THE BROOKINGS INSTITUTION
FALK AUDITORIUM

FACIAL RECOGNITION:
COMING TO A STREET CORNER NEAR YOU

Washington, D.C.
Thursday, December 6, 2018

Introduction and moderator:

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

Presentation:

BRAD SMITH
President
Microsoft

* * * * *

P R O C E E D I N G S

MR. WEST: Good morning. I am Darrell West, vice president of Governance Studies and director of the Center for Technology Innovation at the Brookings Institution. And I would like to welcome you to this forum on facial recognition software. And for those of you who are watching this online through our webcast, we have set up a Twitter feed at #FacialRecognition. That's #FacialRecognition. So feel free to make comments during the course of the event.

So today we want to discuss facial recognition, and this refers to technologies that can identify particular people based on digital or video images. It's been deployed in a variety of different areas. It can be used to find lost children. It can find people who have committed crimes.

But at the same time, there are grave concerns surrounding this software. There's worry that it intrudes into personal privacy, concern about unfair applications by law enforcement and border security personnel, and a fear about racial bias because the trending data often have many more Caucasian than minority images.

In September, we at Brookings undertook a U.S. national survey of 2,000 Internet users about their attitudes towards facial recognition and we found that 50 percent were unfavorable to the use of this software and only 27 percent were in favor. There were interesting differences both by gender as well as age. Women were less favorable about it than men; young people also were less favorable compared to older people. So I think moving forward as a country we need to determine what we think about facial recognition software and what our policies and regulations should be.

To help us understand these issues we are pleased to have Brad Smith with us. Brad, as you know, is the president of Microsoft. In that position he is responsible for

the company's corporate, external, and legal affairs. He leads a team of more than 1,400 business, legal, and corporate affairs professionals, working in 55 different countries. The global scope of what he does basically means the guy never sleeps. (Laughter) He's either on a conference call or he's worrying about something happening in one of those 55 countries.

He joined Microsoft in 1993, so if my arithmetic is correct that means you celebrated your 25th anniversary this year, which in the technology field that is a real achievement. Microsoft is a long-time financial supporter of Brookings and we really appreciate its generosity and support of our activities.

This afternoon Brad is going to make a presentation outlining his thoughts on facial recognition and then we will discuss some of the issues related to that topic. So please join me in welcoming Brad Smith to Brookings. (Applause)

MR. SMITH: Well, thank you, Darrell. Thank you to everyone at the Brookings Institution and thank you to everyone who's come this afternoon or is watching online. I've had the pleasure of coming here many times over the years to talk about some of the leading technology issues and the intersection between technology and policy, and of course these issues are always changing. But certainly one of the issues of today and the future is really about facial recognition.

As some of you know, these are issues our employees have raised. They are issues that employees across the tech sector have raised. And they've done a good job of encouraging us to be thoughtful.

We published a blog, I published it in July, and one of the things that we said in that blog in July is that we would get to work, that we would learn more about this issue. We thought that there was a need for government law and regulation. There was a

need for us and others in the tech sector to step forward proactively and adopt principles. And so I'm here really it's almost six months later to say we have been working. We've been out talking to people. More importantly, we've been listening and learning from people. And fundamentally, what I want to do today is share with you where we think society needs to go, where we think the law needs to go, and where we think tech companies can go and where we will go as a company in particular.

I do think as one embarks on considering this issue it's not a bad thing to pause and reflect on something that I don't think we actually ever think about. One of the first abilities that we all mastered, even when we were infants, was the ability to tell people's faces apart. Oh, not every face that we might encounter while be rolled in a stroller, but we could tell our father apart from our mother, we might begin to recognize a babysitter or a brother or a sister. It is an innate human capability that we don't actually even have to be taught.

And now here we are and it turns out that computers can do it, too. And the reason we're talking about this in the year 2018 is because of the advances we've seen in technology, specially over the last decade. People started to write about facial recognition in the 1960s. So why now? Why in 2018 is it the issue that it has become?

Well, it's really because of four different technologies coming together. The first is the latest in cameras, 2D and 3D. Not just better cameras, but to a large degree we live in a world of ubiquitous cameras in almost every way we might imagine. Of course, it's one thing to recognize one person. To recognize a person and identify that person you actually need large amounts of data, data of large numbers of people's faces. And so we've seen enormous advances this decade in the accumulation of data.

Now, having data is one thing, using it is another. And this is where we're

seeing advances in artificial intelligence, specifically machine learning and algorithms. You put those two things together and people with the right amount of computing power and data storage can actually put facial recognition to work.

But there's one other advance that's been critical, as well. It's the Cloud. What the Cloud has done is made that vast amount of computation power and data storage to everyone. And so you don't have to go buy the computers yourselves and invest in them in order to put facial recognition to work.

Of course, it turns out that there's one other attribute about human beings that is interesting to think about. There actually is a science behind our cognitive ability to recognize people's faces, and that science is now at work for computers, as well. Because it turns out that our faces are as unique as our fingerprints. We all have unique characteristics, it may be the distance of our pupils from each other, it may be the size or shape of our nose, it may be the edge of our jaw. But when computers can use photographs to chart all of those features and knit them together you actually start to put together the foundation for a mathematical equation that can be accessed by algorithms.

Now, I'm here in large part to talk about what this means for society in terms of what governments are going to need to do, how we think about the risks. But before talking about that, it is absolutely critical to note that this technology is actually starting to change the world in lots and lots of very positive ways. We see this working with our customers around the world and the scenarios that are emerging are really interesting.

It might be the National Australian Bank, which is working with us and has now developed a concept, a proof of concept so that you can walk up to an automated teller machine, an ATM, and in a secure way, instead of pulling out your card, have it recognize your face and then you enter your PIN and you're able to withdraw money.

Or it's helping in the context of identifying certain diseases. Here in D.C., in Washington, as part of the National Institutes of Health there is the National Human Genome Research Institute. And one of the things that the institute did a year ago was focus on an important disease called 22q11.2 deletion syndrome. It's a disease that tends more often to afflict people who are African or are Asian or Latin American. And it can lead to a variety of challenges for people, but it often manifests itself in facial characteristics. And it turns out that facial recognition systems can help doctors recognize a patient who has this faster than would otherwise be the case.

Or in some ways and even more immediate way the police in New Delhi this past year used facial recognition technology to identify 3,000 children that were missing. And they could then find those children and reunite them with their families.

Of course, the beauty of facial recognition is it's not just useful for the children of the today or the people who are alive today. At Virginia Tech there's been a project using facial recognition to go back through the archives of photographs of soldiers who were in the Civil War. And some of these people have been identified, but not in every photograph, and hence it is enabling historians to identify certain individuals.

Or in a way that is more likely to impact our daily life Delta Airlines is using facial recognition so you can first check in. And then when you walk down to drop off your bag, the system can remember who you were based on just a few moments ago and you can drop off your bag and it will record that your bag is now on its way to the airplane.

We're seeing it in the world of automotives. We're seeing Subaru with its Forester car and its Drive Focus technology use facial recognition so that you can set your seat and how you want it to be aligned. And then when you sit down in the car it recognizes you and you don't even have to do anything for the seat to adjust. And you can use the

service so that if you're on a long drive, it can make sure that you don't get drowsy, that you're not beginning to lose the ability to pay attention. If you are, it can sound a warning and alert you.

Finally, there's a fascinating example within Microsoft itself where it's not just our technology being used by customers, but it's our technology being used by ourselves. And we've created an application called "Seeing AI." It's the kind of thing that can have a profound impact on the lives of people who are blind or visually impaired because we all walk around with a smartphone and all of our phones have cameras. And with the help of an earpiece somebody who is blind can be sitting at a table in a restaurant or in a conference room and the computer can recognize who it is who is just approaching us and let us know by recognizing that person's face.

So it's important to recognize that there are many, many good things that can and will come from the adoption of facial recognition technology.

Now, recently, there's been important work to test algorithms in the facial recognition space. The National Institute of Standards and Technology has been at this for a number of years. And by coincidence, the day before Thanksgiving they published their latest test.

Forty-five different companies submitted algorithms so that they could be tested and compared to algorithms that were tested earlier in this decade. Microsoft was one of the companies. And virtually across the board our algorithms came out at or very, very close to the top.

I think that's important to say for one particular reason here. Because sometimes when I go to Silicon Valley and people say, oh, I hear you are calling for regulation of technology, I guess you all must feel you're behind, no, we are ahead. We are

at the forefront of this industry when it comes to the development of this technology. We believe that regulation is needed not because we're looking for help because we're behind. We believe that the world needs to have confidence that this technology will be used well, that people's rights need to be protected. And we also believe that if the world has confidence and people's rights are protected, then we'll be able to innovate in ways that benefit society.

So we believe in the importance of law not because we're behind, but because we are ahead. And I think that's the right thing for us to do.

But, of course, as enthusiastic as we are about the opportunities, we also all need to be clear-eyed about the challenges that facial recognition is creating because there are real challenges. And that's why in July, when we said we would get to work to study, we're here in December, that's why I am here in December to say it's time for action.

It is time for people to move forward. It is time for governments to start to legislate and it is time for tech companies to put in place new principles and protection for a very specific reason.

Right now the facial recognition genie is just beginning to leave the bottle. We can think thoughtfully as a society and as a planet about how we want this technology to be governed. But if we just say let's watch and then come back and sit down in some future year, it will be too late. Well, it will be far more difficult to bottle everything back up. So the time to act is really now.

We also think about this from another perspective and it's true in many product markets and in other areas of the economy. We don't believe it's in society's interest to watch a race to the bottom occur. We don't think it makes sense to have a market that is free of regulation that, in effect, ends up forcing tech companies to choose

between being societally responsible and gaining market share. And if we don't put a regulatory floor in place, that is the risk that we run.

We've turned down deals because we didn't believe that the technology would be used well. We've turned down deals because we worried that the technology would be used in ways that would actually put people's rights at risk. But, of course, like any company, you don't want to see the race run by some people who are taking the high road while others who may just not be thinking enough about these issues cause the market to tip. So the time to put a regulatory floor in place is now, as well.

What should that floor look like? Well, that's really the number one question that I've come here today to talk about. Because we think that we've reached the point where governments can start to legislate. They can legislate in 2019 and they can do so in three areas and I'll talk about each of them. They can legislate to address the issues of bias, issues around privacy, and issues that go really to the protection of our democratic freedoms and human rights. And, in fact, it's important for legislatures to focus on each of these three areas.

The first is bias. It has been now well-documented that there are risks of bias not just in the development of facial recognition technology, but in its deployment, as well. Because even if something may work well in a laboratory with a particular dataset and a particular use scenario, it may not work equally well in the field with another dataset or another scenario. And researchers have documented it at this point that there is evidence of bias. There are marked differential error rates when this technology is deployed in certain scenarios, especially for women and for people of color. And hence the risks of misidentification rise when it's used in those communities.

Now, the good news is the tech sector is at work to address this. And the

market, we believe, can encourage the tech sector to address this well and to move even faster. But think about what you need to put to work in order for a market to be healthy and for market dynamics to help solve this kind of problem.

Well, when you think about it, it actually becomes obvious: The market needs to be well-informed. That's why when we go to the grocery store we have the opportunity to read the label on a product. People deserve to know what they're buying. And that is true whether we're going to the grocery store or whether a company or a government or someone else is, in effect, buying a facial recognition service. What we need to do is put laws in place that will ensure that people can act in an informed way.

How do we do that? Well, in effect, it's a two-pronged approach that can both be addressed relatively straightforwardly in the form of new laws. The first is to impose an obligation around transparency: to do what really needs to be done to require tech companies to document the capabilities and limitations of these services and to do that in ways that are clear and understandable. That is a first step. In some ways it's the first step for addressing all of the issues that we need to address.

But there's a second step, as well, and it builds on this obligation that should be created around transparency. We need to enable third party testing and comparisons. Think about the world today. Think about the vital role that groups like Consumer Reports play. Think about what that has done to really improve the safety of automobiles, and it's just one of many products that we rely on every day in our lives. So what we need to do is not only impose an obligation of transparency, but we need to require under the law that the companies that are in this business of providing facial recognition technology, in fact, enable third parties to test these services for accuracy and for unfair bias.

And there are relatively straightforward ways to do this. These have

emerged in the field of technology regulation over the last 15 years. And, in effect, what one can do is require that any company that makes these services available over the Internet, which is the way that they are made available, actually do so with an API, an application programming interface, that will enable third parties that are in the business of testing to actually access the technology and either use that API or some other technical capability suitable for the purpose, so that the service can be used and services can be compared across datasets.

And if we encourage and create that kind of educated market, I believe that we can move faster here in this country and around the world to reduce the risks of this kind of bias.

There's another issue that we need to think about in the context of bias and that's the real-world scenarios that may be encountered today. After all, it's one thing to say don't worry, we're going to create an educated market, it's going to put pressure on companies over time to get better and better, but if you're misidentified tomorrow afternoon, knowing that there may be hope beyond the horizon isn't all that much solace for you today. So we really need to act, as well, to address the use scenarios that are already emerging where these risks of bias are creeping in.

How do we do that? Well, fundamentally, it comes in a relatively straightforward way: that the law require that the people who develop and deploy facial recognition technology ensure meaningful human review. Meaningful human review by trained individuals so that when a facial recognition services identifies someone based on a computerized technique, there is a human who actually looks at the result and thinks about it and does so in particular when these results are used to make key decisions.

And one can prescribe the category of decisions in the law. It's not the most

complicated legal challenge ever encountered. But certainly when decisions are made that are going to impact a consumer's privacy, their personal freedom, their ability to enter a place, or some other aspect of their fundamental or human rights or in other situations, it is not extraordinarily onerous to say the least for the law to require that human beings review data before decisions are implemented.

In a sense, this connects to the final point when it comes to bias. We actually benefit from reminding everyone -- individuals, companies, governments, NGOs, and the like -- of what actually is obvious: just because we use technology to do something, we're not immune for our duty to do something legally. We live, thankfully, in a society, in a country, and even in a world with a variety of laws that prohibit discrimination in different settings. And simply because one is relying on facial recognition, one does not get a pass when it comes to abiding by the discrimination laws that are in place. And it is important for people to be reminded of that as they put facial recognition to work.

So that's the first issue that can be addressed legislatively, this question of bias and discrimination.

That really takes us to the second issue, privacy and really consumer privacy. And I think there are many things that we can learn from as we start to contemplate a future with potentially ubiquitous cameras connected to computers that can recognize people as we go about our day.

I find a lot of insight in this quote, a quote that says, "Recent inventions in business methods call attention to the next step, which must be taken for the protection of the person." It is a quote that speaks to the people on this street in our day. But those words were not written about the people on this street in our day. Those words were written about these people on this street in this day.

And the business inventions, the recent inventions in business methods they were talking about, were fundamentally about this, the camera. And it was about the invention of instantaneous photographs, the fact that cameras had progressed to the point that you could get a photograph immediately rather than through such a lengthy and laborious process of developing film.

And what one found when this was written was that newspapers in the era of yellow journalism were taking these cameras out and, in part, capturing images of people on the street where they didn't necessarily want to be seen. And they were selling those images. And what people concluded, as you see in the rest of the quote, was that it had "invaded the sacred precincts of private and domestic life."

When was this written? In the 20th century? No, this was written in the 19th century. It was written 1890, over 125 years ago, in one of the most famous articles ever written about privacy. It was written by Louis Brandeis and Samuel Warren in their Harvard Law Review piece about the right to privacy. And their view that the right most valued by all civilized men is the right to be let alone.

Think about what they wrote about. Think about the world of instantaneous photographs, that was what captured their imagination. I don't think they ever imagined the world of instantaneous photographs that we are going to experience as our lives continue to go forward. Because we are entering a world where it will be possible to step into the shopping mall and have a camera not just take our picture, but recognize who we are. And it will be a world where it will be possible to go from store to store and from place to place and have these cameras record everything we look at, everything we pick up, everything we purchase, everything we choose not to purchase, every person that we talk to, and every person we meet.

Now, the truth is there are retailers that are doing some pretty amazing things that people will want to benefit from. Because we're seeing retailers innovate in all kinds of ways, ways that will make shopping in a grocery store far faster and more efficient. There will be new experiences that are beneficial. So the issue here is not whether can people do this? We would be the first to say no, the world will get better if people can put this technology to work.

But there are new risks. There are new challenges. And so once again, we should really think about the world we ant to create before we rush forward and create it. And that's why the law needs to move forward in this space, as well.

Certainly there needs to be notice so that in a conspicuous way, before you walk into a store, if the store is going to be use facial recognition to identify you, record you, and the like, it lets you know. Once people know, they can begin to ask questions. They can begin to talk to each other. They can begin to vote with their feet or if they're online they can vote with their thumbs or their fingers on a keyboard.

And then we're all going to have to talk through an issue that, frankly, is more complicated than notice, and that's consent. Because in a world where we expect consumers to have the right to consent to use of their information, we need to start thinking about and talking about how we require the obtaining of consent when it comes to the use of this in public places, in stores, by retailers, and the like.

Well, there's obviously a straightforward way to start and that's simply to say that consent is implied at least in a limited way for particular uses when people see the notice and they walk in. But I would venture that over time we're going to see innovation in this space. We're going to see innovation that has led perhaps in the United States, perhaps in Europe, perhaps in other privacy-oriented jurisdictions to give consumers the

ability to express or exercise their right of consent in new ways. And this is going to be an important topic and it's going to have more than its share of complexity.

And then there's the third and final issue. It really goes to our democratic freedoms. And I think here, too, it's important to recognize that there many uses of facial recognition by the government, by the state that are societally beneficial. They will keep us safer in airports. It may keep us safer in a stadium or at a concert.

If someone enters and then one realizes that that person is on the loose, well, it may be vitally important to use facial recognition to identify quickly where that person is if the person is a threat to public safety. So we should be thoughtful here because this will be important in addressing public safety.

But we need to be balanced. We need to strike the balance that our society has always needed to strike: between safety and democratic freedoms. When you think about it, our democratic freedoms so often turn on the ability of people to assemble, the ability of people to speak, the ability of people to go out and address the public. And these rights that we take in such a treasured way in this country under the First Amendment, in fact, in many ways can be put at risk if we enter a future that is very different from the past that we've ever lived in, not just in this country, but really in the history of humanity. Because the truth is technology is making possible a new type of mass surveillance.

It is becoming possible for the state, for a government to follow anyone anywhere. It's making it possible for a government or the state to follow everyone everywhere. In fact, it's becoming possible for the government to follow anyone anywhere at any time or all the time.

And it's important to pause and reflect societally before we let this future just rush ahead of ourselves. I think it's worth reflecting on some of the more thought-provoking

things that have been written over time because the future I just described has been written about. It was almost 70 years ago that it was addressed by George Orwell, and he painted a picture of Big Brother watching our every move.

So there's a very important question that we in democratic societies most especially need to think hard about: When are we comfortable allowing the state to follow us everywhere using this new technology on an ongoing basis to keep track not just of where we are at a moment, but everywhere we go throughout the day and indeed every day?

The time to think about this absolutely is now in my view. If we fail to think these things through, we run the risk that we're going to suddenly find ourselves in the year 2024 and our lives are going to look a little too much like they came out of the book *1984*.

So what do we do? That's the fundamental question that we all need to think about. In our view, the time has come for legislation to address this issue, as well. And what we would say is that ongoing government surveillance, "ongoing" meaning following someone around using facial recognition, should be permitted, but in defined circumstances only. That we should permit law enforcement agencies to use facial recognition to engage in that kind of ongoing surveillance of a person, a specified individual, in public spaces only in two circumstances.

The first is when the government goes to court and gets a court order. After all, that really is the foundation in our society for surveillance and it always has been. And typically, a court order is based, in this country, on a finding by an independent judge or magistrate of probable cause that an individual has or is committing a crime.

But there is a second narrow circumstance where we think it would be appropriate for governments to act, as well: when there is an imminent risk of death or

serious injury. If there are situations where someone has been identified if they, for example, entered a stadium and then you realize who is there and you need to start to follow that person around so the police can apprehend the person, there may not, in fact, all the time be the time to go get a court order.

And as we think about this, we think it's worth doing so through the lens of one particular set of issues. It's the issues that this country has always dealt with since the Bill of Rights was adopted in the First Congress, and specifically the Fourth Amendment. I've come to the Brookings Institution to talk in the past about the Fourth Amendment. And typically, we've talked about the Fourth Amendment in the context of where it originally began, where it typically arose: the police going to someone's home or into their office, to go into a building, or more recently to access data in a data center.

But I actually think it's a moment in time when we should remind ourselves of what the Founders of our nation actually wrote when they put pen to paper and drafted the Fourth Amendment. The first thing they wrote about was not people being secure in their houses or their papers or their effects. It was being secure in their persons. Because that actually, even literally, is what this issue is about.

But it's also, I think, helpful and important to think about where the Supreme Court itself has been going with Fourth Amendment jurisprudence over the course of the past decade, where the Fourth Amendment has been evolving even this year. Because this is an important year, as so many years have been important this decade, for the Fourth Amendment.

It was this year that the Supreme Court issued the decision in the so-called *Carpenter* case. And the *Carpenter* case, interestingly enough, I think actually addressed an issue that should speak to us as we think about facial recognition.

The question was when can the government or the state go to the telephone provider that you use for your cellphone and access the cell location records? The cell location records, of course, show somebody who has them, including the government, where you're moving. It reflects your physical movement because that is then reflected in those cell tower records.

And what Chief Justice Roberts wrote for a majority of the Court was that in the 2018, people in this country have a legitimate expectation of privacy in the record of their physical movements. And as a result, what the Court decided was that we have a constitutional right to privacy when it comes to our cellphone records. And hence the police cannot access those without getting a warrant.

Well, what are we talking about when it comes to facial recognition? In this scenario we're talking about the movement of ourselves. And so in a very interesting way, I think, facial recognition raises a new constitutional question. Do our faces deserve as much protection as our phones?

If our faces are being used to record our physical movements, then we believe that the answer is and must be a resounding yes. As a company we at Microsoft brought not one, but four lawsuits this decade against our own government to stand up for the fundamental rights that we believe people have to privacy in the context of surveillance. And we believe that this is part of the next generation of issues that our country will need to work through.

And, of course, we don't need to wait for this case to get to the Supreme Court. We don't need to wait for it to be decided as a constitutional question, although I think we can all safety predicted that that day ultimately will arrived. What we can say here and now is that it's time for legislatures to protect this as a matter of statute while we all go

forward and sort out its constitutional implications.

So those are the three areas where we believe that legislatures should act, where laws should be written, and where regulation is needed. And then I would say that there's one more thing that we're thinking about, as well: tech companies need to act.

We should not wait for the government. We need not wait for the government in order to act responsibly. In fact, we need to act in part because this is an issue not in one state or one country, this is a global issue. And our industry needs to address these issues head-on.

That's why one of the things I'm announcing today is that we in Microsoft are acting. We said in July that we would develop principles and that we would apply ourselves and now we are. So we're sharing today the six principles that we are going to adopt and we're publishing a blog today that in addition to describing the legislation that we believe is needed, we'll also give you a short summary of the principles. And then next week, we'll complement these with more details about each of these.

But when you look at this list of six principles, they really correspond to the issues that I've been talking about. They've been talking about the need for us to act to ensure fairness; to be transparent ourselves even before governments act; to ensure accountability, and by "accountability" I really mean meaningful human review; to act to guard against discrimination; to develop services and work with our customers to address notice and consent; and fundamentally, to take a responsible approach not just in this country, but in every country when it comes to the risks of abuse even in the necessary scenarios where we need lawful surveillance.

I want to underscore that while we're going to implement these principles at our own company, we're actually committed to working much more broadly, certainly across

our industry. But one of the things that we'll need to do at Microsoft is go from where we are today, having made the decision about the principles we're adopting, to create policies, to create technology tools and systems so these can be applied across a very large company, to have monitoring and compliance systems in place. So what we're saying today is that we will implement these principles with this kind of support by the end of March next year.

And we're also saying that we will create materials for our customers. We will work with out customers because what we're finding is that most customers want to act in a responsible way. But like all of us, they don't yet have all of the acumen that we'll take for granted 5 or 10 years from now. So we're committed to sharing tools, sharing curriculum, sharing training, and working with customers so they can be responsible.

In closing, I was just say this. I'm not here because we have all the answers, because we don't. We don't have all the answers. This technology is very young. And I think we're all well-served by donning a bit of humility and recognizing that, frankly, we're at a point around the world where we haven't yet even identified all the questions. That's why it's so important to have conversations about this. It's why, in our view, it's so important for governments to start acting. Because if governments act in a limited way, then governments will learn faster. We'll all learn faster from those governments who act.

Because as much as anything else, we think it's time for a different approach as we think about the role of technology in the world. Instead of saying that technology should go forth and then we'll decide what governments should do, we instead need to say this is a time when governments need to keep pace with the pace of technology. And we should recognize that as long as we act in an incremental and thoughtful way, it is more than appropriate to act before we have all the answers.

As much as anything else, it's a time for a dose of common sense. And in

this country, for generations, common sense has always come by a few authors, including Mark Twain. And as he said, the secret of getting ahead is getting started.

It's time to get started. That time is now. Thank you very much. (Applause)

MR. WEST: Well, thank you very much, Brad. we appreciate you sharing your thoughts with us. It's definitely thought-provoking. So does this mean this is the start of your presidential campaign? (Laughter)

MR. SMITH: No.

MR. WEST: So --

MR. SMITH: I am the president of Microsoft. I didn't campaign for it.

MR. WEST: So you're already a president. That may be a better job anyway.

So today you called for two things: more public regulation and a stronger sense of corporate responsibility on the part of technology companies. So I want to push you on each of those two things.

So focusing first on the legislative and regulatory angle. So you outlined several new requirements: more company transparency on the capabilities and the limitations of the technology, third party testing, addressing discrimination, meaningful public notice when facial recognition is being deployed. So these changes we can imagine taking place at the city, state, or national levels. Where do you think people should be focusing their activism? Which levels represent the most promising opportunities for action?

MR. SMITH: Well, I think it's a fascinating question. And of course, when one comes to Washington, D.C., I think one rightly asks the U.S. Congress to consider moving forward, and we do. This is not the most complicated issue that this or the next Congress will have to address, and I think it is appropriate for federal legislation.

But in this country especially, I think we often appreciate that the states, or sometimes these days the municipalities, are the incubators of new ideas. And so we're hopeful, in fact, that we'll see new privacy legislation passed in the next two years here in Washington, D.C. And we would advocate that the Congress include a chapter on facial recognition in a new privacy law. But I think we might see action even faster in one or more states.

And what is really interesting when you think about these issues is to think about them with one particular distinction in mind. Some of these issues, like the protection of democratic freedoms, like the protection of people's privacy in, say, commercial spaces, really needs to be thought about everywhere. It's going to be something that's important in every jurisdiction not just in the United States, but around the world.

But think about the proposal I outlined when it comes to transparency and enabling third parties to test technology. We don't actually need to get that passed everywhere. We just need to get it passed somewhere that matters. Because if a state that has enough clout in this technology spaces, for example, that kind of transparency and testing requirement, then the tech companies that are likely to say, okay, I want to participate in that state, or maybe I'm headquartered in that state, if I want to be in this business I have to make the data available. And once the data is available somewhere, the data's available everywhere.

This is something that we learned from our own experience from technology regulation in Brussels over the years, and it actually means that we can get this market working in a healthy way really quickly. And so one of the things that we're hopeful that we'll see in 2019 is a state of significance in this context, or perhaps a collection of cities, move forward and the market will be healthier as a result.

MR. WEST: Okay. So I'd like to ask about some other possibilities for legislation that some consumer groups have endorsed. So one idea is to limit data usage in regard to facial recognition in particular to the initial purpose, so meaning that you may go to the airport, the airport may collect your facial image in order to safeguard security, but they should not be transferring that image to other venues for other purposes. Should we favor that?

MR. SMITH: I think that that is a great question that, frankly, deserves a robust discussion. It's one of these things where, frankly, we thought about it and, as you can see, we offered a more limited step. But like I said, we don't offer any of these steps saying, oh, my gosh, we are the ones who necessarily have the world's best answer.

I think that there are a variety of scenarios. And, you know, the image that I showed you of Delta at an airport, in fact, the sign they say basically -- right there says this image isn't going to be preserved. So by definition they would comply with what you're saying.

You know, there are scenarios where one might say it should only be used for that specific purpose and for a limited period of time. There might be other scenarios where you would want the ability to get somebody's consent in a broader manner. And yeah, I generally favor opportunities for people to be notified and give extra consent, but I think it's also more than appropriate to talk through, well, what are the extra protections to make sure that that consent is real, that people have a choice, that it's really informed.

So, yeah, I think that there's, frankly, a lot that we're going to learn certainly at Microsoft, I suspect across the tech sector from consumer groups and the civil liberties community as these kinds of issues evolve.

MR. WEST: So a couple of other possibilities. Some people have

suggested the ability to be to correct your data if you can show the data are inaccurate. And then secondly, the right to be forgotten, which, of course, you all recognize from the European Union General Data Protection regulations. Storing facial images only for a certain period of time. What are you views on those things?

MR. SMITH: Well, I think one should put these kinds of issues in the context of what is rapidly becoming a broader privacy discussion in the United States. We as a company, I as a leader of our company, came to Washington, D.C., in 2005, 13 years ago. I gave a speech where I said we thought the time had come for national privacy legislation in the United States. I didn't give it at the Brookings Institution, I gave it on Capitol Hill, and maybe that was the mistake because nobody listened. (Laughter) We are 13 years later and I actually think that one of the good things about the year 2018 is, it's great, we're seeing companies like Apple and Salesforce and others saying, no, now is the time, we do need national privacy laws.

And one may want to tease apart some of these issues, but as a general matter the kinds of rights that individuals have today in Europe, say the right to access your data, the right to correct your data if it's wrong, the right to delete your data, the right to take your data and move it to another provider, we are the only tech company this year when the new regulation took effect in Europe on the 25th of May that said we're going to take all of these rights that these individuals have in Europe and we're actually going to make these rights available to all of our customers everywhere in the world. And so we've been living since the 25th of May with this kind of approach.

And there's been one piece of learning that I think has been really, really interesting and even a little bit surprising. Since the end of May, 2 million citizens in the European Union have exercised their rights on Microsoft's services. Two million people in a

union with 500 million people. In the United States, the number isn't 2 million, it's 3. Three million Americans in a country that is smaller in terms of population than the EU. I think that tells us something. It tells us that Americans care about privacy.

And this almost mantra that one heard in the tech sector 5 or 10 years ago that privacy was dead and that people didn't care about it should be dispelled as a myth. It is a myth in my view. People do care about privacy. It deserves to be protected in this country. And we'll have to work through some of the specifics along the lines you mentioned, but I think Americans deserve a high level of privacy protection.

We'll need to work through nuances. You always do, especially when as we think about where AI and access to data is going as we think about issues like anonymization and the like. But I think in the privacy field writ large it's time for us to get moving.

MR. WEST: So I'd like to move to the corporate responsibility angle. So we know the U.S. is pretty libertarian in its approach to technology innovation. Companies have quite a bit of leeway in terms of what products they introduce and how and when they do that.

Now, you suggest companies, especially in the tech sector, should exercise more self-restraint and should not always commercialize products to the full extent that is possible. So the question I have, is this really viable in a competitive marketplace where you may decided not to sell facial recognition to law enforcement, but somebody else is going to?

MR. SMITH: We live in a year when expectations for the tech sector have grown, and I don't think that's a bad thing. Yeah, I get to work with people not just at Microsoft, but across the tech sector and I don't meet bad people. I don't meet thoughtless

people, but I often meet people who work at places where it's hard get decisions made. And when you're at a company, it's sometimes easy to just keep going in the same direction that you started unless somebody makes a decision to change course. And we're at a time when a course correction, in my view, is clearly needed in many areas of technology.

And so I think that the broader public conversation that we're having is helping us all to learn more, to be introspective. A little humility definitely never hurt anybody, in my view. It's time when people are having to make some decisions. And so I think it's good to encourage companies to be more decisive on this and other issues.

I do believe at the end of the day that there's one decision that you can easily persuade every company that has even the smallest dose of responsibility to make, and that is the decision to comply with the law. And so let's get the law in place. We'll get everybody on this new floor. We can then talk about the world as a whole.

We can talk about the competition that may come from companies in other countries that won't have a law like ours. We can talk about making our case, frankly, and appealing to the hearts and minds of consumers in other parts of the world where I think people care about the protection of privacy, the rights of the individual. This is a time when I think those issues not only should matter, but do. And we need to be able to act more effectively to address them.

MR. WEST: So I'd like to ask you about racial and gender biases, which, of course, you referenced in your talk. And we know that there are higher inaccuracy rates for racial minorities and women based on unrepresentative train data. And there actually was a very sobering example of this this summer when facial recognition was applied to minority members of Congress and it inaccurately concluded that some of them were convicted felons. Now, if this were the whole Congress, that might actually be accurate. (Laughter)

MR. SMITH: Not convicted. Not convicted.

MR. WEST: By the way, that's my comment. That's not his comment. (Laughter) But, you know, these were minority legislators. So should there be some minimum level of accuracy required before we put technology like this into widespread use? And if there is a misidentification what recourse should the affected person have?

MR. SMITH: Again, a great set of questions. And what I put forward on behalf of Microsoft is something that we think says let's move quickly and get the market working and then we'll see if the market can address this problem.

I think it is a real issue that needs to be addressed. I'm actually encouraged by the technology advances that we've even seen this year, so there is a real progress. Some of the problems relate, especially in the past, to issues around datasets, datasets not being as large or as comprehensive as they need to be, and people are more sensitive to that. People are developing new technical approaches to address issues around datasets, that you can build a dataset and complement it through simulation technology and the like. So I think that's interesting.

You know, frankly, one of the things that gives me just a bit of pause is that when I read something like the NIST study that came out a couple of weeks ago, it tested 127 algorithms from 45 companies, but there are some companies that didn't make their algorithms available for testing. And so that's why I think it's important to have an approach that gets all of this data made available and let's see where we are. Rather than take five years to debate the issue and then impose more absolute requirements, let's see if the right combination of law and market incentives can solve this problem in a couple of years. If not, then we may need more protections.

MR. WEST: So I have one more question, then we'll open the floor to

questions from the audience. So in your talk you mentioned George Orwell's book *1984*. And I have a personal angle on this. My wife is an actress and literally this summer she performed in a theatrical rendition of this very play. So, of course, I had read this book many years ago, but I have to say this summer it was quite eerie to see the play now after the advent of facial recognition software, advances in artificial intelligence, and, of course, the spread of video cameras to every major city around the world.

So what seemed to be a dystopian abstraction in 1949 when Orwell first published that book seems a lot more concrete now.

So I'm thinking about mass surveillance and the possible threats there. You mentioned that we need legislation that would prohibit government agencies from using facial recognition to engage in surveillance on specific individuals unless there was a court order or an emergency involving imminent danger. So how would that operate and what do you think would be needed to actually implement that type of role for U.S. Government agencies?

MR. SMITH: I don't think it needs an extraordinarily leap forward in the way that the law works. And the first thing I would note is that when you read Chief Justice Roberts' opinion in the *Carpenter* case you almost have to ask yourself, you know, if a law enforcement agency implemented this tomorrow, and an individual were arrested based on the information obtained by following that person around and that individual went to court, would that individual win a case before the Supreme Court under the Fourth Amendment? It was a 5-4 Court, but interestingly and importantly in this context it was not a 5-Justice majority that relied on Justice Kennedy. So I actually think that there would be certain grounds for optimism that the Supreme Court would protect that right.

And in the same that law enforcement has adapted first earlier this decade

to recognize that law enforcement couldn't put physically a cellphone -- I'm sorry, a GPS locator on a car, and has now said that law enforcement can't go to a telecommunications company and obtain the cell location records. Instead, they have to do what law enforcement knows full well how to do. It's called go to court and ask for a warrant, that we would begin to implement that in these particular contexts, as well.

There's two things that I just think are worth keeping in mind from a broader perspective. The first is Orwell's book. I think that the best way to avoid a problem is sometimes to be able to see it very clearly. And that is one of the services that great literature does for the world and it's what Orwell did for the world. And when you read that book through the eyes of 2018, you realize that that world is now possible, but it's not inevitable.

And the other thing that really inspires me, frankly, is when I read the opinions of Chief Justice Roberts in the *Carpenter* case and in the *Riley* case against California from a few years ago. Because for him, there's a work of literature, it was a letter. It was the letter written by Abigail Adams -- or really to Abigail Adams by John Adams on the 3rd of July, 1776. And in that letter Adams remembered a trial that had taken place in Boston in 1761, when the British government started using these general warrants to go from house to house. And Otis lost his case, but it was that loss that in many ways Adams said inspired the colonists to pursue these rights. And Adams to the day he died said that really it was that day, that case, that courtroom that set the nation on a course of independence.

So we'll all have to work through where do the commas go in sentences in new statutes, but if you can remember one future that was painted by George Orwell and say that's the future we want to avoid, and if we can remember this vision from the past that

made this country what it became and what it has always been, I think those kinds of things, frankly, play a really important role in helping us for our generation find the right path.

MR. WEST: Okay, let's open up the audience to questions. Right here on the aisle there's a woman and there's a microphone coming over. We would just ask you to ask a question as opposed to giving a counter speech.

SPEAKER: Hi, thank you so much for being here. I was wondering how you plan to use the position of Microsoft to advocate for these kinds of changes in Congress and also bringing other tech companies into the fold of advocating for it; educating those who might be against it, such as law enforcement organizations or other companies -- we won't name any names. And then have you already reached out to any House or Senate offices or other offices you'd like to see take the lead on this initiative? Thank you.

MR. SMITH: Yes, yes, yes, and yes. (Laughter) No, I would say --

MR. WEST: Okay, next question, please. (Laughter)

MR. SMITH: No, we've been talking with other tech companies, the trade associations, the civil liberties groups, the privacy groups, the consumer groups, law enforcement groups. You know, this needs to come together around a big table with a seat for everybody. So we've been talking to a number of people.

I've been talking with people, senators and members of Congress. We've been talking to people in certain state capitals. And we've been working with legislators on the drafting of legislative language. And so we hope that things can start to move.

And, look, as you all know, you live here every day, I visit. You don't get anything done without people coming together, without ensuring that everybody's voice is heard, without finding certain paths to compromise, especially when one is talking about legislation.

I always think one needs to be a little bit more circumspect or sober these days in Washington, D.C., just because it's a decade when it's proven generally difficult to get things past. I'm hopeful that we'll see Congress act, but I'm probably more optimistic that if something's going to happen in the first half of 2019, it may happen in the state capital or even in a municipality, and that's okay because that will put us on the path ultimately to national legislation.

MR. WEST: And if I can add just one quick footnote to what Brad said. A couple months ago, I addressed the Midwestern Governors Association. And I can tell you, people at the state level are really engaged in these issues. They're thinking about them. Of course, they're interested in the economic development aspects of technology, but they can also see warnings signs just based on everything we read in the newspaper today. So I think there's a lot of interest at every level of government.

Okay, there's a question here.

SPEAKER: So I have a question. Thank you for coming to Brookings. Thanks for talking about this. And shameless, plug we have a paper coming out on algorithmic bias shortly, so good to see you talk about that.

So legislation is normally put out there to reduce consumer harm, right? But given, and you said this, the nascent nature of this technology alongside what Darrell mentioned, the insufficient training data, there's been great studies at MIT around the recognition of darker-skinned hues when it comes to facial recognition data; and then the general broader conversation that we're talking about with AI around fairness, accuracy, and the long conversation around digital due process, would it be more appropriate to do more of a multi-stakeholder engagement process around this first before we push for legislation? So I'm just really curious about that because would we be kind of putting this out the cart before

the horse when we should maybe be bringing civil society, corporations, and others together to figure out those use cases?

MR. SMITH: Well, I would say a couple of things. First, I think that the art of legislation is by definition a multi-stakeholder process. Legislation doesn't get passed, certainly in the United States or in Europe or other places, without multi-stakeholder engagement. So the real question is not whether one should pass a law without multi-stakeholder engagement, but whether we can move both of these things forward at the same time.

And from our vantage point, we think that the market can work well if it's well-informed. If there's a level of transparency and if there is this ability for third party testing in an appropriate way.

And so, look, this isn't the world's biggest, heaviest cart that we're trying to build here. That would be one of the points I would make. I think that if anything, others will say we need a bigger cart. And so we would say, well, let's start with a few carts that are reasonably sized for the circumstances and then we can continue to learn.

I am by no means here to say that this is the one and only law that anyone's ever going to need to pass. But I do believe that if this law is passed soon, then we may solve some of these problems more quickly and then we'll all be much better informed in the context of multi-stakeholder engagement, to then think about and talk together about what might come next.

MR. WEST: Thank you. There's a question over here, the gentleman on the end.

SPEAKER: Thank you so much for the great presentation. You spoke at length today about the need to prevent states from abusing facial recognition technology. In

the past you've also spoken and written quite thoughtfully about why the technology sector needs to engage more with the Pentagon and U.S. military. I was wondering if you could share some of your thoughts on how facial recognition technology might be used by the military or should be. Is that a separate sphere or do your six principles still apply there?

MR. SMITH: It's a really good question. And I guess the first thing I would say is we're all learning and certainly we are continuing to learn. You know, certainly there are scenarios where one could deploy facial recognition in military use. Certainly when you think about aircraft, whether they're piloted or whether they're drones and they're piloted by people on the ground, people are trying to identify certain individuals at times, say terrorists and the like.

And would certainly say that these kinds of principles deserve some very serious attention and need to be addressed. You certainly don't want to make decisions that are inaccurate based on misidentification or bias. And I don't think that as a society we're broadly comfortable in that kind of scenario. For example, letting machines make these decisions. So this whole notion of meaningful human review is really of vital importance.

And so in the tech sector there have been some well-publicized situations where employees have expressed concern about the use of artificial intelligence by the militaries of the world. And one of the things I find in listening to our employees is that it's good to listen to our employees. It doesn't mean that we see the decision-making.

I mean, you know, we obviously made a very different decision from Google when it came to artificial intelligence in the military, but we didn't say one thing, we said two. And so far no other tech company has said these two things or said them together. We said we will make our technology, including artificial intelligence, available to the United States military, but we will engage not just actively, but proactively as citizens to address these

issues, to talk them through, to advocate for appropriate laws.

And I think we're learning a lot, even though it's really very early days. I think we're learning that we all have to figure out what the issues are. I find especially when you put AI together with military scenarios the first thing we have to do is identify all the questions, and I don't think we have yet. I mean, when we published the blog I wrote in July, we at least were able to say here are seven or eight questions. And I feel like we're still assembling the questions societally in this space.

I also think that the United States military has this incredible tradition of thinking deeply about ethics. And I find it really interesting that you cannot graduate from West Point or Annapolis, for example, without taking a course in ethics. But unless you attend Georgia Tech, you can get a degree in computer science from one of the 10 leading universities in this country in this field without having to take a course of ethics.

So I actually think it's a moment when we should recognize that we in the technology sphere have new questions to bring to, say, the military and we have things that we can learn together. And I, frankly, think and I hope that a decade from now the computer science departments of the universities of this country will have an ethics in artificial intelligence or an ethics in computing course as a required course for the computer and data scientists of tomorrow.

So, yeah, I would say more than anything we have a lot of work to do and we're going to do our best work if we do it together and in a way where we get to listen to and learn from each other.

MR. WEST: Okay, I think we have time for one more question. There's a lady right here, if you can bring the microphone over to her. We'll give you the last question, so it has to be a really, really good question. (Laughter)

MS. WONG: Thank you so much. Katie Wong with NTDTV. My question is about China. Because we know nowadays China is actively using this artificial intelligence in society surveillance and repression. And as you are also operating in this market how can you protect your own customers' privacy and apply these principles that you have mentioned about? And also, how to protect your technology from being used by or stolen or forced to be used by those totalitarian regimes? Thank you.

MR. SMITH: Let me say two things. First I'll answer a question without talking about China, per se, and then I'll talk about China, per se.

The truth is we look around the world and one of our six principles is about where we're comfortable having our technology deployed by the state, by governments, and that's a global principle. And there are, without naming any specifics, there are definitely countries where we are and will not be comfortable providing our artificial intelligence technology to governments, especially for uses where they could be, for example, put to work for ongoing or mass surveillance or other scenarios where we believe people's human rights would be at risk. And there's work that we've turned down, there are deals that we've turned down in some parts of the world where governments have wanted to license our technology and we just were not comfortable that it would be deployed in a way that would protect people's human rights. So we'll continue to apply that principle on a global basis.

And, look, we should keep in mind there are days when people have concerns about the protection of human rights or civil liberties here in the United States, too. So no single country has a monopoly on either end of this spectrum. This is something we need to think about quite thoughtfully and globally.

And then I do think that there is a global conversation that is going to need to be had. Artificial intelligence technology is not the repository of a single company or a

single country. I think people generally perceive that there are certain countries that are in a stronger leadership position. The United States, I would say and I think most people would say, is in the leadership position. And I think most people would say and I would say that China is in a very impressive position, as well, number two.

And when we think about ethical issues for artificial intelligence we need to find our way to a global discussion. Now, I don't say that with any naïve sense that this is the easiest issue for people around the world to sit down and come to an agreement, but it needs to be on the table. It needs to be part of the conversation.

And I think especially when we look at the governments and the consumers of Europe or Canada or Japan or South Korea, Australia, New Zealand, Singapore, many other places, I think they're going to be watching. And I think that's a good thing. I believe that if we can pursue a responsible path and we can take a path that really commits to protect people and people know it, then they can choose. And I believe that the people of Europe and Canada and these other places are going to want to choose technology that comes from companies that have high standards of protection for people.

So I welcome that kind of conversation and I also respect that there are rich philosophical traditions all around the world and we need to really engage with each other to talk these through.

MR. WEST: Brad, thank you very much. Lots for all of us to think about. So please join me in thanking Brad.

MR. SMITH: Thank you. Thanks for coming. (Applause)

* * * * *

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