so great on paper. It's like, oh yeah you broke the law, I'm going to go to the judge. What's a judge, we don't have that, we don't have a court on this, we don't have the expertise on this. So unless the institutions are create alongside GDPR and you don't actually have

contradictory things being said, section one here and section two here and they actually contradict each other in some ways. GDPR is a good start but I would not hang my hat on this as being the regulatory system.

MR. WEST: Okay we'll give Mike the last word on the panel.

MR. O'HANLON: Just a very tiny thought which is a much broader perspective with less knowledge than my co-panelists. I would simply observe that it's sort of, the last few years that the private giants are really becoming more scrutinized. Because for 20 years, they were the superhero's right, of the modern economy. You couldn't walk down the street without seeing a book celebrating Bill Gates or Steve Jobs or whoever and they could do no wrong and they were creating this new economy. And they are amazing people. But the Edward Snowden's and then the government debate about Wikileaks, that was taking all the scrutiny and all the hits on what big data was doing to our lives in a nefarious way. That was sort of the extent of the debate through the early part of the 21st century as I think back and perceive it.

And heck, the dot com world was even getting credit for the Arab Spring. Facebook and Twitter helped people mobilize in Terries Square. That was sort of the dynamic for a long time. Now we're entering into a world where I doubt the big ones are ever going to receive quite that much of a by on just being good and being for the betterment of humanity without any questions being asked.

The very last thing I'll say is if you want a general overview of AI and cyber, read Darrell's new book which is called, *The Future of Work*, and it is partly about the future of work. It is also a very nice summary of a lot of these

other issues that we're talking about today. An early plug for your forthcoming book, my friend.

MR. WEST: Okay Mike, lunch is on me after that. We're out of time but I want to thank Heather, Mike, Paul and Chris. Very enlightening conversation, thank you very much.

* * * * *

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