THE BROOKINGS INSTITUTION

FALK AUDITORIUM

HOW TO BUILD GUARDRAILS FOR FACIAL RECOGNITION TECHNOLOGY

Washington, D.C.

Thursday, December 5, 2019

PARTICIPANTS:

Remarks:

THE HONORABLE CHRIS COONS (D-DE)
United States Senate

THE HONORABLE MIKE LEE (D-UT)
United States Senate

Moderators:

NICOL TURNER LEE
Fellow, Center for Technology Innovation
The Brookings Institution

DARRELL M. WEST
Vice President and Founding Director, Center for Technology Innovation
The Brookings Institution

* * * * *

P R O C E E D I N G S

MR. WEST: Good morning. I'm 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 our forum on facial recognition.

So software that identifies faces is being used in airports, retail establishments, and by law enforcement. It's raised many questions about privacy, surveillance, and bias. And some cities already have enacted limits or outright bans on the use of facial recognition by local law enforcement. Others believe that bans go too far and are thinking instead about how to enact guardrails in order to protect people's privacy.

So today, we are honored to welcome two senators to Brookings who will introduce the bipartisan Facial Recognition Technology Warrant Act. That bill requires federal law enforcement to get a court order before using facial recognition on targeted ongoing public surveillance of individuals.

Senator Chris Coons is a Democrat who represents Delaware, and he was elected to the Senate in 2010. He serves on the Senate Appropriations, Foreign Relations, and Judiciary, among other committees. He's been a leader in expanding access to technical training and higher education. He's a co-founder of the Senate Law Enforcement Caucus. When he was in Delaware, he served for the second largest law enforcement agency within the state. And he's been a long-time proponent of figuring out how to protect civil liberties during the digital era in which we live.

Senator Mike Lee is a Republican who represents Utah. He also was elected in 2010. He serves on Senate Judiciary, Commerce, and Energy and Natural Resources, among other committees. And he has been a leader on issues concerning economic prosperity, fiscal responsibility, personal liberty, and digital issues.

Each of them are going to outline their thoughts on facial recognition and the latest legislation they have introduced. And then Nicol Turner Lee and I will have some questions for them.

So we will start with Senator Coons.

SENATOR COONS: I note the rousing applause. (Laughter and applause) Good morning, everybody. Welcome to Brookings. What a gorgeous day to have a conversation about technology, civil liberties, civil rights, and public safety. I'm Senator Chris Coons from Delaware, and I am

honored to be joined by my friend and colleague Senator Mike Lee of Utah.

Thank you, Darrell, for that introduction. And thank you to Brookings for hosting, and to Dr. Nicol Turner Lee for moderating, and to Leti Davalos and the Center for Technology and Innovation here at Brookings for helping facilitate today's conversation.

As we all know, technology is accelerating in its ability to gather data about us everywhere all the time, in some of the most intrusive ways possible. I am literally, willfully, willingly I should say carrying with me a device that is essential to daily life. And I can, frankly, barely navigate driving around town or communicating with my family or staying in touch with my office or shopping without this thing. But it is also carrying a real-time tracking and monitoring device, a listening device, a device that sends data really every second of every day about exactly where I am, what floor I am on in a building, what building I'm at, how fast I'm going, where I parked my car.

And we all know this, but it is worth refocusing for a moment on the fact that the United States and our history as a constitutional republic, as a society that has chosen to order itself according to some core principles has long had to strike a balance between civil liberties and public safety. And while these advances in ways I just described are making our lives remarkably easier, it's also critical that we understand the real costs that come with these increases in advances in technology.

Today we're focusing on one of those new technologies: facial recognition. And we're having conversations in Congress about how a federal framework can help start this conversation and possibly strike the right balance between public safety, efficiency, privacy, and our constitutional rights. This conversation about facial recognition I think is long overdue.

Facial recognition is a valuable tool for law enforcement. It helps keep us safe. The ability to quickly deploy facial recognition software has the potential in a wide range of cases. Obviously, in the case of a terrorist who's just bombed a major public event, like the Boston Marathon. The ability to track them and apprehend them quickly is a critical tool in the toolkit for federal law enforcement.

The ability to find someone with Alzheimer's who has wandered away from their family and from a care-giving situation. The ability to quickly identify a child who is believed to have been kidnapped and be at risk of being exploited. There are positive use cases for facial recognition technology.

But if left unregulated, facial recognition technology also has the potential to invade the everyday privacy of literally every American, every person in this nation. The ability to be tracked or identified without your knowledge or consent in public at any point, at any time, I think creates obvious and significant Fourth Amendment concerns.

Problems with the accuracy and bias inherent in this technology also creates significant civil rights concerns. So we have to have rules in place that strike the right balance between civil liberties and civil rights and public safety. Right now that conversation mostly revolves around two poles: either law enforcement can use this rapidly emerging technology that is very forceful in any way they choose, any time they choose, or it has to be completely banned.

So far, a few municipalities have enacted bans. There's just the beginnings of a conversation by one presidential candidate about a complete federal ban. But somewhere between these two poles of a wild West where this powerful technology's unregulated and one where it's completely banned has to be a meaningful conversation.

So my bill with Senator Lee suggests how to set rules around one particular application of facial recognition technology when federal law enforcement uses it to surveil a particular individual over time. Targeted, persistent tracking creates significant Fourth Amendment concerns and can run up against our legitimate expectations of privacy.

So our bill would make it so that federal Law enforcement can't use facial recognition technology to conduct individually targeted surveillance without first showing probable cause. This is a commonsense approach that sets procedural guardrails similar to those set in other cases of intrusive searches by law enforcement. So here's the bottom line: our bill is the beginning of a conversation.

You may know that we both serve on the Senate Judiciary Committee together. You may have the general impression that there's not much going on the Senate Judiciary Committee except fighting over nominations and some other important thing that's going on in the House that's about to take up a whole lot of our time and energy. I cannot tell you how grateful I am to have a colleague who is willing to look past some of our deep current partisan divides and recognize that this is a significant challenge facing our nation and, frankly, our world.

The other major committee on which I serve is Foreign Relations. And I'll tell you as

someone who led a congressional delegation to China, Taiwan, Japan, South Korea earlier this year and who has spent a lot of time on the continent of Africa, I am struck at how quickly the capabilities of digital surveillance and of the control of populations is spreading throughout the world.

And I think it is critical that the United States demonstrate what is possible in a constitutionally ordered republic that is committed to the balance between civil liberties and civil rights and public safety, to show the world it is possible to deploy these rapidly emerging technologies in a way that still protects space for individuals to live their lives and to express themselves in ways that protect individual liberty and freedom.

I look forward to continuing to work with members of law enforcement, with civil rights and privacy advocates, and with industry to get this right. And more than anything, I look forward to working with my friend and colleague, Senator Lee.

Thank you very much. Let me turn it over to the senator. (Applause)

SENATOR LEE: Thank you very much. It really is an honor and a privilege to be here at Brookings, especially with my friend Chris Coons. Chris is someone who I deeply enjoyed working with over the nine years that he and I have served in the Senate. He's someone who enjoys and commands an enormous amount of respect along every end of the political spectrum and is one of the most well-liked and beloved members of the United States Senate by Republicans and Democrats alike.

When Senator Coons and I first started working on this legislation we decided that it was important to find a reasonable approach to balancing the interests that we have at stake here, the obvious civil liberties concerns that Americans have, and that it provides to law enforcement is a very significant thing. It's something that we shouldn't ignore.

We always have to recognize that as technology advances, as it makes government more efficient, that can be a good thing. At the same time as that happens, as government becomes more efficient, potential for abuse escalates dramatically.

I sometimes look for simple analogies from popular culture to remind me of why I want certain types of reforms in government. One of the best analogies that I can think of in some of these areas dealing with civil liberties is, of course, the Stay Puft Marshmallow Man from the original *Ghostbusters* movie. (Laughter) If you remember --

SPEAKER: How could you not?

SENATOR LEE: Yeah, yeah, exactly. How could you not think of that? If you remember at the end of the movie they're told by this deceased demon demagogue don't think of anything because whatever you think of right now is going to result because of some kind of curse and that thing becoming large and destructive. And they all said, okay, we're not going to think of anything. And apparently, one of the Ghostbusters thought of the Stay Puft Marshmallow Man, who by the time they noticed it coming was the size of a skyscraper and was stepping on houses, automobiles, churches, everything in its way.

This is, in some ways, reminiscent of the risks associated with our individual liberties and government when government grows big, when government becomes destructive of our liberties. It isn't always that the government itself hates us or that it's bent on doing evil, at least not in our country, at least not all of the time. Sometimes that is the case, but sometimes it isn't. Sometimes it's just because he's the Stay Puft Marshmallow Man and he's as big as a skyscraper and he's clumsy and your house or your automobile or your church or your synagogue or mosque happens to be in the way. This is one of those areas where I think we run into some risk there.

Well, many of us might prefer a moratorium on the use of facial recognition without a warrant. We think this legislation that we've developed comes a long way in protecting American civil liberties and providing clear guidelines to law enforcement where none current exist.

So this is a big area. It's one that we realized we can't conquer in one fell swoop, but we think this bill goes a long way. It's a positive step in the right direction.

While federal, state, and local governments have many different uses, different legitimate users, for facial recognition technology, this legislation narrowly targets just the use of facial recognition technology for targeted, ongoing surveillance conducted over a period of 72 hours. Due to the many uses of facial recognition technology we decided to focus this bill on only that type of targeted, ongoing surveillance, meaning for more than 72 hours, because we feel that it raises Fourth Amendment interests comparable to those that were at issue in both the *Jones* case and the *Carpenter* case.

Unfortunately, in both *Jones* and *Carpenter*, the Court declined to formulate a bright-line rule regarding the precise point at which tracking becomes a search. Nonetheless, there are some clues that we can take from both *Jones* and *Carpenter*.

For example, in the Supreme Court's 2012 ruling in *United States v. Jones*, we had a case that involved the use of GPS tracking to monitor the movements of a car over a period of 28 days. And the Court analyzed this surveillance under the reasonable expectation of privacy test.

In concluding that this surveillance violated the Fourth Amendment, Justice Alito's concurring opinion explained that the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses society's expectation has been that law enforcement agents and others would not and, indeed, in the main, simply could not secretly monitor and catalogue every single movement of an individual's car for a very long period.

In this case for four weeks law enforcement agents tracked every movement that the respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search for the line was surely crossed long before the four-week mark. So Justice Alito's concurring opinion doesn't say that there wasn't a breach prior to that. But he's saying certainly at some point prior to the end of that four weeks it was crossed.

In *Carpenter v. United States*, in a case cited just last year, well, the Court found that the government's access to 127 days of cell-site location information obtained from a wireless carrier without a warrant violated the individual's reasonable expectation of privacy. The Court failed to create a bright-line rule of how many hours' worth of cellphone site location information is sufficiently intrusive to intrude on the person's reasonable expectation of privacy.

Due to the fact that facial recognition technology relies on the use of cameras in public places, it may in some ways, due to the fact that it operates in public, not present exactly the same type or in some cases the same degree of invasiveness or the same type of comprehensive picture of a person's life as does cell-site location or GPS data. Nevertheless, we believe that this does present its own type of invasiveness. In some ways it's not as bad in the sense that, in theory, once you go in your home there, let's all hope and pray, will not be cameras, public cameras monitoring your every move within your home.

On the other hand, it can also be more invasive in the sense that they can tell your facial expression, something about your mood, something about what you're wearing, what you're holding, what you're eating that the GPS and cell-site location data can't. And so they present comparable but

substantively different risks, both significant risks to our individual liberties.

So our goals with this legislation were to protect Americans' reasonable expectation of privacy in this area with regard to facial recognition. Providing a clear standard, at least one of what will eventually become many clear standards, for federal law enforcement for circumstances where they must seek a warrant if they want to use FRT.

Our decision to focus on ongoing surveillance does not mean that we don't have any concerns with other uses of facial recognition technology. Quite to the contrary. We've both joined Senate Homeland Security and Government Affairs Chairman and Ranking Member, the Chairman Senator Johnson and the Ranking Member Senator Peters, in a letter to both the Department of Homeland Security and the FBI requesting information regarding their request to check photographs against driver's license databases within several states, including my state of Utah. We simply do not believe that a single one-size-fits-all approach to facial recognition would be effective.

More to the point, we know that this is a place where we can start. And if we can start cabining off piece by piece areas where government should not act and where it could and inevitably would invade our civil liberties, we can start there and that's what we're doing. Thank you. (Applause)

MR. WEST: Okay, I want to thank you for sharing your views. I want to commend you for thinking about how to impose guardrails on what Senator Coons called the wild West of facial recognition, which apparently has very few restrictions right now.

And obviously, also, we want to encourage and applaud the bipartisan spirit represented here, and we need more of that here in D.C.

So the bill that you have introduced kind of stands in contrasts to outright bans and kind of thinking about what are conditions under which we can use facial recognition. And I think one of the interesting features of this is the court order aspect of this. And there are several conditions attached to the use of the court order in terms of needing a warrant in cases of ongoing surveillance exceeding 72 hours, limiting the warrants to a maximum of 30 days, but then allowing facial recognition without a court order in circumstances requiring immediate action.

So I'd like to ask each of you just your thinking on how you decided on those particular conditions and how you reached the 72-hour limit, the 30-day limit. Either one of you.

SENATOR COONS: I'll offer up my thanks to my very capable counsel, Andy and Aaron, who negotiated a lot of the back-and-forth with Senator Lee and his staff.

If you want to know exactly how we got to 72 versus 48 versus -- right, I mean, this is, frankly, an attempt at starting a conversation. Somewhere between you can't use facial recognition technology without a probable cause warrant at all and you can use it for an unlimited period of time. We had to sort of strike a reasonable balance that we thought was an opening position.

I think the idea that the warrants last 30 days or are renewable for 30 days and that it's for 72 hours, by the way, going forward or going backwards, is an intriguing way to sort of put down a marker and say we don't want to prevent all use of this technology, but we want there to be guardrails.

MR. WEST: Senator Lee?

SENATOR LEE: One of my favorite law professors was a guy named Fred Gedicks. He taught me torts and constitutional law later in my law school career. I remember during our first year of torts class asking him a question about how you tell, how you can figure out the moment at which someone has deviated from the standard of care such that they've committed a negligent tort. And he said seven. (Laughter) What do you mean? He said when there is a difficult line to be drawn in the law, when the legal standard requires you make a determination, you draw the line at seven. I said, okay, well, that's very helpful, thank you. (Laughter)

SENATOR COONS: And clearly, we apply that here because it's actually a 72-hour.

SENATOR LEE: Yeah, we just added a two. (Laughter) We added a two and it worked.

SENATOR COONS: It's funny, my con law professor said three. I said what do you mean? He said it's always got to be a three-prong test. Right? (Laughter) If it's (inaudible), whatever it is, we have to have a three-prong test.

MR. WEST: So I want to introduce my colleague Nicol Turner Lee. She is a fellow in our Center for Technology Innovation. She works on issues of digital technology, AI, and privacy, and she's writing a book about digital disparities. So you have a question, as well.

MS. TURNER LEE: Yeah, thank you, Darrell, for that shameless plug. And Senator Lee almost sat in my seat. (Laughter) So we know the Lee affiliation is real.

I actually want to ask a question on the bill and then I have another question hopefully

we'll get to on the technology itself. So there is a copy out on the bill around sort of this time stamp when it comes to surveillance. I'm curious, given that we've had conversations on privacy, the extent to which when we say that the surveillance is sort of completed, that the data is either deleted or, you know, is not sort of archived in ways that can go back to those subjects and sort of redo this process. Because I think that's been some of the concern in terms of data minimization. Right? What happens when somebody is originally surveilled?

And I think the concern about facial recognition technology is our faces really don't change. Right? And if they don't change, it's a really good indicator for law enforcement that we're probably that person.

So just curious in terms of your thinking around, you know, data deletion, privacy. You know, where do we sit when that surveillance period window shuts? And how do we handle that with care?

SENATOR COONS: I've just looked at some pictures of me when I was first elected, I wish it were true that our faces don't change. (Laughter) Ten years in Washington and my face has changed. But I take your point.

One of the things we have engaged in a vigorous and sustained debate in Congress about is the application of the PATRIOT Act and some of the accumulated -- and this is around typically meta data, around email communications, but when there is the technical capability to accumulate literally vast, almost unlimited bodies of data and then to query it over and over, over a long period of time, you're right that we can have cumulative errors in terms of misidentification based on poor use cases or where the technology doesn't advance.

One argument I think against a complete and total ban on facial recognition technology, first, is that it's advancing rapidly in other parts of the world, and second is that it won't get better. Part of what we tried to do in this bill is to direct federal agencies to partner with NIST in order to improve the quality and reduce the discriminatory or the unequal impacts of facial recognition technology.

And I do think coming up with an approach to data minimization so that there doesn't end up being this vast body of nationally accumulated data is an importance piece of striking the right balance between civil liberties and public safety.

A key difference between the United States and some other countries where facial recognition technology is rapidly advancing is that we don't have a sort of backend integration between every time you into a Wawa to buy a coffee, every time you go through a toll booth and pay a toll, and every time you get your picture taken coming into a building, those are not all, currently, in one unified backend database. In other countries they are.

MS. TURNER LEE: That's right.

SENATOR COONS: And the consequences in terms of continuous surveillance in all aspects of your life are daunting and I think we need to make sure that we're doing the right thing in terms of minimizing the potential for that happening here.

SENATOR LEE: One of the things that keeps governments in check, in theory, has always been the availability of limited resources. And so one of the problems that we had at around the time of the American Revolution was that in the words of the Declaration of Independence, the king had sent forth vast swarms of officers to collect taxes and otherwise impose regulations that were designed to promote the interest of the crown and to help pay for wars and things like that. And so our people felt overwhelmed because, all of a sudden, the capacity of the crown within the American colonies was significantly greater than it had been. And the intrusiveness into their daily lives was significantly enhanced.

There's something of an analogy here. I don't want to make too much of a stretch of it, but when we acquire the ability to collect and store a whole lot of data and then to automate our access to that data, if we don't have guardrails around it, it'll have sort of the same effect of a big force change where, all of a sudden, the government, much like Colonial America pre-Revolution, all of a sudden, the government had a lot more ability and reach into peering into things that are none of the government's business. And so that's why we've got to put some guardrails around things like this that can otherwise tell a whole lot about you. It's none of their darn business.

MS. TURNER LEE: That's right.

MR. WEST: So I have a question about the possible biases of facial recognition. So there's been evidence of racial biases, gender biases, and other types of things. And as a result of that, some people have suggested that we should suspend deployment, have a moratorium until the accuracy

levels increase and that the racial disparities drop. Others, and your bill falls in this category, suggest that we should move ahead with deployment, but then you propose to work closely with NIST to establish testing systems regarding accuracy.

So why that approach as opposed to the moratorium?

SENATOR LEE: By requiring testing and by working with NIST and requiring regular reporting on this, we think we can work the kinks out in the system. Some of the biases inherent in the system relate to just inadequate data built up already. And we think that by allowing it to be deployed, but requiring systematic reporting and reporting to Congress, we can work out the bugs in the system. We're told that it is relatively easy to do. It's just that with the relatively small pool of data available to them in some areas, they haven't yet figured out how to make it more accurate, but that's coming.

SENATOR COONS: Well, two things, if I might just add. NIST is the National Institute for Standards and Technology, one of the most significant and little known and underappreciated federal agencies that does important scientific research across an incredibly broad range of areas, including cybersecurity. Part of the challenge I think, Mike, is that the data pools they've been drawing from overwhelmingly rely on photo arrays of people who are incarcerated. And there need to be both broader data used and much more careful attention to the ways in which existing biases in our society and our criminal justice system are being compounded by the early stage deployment of facial recognition technology here.

If I could, just to expand on a comment Senator Lee made a moment ago. In the Colonial era, part of that searching power of the king was quartering troops in Americans' homes. That's why we have a Third Amendment. And part of what this makes possible -- and by "this" I'm not pointing to my butt, I'm pointing to my cellphone in my back pocket, forgive me. (Laughter) I'll continue to wave the example as that struck me as a very odd gesture even as I was doing it. Part of what this makes possible for the very first time is literally the equivalent of the quartering of federal troops in our homes.

If you think about all the previous cases, right, *Olmstead*, where I think it was Justice Brandeis said a fairly famous dissent, was the wiretapping case from the 1920s, when, right, the federal government was confronting national organized crime and the result of Prohibition and using wiretaps for the first time. He had a fairly forward-looking dissent about how technology can advance in ways that we

couldn't foresee and can engage the forces of government in searching intrusions.

That was about, you know, federal agents being able to listen in on your telephone calls. But you can only have someone listening in on a telephone call when you picked up the phone and made a call, which at that time was relatively rare. I don't think that was overturned until *Katz* in 1967.

These things aren't just telephones that track us and monitor us and engage us when we choose to use them. As a number of bipartisan letters that several groups of senators have sent to Google and others I think are increasingly demonstrating, our vehicles have continuous tracking and monitoring in them; it's not just Alexa, it's your smart TV; and with the Internet of Things, it is very soon going to be almost literally everything in your house is gathering data about you all the time.

This is the first time since the Colonial era that you've literally got the equivalent of troops quartered in homes in a way that sort of breaks that most fundamental American sense of what it means to be secure in our papers and effects.

MS. TURNER LEE: Yeah. So I'd like to follow up on that and put out a shameless plug, too. Here at Brookings we do work on AI and one of the areas that we're looking at is this sort of fragmentation of datasets. So we actually have some proposals around, you know, how do you create more robust datasets that assist in anti-bias experimentation? So there's NIST, there's the National Science Foundation, but we got to do a better job I think overall.

But I do want to, and before we run out of time, sort of speak to this idea of surveillance. Right? If we go pre-Colonial, there's a history of, you know, not having all these tools that we have today. But surveillance also means for law enforcement, or could mean, that it goes beyond just criminal intent to civil society participation. We saw that in China, you know, with the use of facial recognition technology to arrest protesters.

I guess the question I have is we look at this bill as sort of this first step to frame this conversation on guardrails for law enforcement, federal law enforcement, in fact. What does that mean in terms of the nature of surveillance of people who are not basically maybe being criminally intentional, but people who are protesting for rights or freedoms or, you know, groups like Black Lives Matter and others who may be surveilled for other reasons outside of the criminal intent? How will the bill in some respects sort of protect their civil liberties to expression?

SENATOR LEE: That's a great point and I think that is an added feature of this bill is that if you can't have ongoing continuous surveillance of a person without a warrant, then you're not going to have this temptation to just sort of randomly collect or maliciously collect information about somebody. Let's see what Bob's doing today, you know. That's not going to happen. They're going to have to discard that regularly.

I remember a few years ago, when I was working for our governor back in Utah, one day I got to go back into the control room and see where they controlled the security cameras within our state capitol building. And we turned it around, I found one of my friends, I would focus it on him for a minute just to mess with him. I followed the camera with him out there. And all of a sudden, I thought, you know, that's kind of creepy.

MS. TURNER LEE: Creepy.

SENATOR COONS: It's weird. This is deeply creepy

SENATOR LEE: That's really creepy. If you could do that and if you could do that with a degree of automation, with the AI tools available for scanning your face over a period of time, even if you didn't start out with the assumption I'm looking for a crime or I'm watching a crime in process, that is in some ways the worst thing that we can imagine, and that's what this prohibits, too.

SENATOR COONS: And the reality is there are countries around the world right now that are using this type of technology to harass, to interfere with, or to arrest human rights activists, journalists, minority party politicians. I've been to a half-dozen countries where this isn't just a matter now of the government turns the Internet off when there's a protest or a riot in the capital. They're literally tracking daily the movements of people who speak out against their government or speak up for environment interests or concerns or civil liberties or civil rights.

And I wish we could say with a straight face that the United States has no history of that kind of -- but, boy, you'd have to be blind to our own history to suggest that the tools of federal law enforcement have never been used to surveil and interfere with our civil rights movement, our anti-war movement. Obviously, within living history that has happened. So we need to be mindful of that, the very real risk of it.

I will have a hard time getting out of my mind the picture of the Stay Puft Marshmallow

Man as the exemplar of, you know, sort of an overreaching federal government, but at least it tastes good, so. (Laughter)

I do think Senator Lee started us off with a helpful metaphor, which is that even though basically well-intentioned, even though positive in its initiation, in its initial conception, an overweening, overreaching, overly powerful government that can collect data on us all the time everywhere, anywhere, and that doesn't have guardrails in terms of how it's using that tool can initially begin trying to interdict and prevent crime or trying to prosecute crime, and can quickly bleed over into interfering with what I think is the most American right. I keep trying to suggest a reformulation of our First Amendment rights as the right to have an opinion, to have an enthusiasm, the right to be weird, the right to just engage in odd conversations and offbeat hobbies.

And if you can't go to a sporting event without being concerned that there's literally continuous surveillance of every single face in the crowd, and then face some searching response from law enforcement to your simple presence at a rock concert, at a speech, or a rally or at a sporting event, then we've lost in some ways what is I think the most fundamental thing that makes it worth being Americans, which is the right to have opinions, hobbies, interests, and associations.

MR. WEST: Actually, I thought you were talking about Brookings when you were talking about the right to be weird. (Laughter)

Let's take a quick question from the audience. There's a gentleman right here on the aisle. There's a microphone coming up from behind you. If you can give us your name and your organization.

MR. TUCKER: Thank you. Patrick Tucker with Defense One. Two quick questions for Senator Coons. I wonder if you could elaborate on your experiences abroad and if there was a specific example perhaps from China that led as the impetus for this legislation.

And for both of you, it seemed like there's a practical kind of gap that I'm not understanding in your legislation, which is that if I'm out in public I don't have an expectation of privacy in terms of my appearance. I can be photographed. And if that weren't the case, then we wouldn't be able to deploy police helicopters.

So does your legislation particularly take a look or regulate the accumulation of public

photographs? Does it regulate the application of machine learning algorithms to those photographs? Like which of those two things is a potential violation of my expectation of privacy? So thanks.

SENATOR COONS: Unless I mishear you, it's the intersection of the two. So it's really more federal law enforcement is engaging in intentional continuous surveillance of you using digital tools. So that really can be the combination of facial recognition technology, the accumulation of images, and then machine learning to track you. I mean, getting one image of you as you get into, you know, one government building's lobby isn't the core concern here. It's using facial recognition technology to track you and your movements and your associations and your activities over several days, first, and feel free to disagree.

Second, I think fairly obviously the reeducation camps of the Uyghurs in Western China and the press accounts of the extent to which the government in China is using facial recognition technology to monitor and control wide swaths of their population is one of several examples in other countries that I think raise profound concerns about civil liberties and civil rights.

SENATOR LEE: Like Senator Coons, I visited Ürümqi a few years ago in Western China, and I saw the kind of surveillance state that's there. I mean, there is a significant surveillance state in China generally. It's particularly pronounced in the areas where a lot of Uyghurs live, and that is of deep concern.

But, yeah, I agree completely with Senator Coons' answer to your question. It's the intersection of the two and that's dangerous.

MR. WEST: Okay. Unfortunately, we are out of time, but I want to thank Senators Coons and Lee for sharing their thoughts and we look forward to continuing the conversation with you. And if you could just stay seated for a minute so they can get back to Capitol Hill, thank you. 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