This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

RPTR BRYANT

EDTR CRYSTAL

SAFEGUARDING DATA AND INNOVATION:

SETTING THE FOUNDATION FOR THE USE

OF ARTIFICIAL INTELLIGENCE

WEDNESDAY, OCTOBER 18, 2023

House of Representatives,

Subcommittee on Innovation, Data, and Commerce,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 10:03 a.m., in Room 2123, Rayburn House Office Building, Hon. Gus Bilirakis [chairman of the subcommittee] presiding.

Present: Representatives Bilirakis, Walberg, Bucshon, Duncan, Dunn, Lesko, Pence, Allen, Fulcher, Harshbarger, Cammack, Rodgers (ex officio), Schakowsky, Castor, Dingell, Kelly, Soto, Clarke, and Pallone (ex officio).

Also Present: Representatives Obernolte, Carter of Georgia, and Cardenas.

Staff Present: Kate Arey, Digital Director; Sarah Burke, Deputy Staff Director;

Michael Cameron, Professional Staff Member; Sydney Greene, Director of Operations; Jessica Herron, Clerk; Nate Hodson, Staff Director; Tara Hupman, Chief Counsel; Peter Kielty, General Counsel; Emily King, Member Services Director; Tom Kurth, Chief Counsel; Viswajith Mallampati, Intern; Carla Rafael, Senior Staff Assistant; Brannon Rains, Professional Staff Member; Teddy Tanzer, Senior Counsel; Joanne Thomas, Counsel; Dray Thorne, Director of Information Technology; Evan Viau, Professional Staff Member; Caitlin Wilson, Counsel; Hannah Anton, Minority Policy Analyst; Keegan Cardman, Minority Staff Assistant; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Daniel Greene, Minority Professional Staff Member; Tiffany Guarascio, Minority Staff Director; Cornell Harris, Minority Intern; Lisa Hone, Minority Chief Counsel, Innovation, Data, and Commerce; and Joe Orlando, Minority Junior Professional Staff Member.

Mr. Bilirakis. The subcommittee will come to order.

The chair recognizes himself for an opening statement.

Good morning, everyone. And thank you to all the witnesses for being here for this very important hearing.

For years Congress, and especially this committee, has been examining one form or another of artificial intelligence, whether it was exploring how social media companies develop their algorithms or looking at next-generation vehicles and how they will transform safety and mobility.

Central to these discussions has always been the need for America to lead in the development of standards and deployment and what AI means for our data.

We kicked off our subcommittee hearings this year with a focus on our competitiveness with China, where we learned why it is critical for America to lead the world in key emerging technologies and why it is imperative for Congress, as a first step, to enact data privacy and security law.

AI has so many different applications, from auto filling text messages or Excel spreadsheets all the way to generating unique images and speeches. But at the base of these applications is the need to collect and properly permission information to train and grow these AI models.

Without a data privacy and security standard that dictates the rules for how companies can collect, process, store, and transfer information, bad actors may have unfettered access to use and exploit our most sensitive information.

We have seen true innovators in this space using information they collect to help provide goods and services or improve what they are offering to users. For example, I

have heard of internet service providers using information they collect from their customers to build AI processes to better understand when an outage may occur and how to prevent it.

Additionally, in the healthcare sector, AI can unlock greater speeds to processing information on diagnostic imaging and screenings or discovering new possibilities within the drug development pipeline.

That being said, there are entities that don't have our best interests in mind when they collect, purchase, or disseminate our information. In several instances, this is done under the radar without the consumer ever knowing it happened.

We have seen how data collection practices have allowed data brokers to build profiles on Americans and sell them to any bidder or even giving them to foreign adversaries, unfortunately; or how we have seen Chinese companies, like TikTok, collect everything they need to build out their algorithms, which are blocked from leaving their own borders of China but used to push harmful content to our children here in the United States.

Earlier this year, we saw the horrible content TikTok has pushed to children, like self-harm and suicide encouragement, and now war crimes and terrorist content are being touted on the platform, unfortunately.

This committee examined issues like this last year when we passed comprehensive data privacy legislation out of committee almost unanimously, which included requirements for companies to conduct impact assessments on how their algorithms could be harmful to children. In fact, our legislation was touted as having the strongest online protections for children to date and overall would provide stronger protections than any State law.

Unfortunately, the current reality is millions of Americans have no protections or control when it comes to their sensitive information, and there are bad actors, as we know, and companies who will abuse this gap in protections to their own benefit.

Americans deserve more transparency around what companies do with their information, more control over how their information can be used, and better data security practices from the entities that use it.

I look forward to hearing from our witnesses on the importance of enacting a data privacy law and how that can set the United States up for success to lead the world in AI.

I thank all of you for being here today, and I look forward to your testimony.

I yield back.

And now I recognize the gentlelady, my friend from Illinois, Ms. Schakowsky, for 5 minutes for her opening statement. Thank you.

[The prepared statement of Mr. Bilirakis follows:]

******** COMMITTEE INSERT ********

Ms. Schakowsky. Thank you, Mr. Chairman.

And thank you to our witnesses for being here today.

I want to say that artificial intelligence, or AI, has transformed our lives, from healthcare to Hollywood, in so many ways. The fuel for AI is consumer data.

And in a way I feel like this is deja vu all over again. Here we are talking about how consumers feel afraid online.

And when we talk about AI today, most people really don't even know what we are talking about. And yet they may feel the impact in all kinds of negative ways.

Because of AI and algorithms, there may be people who are discriminated against, that people of color may not be able to get the healthcare that others are able to get.

We are aware of all kinds of experiences that people have had. And I wanted to give you another example.

There used to be -- well, there still is -- a scam that says -- you get a phone call that says: Your son is in deep trouble and you better send us some money in order to make sure that we take care of him. And people have, particularly older people, have fallen for that.

Now they can have your son's voice. All it would take is maybe 3 seconds to develop that voice, and you absolutely think that you better act immediately or your child is in danger.

And so AI presents all kinds of challenges to us.

On the other hand, of course there are advantages too. But we passed legislation. We passed a comprehensive consumer safety bill to protect people's data. Our bill passed the House -- passed not the House, unfortunately -- passed this full

committee almost unanimously to make sure that we protect consumer data. And we need to get back to that right away. And we need then to include in that AI.

As we know, States are moving ahead without us. There are now 13 States in the last year who have adopted data privacy legislation.

One of the things that we wanted to do was have something nationwide that would protect consumers. And I feel like we made such great progress in a bipartisan way in doing that. And we could move ahead now in adding AI to that as well, and we ought to get on it right now.

So I am really calling on all of us to be able to get back to being a Congress that can act, and when we do that data privacy is among the very first things that we do.

Data protection is something that we can do. People can be protected from scams. We can protect workers. We can protect businesses that also can become victims of AI.

And so my call today is let's get going. Let's get a Congress that can function. And when we do, let's move ahead on protecting consumers that are still finding that their most precious and private data -- and in our bill, Congressman Bilirakis, when we worked together, we did a lot for children as well and protecting children and the most vulnerable.

So I say let's get back to business and let's finally get it done across the finish line.

And with that, I yield back.

[The prepared statement of Ms. Schakowsky follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. The gentlelady yields back. I appreciate those comments.

I now recognize the chair of the full committee, my good friend, Mrs. Rodgers, for her 5 minutes for her opening statement.

The Chair. Good morning, everyone.

Yesterday, Congresswoman Debbie Lesko announced that she would not be seeking reelection. And I just would like to start by honoring her service.

Is she still here? Oh, yeah, there she is. Yes.

I wanted to begin by honoring her service to our Nation as well as her leadership on the House Energy and Commerce Committee.

I know that she is going to finish strong and we are going to have many more times where we can honor her. But I just wanted to recognize her and this decision and just let her know that we look forward to her finishing strong in the days ahead. But we are going to miss her in the next Congress.

Mrs. Lesko. Well, thank you, Chairwoman.

And you guys still have 15 months to put up with me. And I don't have to worry about reelection, so it might get wild. Who knows?

The Chair. The best is yet to come.

Well, welcome, everyone, to our series of AI hearings and the seventh data privacy-related hearing that we have held this year.

The promises of artificial intelligence are extensive, from more affordable energy and better healthcare to a more productive workforce and a better standard of living. Unlocking this technology's potential could radically strengthen American economic and technological leadership across the board.

In addition, the power of AI can also be abused and raises serious concerns and challenges that must be addressed. It is critical that America, not China, is the one addressing those challenges and leading in AI's development and deployment.

The best way to start is by laying the groundwork to protect people's information with a national data privacy standard. This is foundational, and it must be the first step towards a safe and prosperous AI future.

If used correctly, AI can be a source for good. It could help us unlock life-changing technologies, like self-driving vehicles and enhanced health diagnostic systems, enhanced protections against national security threats and data breaches, while assisting companies and law enforcement to better scan internet platforms for illegal activity, like child sexual abuse material and fentanyl distribution.

To unlock these benefits, though, we need to first establish foundational protections for the data that powers many of these new AI tools, and it is vital that it be led by the U.S.

Data is the lifeblood of artificial intelligence. These systems learn from processing vast amounts of data. And as we think about how to protect people's data privacy, we need to be considering first and foremost how the data is collected and how it is meant to be used and ensure that it is secured.

It is time that we provide people with greater transparency and put them back in control of the collection and the use of their personal information.

Key to this is ensuring the safety of algorithms used by online platforms, which serve as the instruction manuals for artificial intelligence.

By making sure algorithms are being developed, operated, and training AI responsibly, we can provide Americans with greater transparency for how their data is

analyzed, how these systems identify patterns, how they make predictions, and how their interactions with online platforms are used to determine what content they see.

Put simply, trustworthy algorithms are essential components in a responsible deployment of AI. Failing to enact a national data privacy standard or allowing China to lead the way heightens the risk over the collection and misuse of data, unauthorized access and transfers, and greater harms for Americans and our families.

We need to prioritize strengthening data security protections to safeguard people's information against threats. The theft and exploitation of sensitive information, especially biometric data, pose severe risk to individuals and organizations.

If we establish stronger data privacy protections for Americans without equally robust data security requirements along those rules on collection and use, the number of data breaches and abuses will continue to rise and compromise people's information.

Building those laws early would ensure greater public trust in AI, which will ensure future innovations are made in the U.S.

To ensure American leadership, we must strike the right balance with AI, one that gives businesses the flexibility to remain agile as they develop these cutting-edge technologies while also ensuring the responsible use of this technology.

A national standard for collection and handling of data will provide businesses, creators, and every American with clear and understandable protections wherever they are.

I look forward to discussing the path forward today, and I yield back.

[The prepared statement of The Chair follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. I thank the chair.

I now recognize my friend from New Jersey, the ranking member of the full committee, for his 5 minutes of an opening statement.

Mr. Pallone. Thank you, Chairman Bilirakis.

And I have to say that I also regret Debbie Lesko leaving. She is always smiling, pleasant, and tries to work in a bipartisan basis.

So maybe we can convince you to change your mind, but probably not.

To the issue of the hearing today, let me just say that despite what the chairwoman says, I am very concerned about what we can actually accomplish if this paralysis with the Speakership continues. It is now 16 days since the House has been paralyzed without a Speaker. We are 30 days away from another potential government shutdown.

This hearing comes at a time when House Republicans' dysfunction is hurting the American people, weakening our economy, and undermining our national security, in my opinion.

And all year, House Republicans have caved to the extreme elements in their party, who have no interest in governing. They have forced cuts to critical Federal programs in spite of a funding agreement between the former Speaker and President Biden, and they came close to a government shutdown that would have cost our national economy upwards of $13 billion a week and forced our troops to work without pay. And I just think the American people deserve better.

Democrats have repeatedly tried to stop this dysfunction from hurting everyday Americans, but it is long past time for House Republicans to reject the extremists in their

party. We should be working together to lower costs for American families and to grow our economy and the middle class, and it is time for the chaos to end.

Now, last year, now-Chair Rodgers and I were able to work across the aisle and pass the American Data Privacy and Protection Act out of the committee by a vote of 53 to 2. That legislation included many important provisions, including provisions focused on data minimization and algorithmic accountability.

Clearly defined rules are critical to protect consumers from existing harmful data collection practices and to safeguard them from the growing privacy threat that AI models pose.

And I strongly believe that the bedrock of any AI regulation must be privacy legislation that includes data minimization and algorithmic accountability principles. Simply continuing to provide consumers with only "notice and consent" rights is wholly insufficient in today's modern digital age.

Artificial intelligence is certainly not new. However, the speed at which we are witnessing the deployment of generative AI is staggering, and the effects it will have on our everyday lives are tremendous.

There has been an explosion of AI systems and tools that answer consumers' questions, draft documents, make hiring decisions, influence the way patients are diagnosed, and make employment and housing decisions.

Many of these systems are trained on massive amounts of data Big Tech has collected on all of us. And that is why the lack of nationwide protections around what data companies can collect, sell, and use to train these AI systems should concern every American.

Now, since sufficient guardrails do not exist for America's data and AI systems, we

are, unfortunately, hearing of a growing number of reports of harmful impacts from the use of AI systems. This has included the creation of deepfakes, leaking of personal data, and algorithmic-driven discrimination.

There have been instances where AI has been used to mimic real people's voices to convince consumers to send money to someone they think is a friend or relative. Chatbots have leaked medical records and personal information. And AI systems have discriminated against female candidates for jobs and people of color in the housing market.

This is all extremely concerning. We cannot continue to allow companies to develop and deploy systems that misuse and leak personal data and exacerbate discrimination. And that is why we must make sure developers are running every test they can to mitigate risk before their AI models are deployed.

Congress must also continue to encourage agencies like the FTC to enforce the laws they already have on the books. I commend the FTC for their work to fight scammers who have turned to new AI tools like the ones that mimic the voice of a friend or loved one in order to trick consumers out of their life savings. We must continue to fully fund these agencies as technology continues to advance and the threats to consumers continue to grow.

So I will also continue to push for a comprehensive national Federal privacy standard. It is the only way we can limit the aggressive and abusive data collection practices of Big Tech and data brokers, ensure that our children's sensitive information is protected online, protect against algorithmic bias, and put consumers back in control of their data.

So I look forward to the discussion today.

Mr. Chairman, I yield back the remainder of my time.

[The prepared statement of Mr. Pallone follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. I thank the gentleman.

First of all, I want to thank the witnesses for being here. And we are going to try to stick to that 5-minute rule. We are going to stick to the 5-minute rule, for obvious reasons. We will have a vote on the floor at approximately 11. That may change. But we are going to anticipate a vote at 11, and we will recess and come back. So I want to thank you in advance for your patience.

Our first witness is Raffi Krikorian, a good Armenian name, chief technology officer at the Emerson Collective.

You are recognized for 5 minutes.

STATEMENTS OF MR. RAFFI KRIKORIAN, CHIEF TECHNOLOGY OFFICER, EMERSON COLLECTIVE; MS. AMBA KAK, EXECUTIVE DIRECTOR, AI NOW INSTITUTE; MR. CLARK GREGG, ACTOR AND SCREENWRITER, SAG-AFTRA; THE HONORABLE VICTORIA ESPINEL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, BSA, THE SOFTWARE ALLIANCE; AND THE HONORABLE JON LEIBOWITZ, FORMER CHAIR AND COMMISSIONER, FEDERAL TRADE COMMISSION

STATEMENT OF RAFFI KRIKORIAN

Mr. Krikorian. Thank you, Subcommittee Chair Bilirakis, Subcommittee Ranking Member Schakowsky, Chair Rodgers and Ranking Member Pallone and members of the subcommittee. My name is Raffi Krikorian. I am the chief technology officer at Emerson Collective, and I appreciate the subcommittee's ongoing interest in protecting the digital privacy rights of Americans.

Personally, I have been fortunate to work in the tech industry for over 20 years. At Twitter, I was the vice president of engineering. At Uber, I was the director in charge of the self-driving car efforts.

And I now have the pleasure of working at Emerson Collective, where we recognize that complex societal problems require innovative solutions. We use a unique combination of tools -- philanthropy, venture investing, even arts and others -- to spur measurable and lasting change in a number of disciplines, including technology.

So I would like to start with a very simple fact. We live in an age of rapidly increasing digital surveillance, and very few users understand the tradeoffs they make

when they are using their phones or the web.

Not only are applications doing more with users' data than users expect, that usage is accelerating and evolving at an unprecedented speed, and within this regime notice and consent are failing us. By now, we are so used to seeing advisory pop-ups listing our consent to accept cookies that we are more annoyed by them instead of being informed by them.

So in order to move forward, I propose we need to step back and look at the heart of the problem.

First, the data economy is becoming incredibly complicated. It is increasingly difficult to explain to everyday consumers how their data is being collected and being used.

Amazon knows every product a user has ever viewed, how long they have dwelled on a specific page on their Kindle, as well as searches across all of Amazon's retail partners. And that is just Amazon. Users are generating lots and lots of data, and that data is being found in lots and lots of different places.

And don't get me wrong, users are generally delighted by these personalized experiences. But, again, I contend that users don't understand the tradeoffs that they are making for these experiences.

So a problem, though: The notion of data minimization comes in direct conflict with data-hungry artificial intelligence algorithms. Retailers and advertisers are gathering our personal data so they can make better predictions on how to sell us things.

But in the case of AI and deep learning models, more data is essential to make AI function at all. AI developers pride themselves on models that detect patterns that humans themselves will not be able to see. So, therefore, it behooves them to feed the

machine as much data as they possibly can.

Data collection is no longer just a sales tactic, it is an existential necessity. And for more problems, we are seeing technological trends that go beyond just capturing data via applications.

One trend I might call out is this notion of voluntary data surrender. Users are willingly sharing data about themselves all the time, unaware or unconcerned of whose hands it might fall into.

I am speaking about social media, of course, which along with the prevalence of cameras on our smartphones has caused an explosion of data that we put online. And one can argue that there might be no expectation of privacy in a public space, but I would contend that we are seeing 21st century technology in collision with 20th century norms and laws.

AI tools are being trained on these vast data links found in public spaces, and we are training them to do things like identify people from an image on any camera anywhere.

And these tools can do more than simply identify people, but they can mimic them as well. Today's hearing alone will generate enough samples of my voice that anyone will be able to make a convincing synthetic replica of me.

And I don't want to be alarmist. That is only one trend. I can obviously name more.

So notice and consent won't be able to mitigate any of this. So what do we do?

Well, first off, I believe we need increased efforts to promote and expand digital literacy, especially around the ideas of data and privacy. Users should better understand the data economy in which their personal information is being used and

traded within.

And we need to incentivize application developers to do a better job to explain to users up front what they are consenting to and how their data will be used.

After the initial consent process, users should have agency over how their information is flowing through a software application's companies, and end users need access to that full life cycle and have visibility into that full life cycle of their data.

They should be given clear ways to understand the tradeoff between what they have given away and what benefits or harms might come from them or their community, and that users should be able to both revoke consent and delete their data from the application if they so choose.

And these are just things we can do in a user-centric way, giving power and agency back to users. There is an entire other class of solutions I am happy to talk about around companies and application developers.

So I sincerely praise the bipartisan work this committee has done in its advancement of the American Data Privacy and Protection Act, and I believe that this should be treated as a foundation for more work going forward.

The problems that we can identify today are just that, the problems of today. There will almost certainly be new issues to tackle as these technologies continue to evolve, and setting up a legislative framework so that we can adapt quickly as these new issues appear is vitally important.

So I thank you for the opportunity to share my perspective here.

[The prepared statement of Mr. Krikorian follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. Thank you very much. I appreciate it.

Our next witness is Amba Kak, executive director of the AI Now Institute.

You are recognized for your 5 minutes. Thank you again.

STATEMENT OF AMBA KAK

Ms. Kak. Chair Bilirakis, Ranking Member Schakowsky, Chair Rodgers, and Ranking Member Pallone, as well as members of this committee, thank you for inviting me to appear before you. My name is Amba Kak, and I am the executive director of the AI Now Institute, and I have over a decade of experience in global technology policy.

I want to make one overarching point in today's testimony, and that is that we already have many of the regulatory tools we need to govern AI systems. Now is the time to extend what we have in pursuit of ensuring that our legal regime meets the moment.

Specifically, I encourage this committee to prioritize the passage of a data privacy law, like the ADPPA, and in particular its strong data minimization mandates, which have already received the resounding support of this committee.

In fact, this notion that we need to create new frameworks from scratch largely serves large industry players more than it does the rest of us. It serves to delay and to provide current actors with significant influence on both the scope and the direction of policymaking.

Data privacy law is a core mechanism that can help mitigate both the privacy, but also the competition implications of large-scale AI. And I will build to this argument making three specific points.

The first, that data privacy regulation is AI regulation.

Soon after the public release of chatGPT there were questions from the public on what data these models had been trained on, followed by panic when people began to

realize that chatGPT was sometimes leaking personal data accidentally.

This example was not a one-off. There are ongoing privacy and security challenges introduced by large language models, which both routinely and unpredictably produce highly sensitive and inaccurate outputs, including personal information.

Regulators in many parts of the world with strong data privacy laws moved very quickly. Italy even issued a temporary ban on chatGPT based on concerns that it was out of compliance. And this ban was lifted only after open AI provided an opt-out for users to prevent their conversations from being used for training data.

Here in the U.S., while enforcement agencies have and continue to do all they can with existing authorities, the lack of a Federal privacy law undoubtedly held us back from demanding accountability, particularly as panic began to spread.

And taking the ADPPA as an example, here are a few of the tools we would have had and would have to regulate AI.

First, we would have data minimization, which would mitigate the supercharged incentives to excessively hoover up data about users.

Second, we would have data rights, which could compel transparency into these largely opaque AI systems.

And finally, we would have civil rights provisions to boost what Federal agencies are already doing under existing laws to curb algorithmic discrimination.

My second point is that when regulating AI, privacy and competition goals must proceed in concert. They are two sides of the same coin.

As it stands today, there is no large-scale AI without Big Tech. Companies like Google, Microsoft, and Amazon dominate access to computational resources and other companies, as a rule, depend on them for this infrastructure.

This is closely related to their data advantage, which enables them to collect and store very large amounts of good quality data about millions of people through their vast market penetration. This data advantage can give models that are developed by Big Tech an edge over those developed without the benefit of such data.

Now, this push to build AI at larger and larger scale only increases the demand for the very same resources that these firms have accumulated and are best placed to consolidate. Any regulatory effort must also address this market reality.

Privacy and competition law are too often siloed from one another, leading to interventions that could easily compromise the objective of one issue over the other and which is why, to conclude, of all of these provisions we most strongly recommend legally binding data minimization rules that draw clear lines around collection, use, and retention.

Tech firms already have very strong incentives for irresponsible data surveillance, but AI pours gasoline on them, fueling a race to the bottom.

Data minimization acts as a systemic antidote that addresses both first-party data surveillance as well as the consolidation off the existing data advantage in Big Tech.

The FTC recently penalized Amazon for storing children's voice data, and Amazon justified this by saying that they would be using it to improve their Alexa algorithm. We can't let these practices continue.

In conclusion, it is worth underscoring that there is nothing about the current trajectory of AI that is inevitable and, as a democracy, the U.S. has the opportunity to take global leadership here in setting a trajectory for innovation that respects privacy and upholds competition. Data minimization would be a major step forward on both counts.

Thank you.

[The prepared statement of Ms. Kak follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. We appreciate it very much, and thanks for sticking to the 5 minutes.

Now I will recognize Clark Gregg, who is an actor -- by the way, I am a fan -- and a screenwriter at the Screen Actors Guild-American Federation of Television and Radio Artists.

You are recognized, sir, for your 5 minutes.

STATEMENT OF CLARK GREGG

Mr. Gregg. Thank you very much.

Thank you, Chairman Bilirakis, Ranking Member Schakowsky, Chair Rodgers, and Ranking Member Pallone. For me, it is a great honor to appear before this important committee.

My name is Clark Gregg. As you said, I am an actor. I am a screenwriter. I am a proud member of SAG-AFTRA and of the Writers Guild.

Some of you might remember me as Agent Phil Coulson in the Marvel Cinematic Universe. In that role, my character had access to advanced and even alien technology that worked through biometrics. But that futuristic comic book tech has already become a reality.

Data privacy issues affect everyone. Given that more and more of our data is protected by biometric technology, it is critical that we protect data, such as voiceprints, facial mapping, even personally identifying physical movements. We strongly support the committee's work to construct national data privacy and security protections so that our personal information cannot be used without our consent.

I am here because this issue has been top of mind this year for my fellow writers and SAG-AFTRA members, actors, broadcasters, recording artists. We are currently in a fight to protect personal information such as voice, likeness, and audiovisual material online.

Actors, like anyone else, deserve to have their biometric information protected from unauthorized access and use.

Our voices, images, and performances are presently available on the internet, both legally and illegally. Because we do not have data and privacy and security protections across the Nation, AI models can ingest, reproduce, and modify them at will without consideration, compensation, or consent for the artists.

That is a violation of privacy rights, but it is also a violation of our ability to compete fairly in the employment marketplace. And these fakes are deceptively presented to viewers as if those performances are real.

Like any performer in a Marvel or any visual effects-driven film, I have been scanned. I have been scanned many times. You step into a tiny dome where there are literally hundreds of cameras. They record every detail and angle of you and they create something called a digital double, which scared me 10 years ago. It really scares me now.

This can be used with your voice, either real or synthesized, to recreate your character, to create a new character, or in the wrong hands, ironically, as you said, Chairman Bilirakis, a bad actor. It can create a new you that can roam the internet wreaking havoc in perpetuity.

Now, it is hard enough for me to keep this me out of trouble. I don't have time to wrangle another one.

Tom Hanks' stolen likeness was recently used to sell a dental insurance plan. Drake and the Weekend released a new single that was streamed by millions. This came as quite a surprise to both Drake and the Weekend, because they had not released a new single.

Even in my starving artist days, which went on for quite a while, I chose never to work in the adult end of my business, although a few of the cinematic -- Cinemax projects

I read for came uncomfortably close. But I was recently sent very lifelike images of myself engaged in acrobatic pornography with, I will admit, abs that I would kill for.

It is funny, but it is also terrifying. Deepfake porn is already a thing, and it is not a thing that I or my fellow performers signed up for, especially if we are not getting paid. I am kidding.

People and, indeed, humanity are more than just bits of digital information to be fed into a computer. And as AI grows exponentially by the minute, it is not just the film and television studios we have to worry about. This issue impacts every single American.

Biometric information, even something as routine as a voiceprint or a facial map, can be exploited in ways that pose a danger not just to the broader public but to national security, as you well know.

As more companies use biometric information to verify identity, these risks expand exponentially. We must be vigilant and protect our data. We ask that key questions be answered. How and why is our biometric information being collected? How is it being used? Are there limitations on its use? What control do we have over the data?

In our SAG-AFTRA AI guidelines, we demand the following answers. Are voice and likeness assets being safely stored? Who has access to them? What happens to data when the contractual relationship ends? What happens if there is a data breach?

Privacy laws in over two dozen other countries and many U.S. States address these essential standards for biometric data, but overall the U.S. is behind the curve. There are no comprehensive Federal privacy laws, so individuals must depend on our inconsistent State laws.

SAG-AFTRA will fight to protect our members' voices and likeness from unauthorized use, but all individuals deserve safeguards against unauthorized access to their biometric data.

In addition to the protections in this bill, we believe Congress must put guardrails in place now to prevent future misappropriation of creators' digital identities and performances. Our sector is under assault today. It may be your sector tomorrow.

In closing, I want to say that being an actor can be a strange way of life. What you spend your life learning to create with is yourself, your face, your body, your memories, your life itself. When it works, that very uniqueness creates a character, a story that is universal, ineffable, something that brings people together.

For artists and creators, this is an existential threat. If we don't protect our words, our likenesses, they will be harvested, mimicked, essentially stolen by AI systems and those that use or own the technology.

We have arrived at a moment that is eerily reminiscent of the moment when indigenous peoples first saw cameras and expressed a prescient fear that the machines might steal their very souls.

As the dystopian sci-fi classics tell us, the computers may be coming for us, but we don't have to make it easy for them.

I thank you for your time.

[The prepared statement of Mr. Gregg follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. Thank you.

All right. Next we have Victoria Espinel, president and chief executive officer of BSA, The Software Alliance.

You are recognized for your 5 minutes.

STATEMENT OF VICTORIA ESPINEL

Ms. Espinel. Thank you.

Good morning, Chair Bilirakis, Ranking Member Schakowsky, and members of the subcommittee. My name is Victoria Espinel, and I am the CEO of BSA, The Software Alliance.

BSA is the advocate for the global business-to-business software industry. BSA members are at the forefront of developing cutting-edge services, including artificial intelligence, and their products are used by businesses of all sizes across every sector of the economy.

I commend the subcommittee for convening today's hearing, and thank you for the opportunity to testify.

Safeguarding consumers' personal data and responsibly regulating artificial intelligence are among the foremost technology issues today. Constituents in your districts rely on a wide range of data services to support their local communities and economies. But to fully realize the potential requires trust that technology is developed and deployed responsibly.

The United States needs both a comprehensive Federal privacy law and a Federal law that creates new rules for companies that are developing and using high-risk AI systems. Actions on both priorities will help promote the responsible use of digital tools and protect how consumers' data is used.

We appreciate this committee's strong bipartisan work to pass the American Data Privacy and Protection Act last year and your decision to address both privacy and

artificial intelligence in that bill. Your effort proves that bipartisan consensus on privacy and AI can be achieved, and we look forward to continuing to work with you as you refine your work on these issues.

For too long, consumers and businesses in the United States have lived in an increasingly data-driven and connected world without a clear set of national rules.

We need a Federal privacy law that does three things: requires businesses to only collect, use, and share data in ways that respect consumers' privacy; gives consumers new rights in that data, including the right to access, correct, and delete their data; and ensures that companies that violate their obligations are subject to strong enforcement.

The tremendous growth of AI has underscored the importance of these issues. As this committee has recognized, a Federal privacy law will create important new requirements for companies that collect and use consumers' information, including in connection with AI.

Thoughtful AI legislation is needed too. It can further protect consumers by ensuring that developers and deployers of artificial intelligence take required steps to mitigate risks, including conducting impact assessments to reduce the risk of bias and discrimination.

Privacy and AI legislation will help support the digital transformation of our economy and spread benefits broadly that lead to growth and new jobs across industries.

Farmers can use AI to analyze vast amounts of weather information, to use less water and maximize their harvest.

Manufacturers can revolutionize how their goods are designed and made.

Suppliers and distributors can retool how goods are ordered and delivered.

And construction companies can build AI-generated digital twins of real-life cities to better understand the impacts of a proposed design.

Thoughtful Federal legislation is the best way to promote trust and technological adoption.

I want to emphasize that in order for legislation on these issues to be effective and workable, it has to reflect that different companies have different roles.

In privacy, there is widespread recognition that laws must distinguish between companies that decide how and why to process a consumer's data and the service providers that handle that data on behalf of other businesses.

In artificial intelligence, there is a similar dynamic. At BSA, some of our companies develop AI. Some of our companies deploy AI. Many of our companies do both. And both need to have obligations.

This committee recognized the importance of these distinctions as you advanced privacy legislation last year, and we look forward to continuing to work with you.

I want to conclude by emphasizing the importance of U.S. leadership on both privacy and artificial intelligence.

There is widespread consensus from industry, from civil society, and from consumers that the United States needs Federal privacy legislation. We also need legislation that sets thoughtful rules for high-risk uses of AI. The bill this committee passed last year -- almost unanimously -- already reflects key aspects of those rules.

Other countries are addressing these issues, adopting privacy legislation, and moving quickly on AI regulations. The U.S. is a leader in technological innovation, and we should be a leading voice in shaping the global approach to responsible AI. The time to do so is now.

Thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Ms. Espinel follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. Thank you so very much.

And our final witness is Jon Leibowitz, who is the former Chair and Commissioner of the FTC.

You are recognized, sir, for your 5 minutes.

STATEMENT OF JON LEIBOWITZ

Mr. Leibowitz. Chair Bilirakis, Ranking Member Schakowsky, members of the subcommittee, thank you for inviting me to speak today on two important and related issues: the need for a statutory framework governing artificial intelligence and why Federal privacy legislation is a critical -- critical -- first step towards responsible development and deployment of AI.

As you have heard from my fellow panelists, the rapid growth of AI technologies is bringing extraordinary benefits to every American, but it can also be used to create very real harms. Your committee deserves credit for tackling this issue with a series of hearings.

But as we engage in that important debate, let's not forget the essential need for Federal privacy legislation, which, as you also heard from my fellow panelists, addresses many of these very issues, including the use of personal data through AI.

Now, we live in an era in which data is incessantly collected, shared, used, and monetized in ways never contemplated by consumers themselves. AI has amplified these disturbing trends. It is because consumers have so little control over their personal data and it is shared at will by companies that AI can be deployed so perniciously.

Some large companies have developed ethical approaches to the use of AI, but most businesses are looking for direction and, unfortunately, they are not going to get too much direction from existing laws and regulatory authorities, which are not an adequate match for the problems created by misuse of AI.

For example, the FTC has authority to prohibit "unfair or deceptive acts or practices in or affecting commerce," and some commercial behavior, like using AI for identity theft or fraud, clearly violates the FTC Act and companion State laws. That is good.

The FTC could likely enjoin the company that recently created an AI-generated version of Tom Hanks without his permission and used that image to peddle a bogus dental plan. And, by the way, I couldn't have made that up.

It is not clear that an AI-driven deepfake, though, even if it is deceptive, always comes within the definition of commerce. In other words, legislation is by far the best way to clarify in advance what responsibilities deployers of AI must consider and what risks they must disclose to others.

What is the best approach? I doubt we know that yet. The European Union, through its AI Act, would classify systems according to risks they pose to users. Some States are starting to look at regulating AI, and States can be laboratories of democracy.

But no matter how well-intentioned and thoughtful State laws may be, Federal legislation around AI is far more preferable than a patchwork of State statutes.

And at the same time, Americans deserve a muscular Federal law that will give us greater control over our own information wherever we live, work, or travel, and require more transparency and accountability by corporations. I heard all the members say that today.

Last year, you wrote that bill, one that would create a foundation upon which AI rules could develop. Its provisions are stronger than any single State law and smarter in many ways than the GDPR that governs Europe. It shows that members on both sides of the aisle could work together on a quintessentially interstate issue to create a privacy

regime benefiting all Americans.

The ADPPA was not a perfect piece of legislation, and collectively you may decide to make some modest changes to it when you reintroduce it this year, this year's version. But you reported it out of committee by an overwhelming and bipartisan 53-to-2 margin -- 53 to 2.

In contrast, Congress will need to do a lot of collective thinking before it decides where it wants to end up on AI.

Now, the unprecedented interest by lawmakers in AI-related issues is a welcome development. Indeed, Congress should work on crafting a framework for AI at the same time it protects consumer privacy. But a comprehensive AI law may be several years away.

Comprehensive privacy law, though, should not take that long and is entirely within this committee's jurisdiction and Congress' reach.

In fact, your privacy proposal included many of the same components upon which responsible AI development will be built: requirements for data security, restrictions on collecting information without consumer permission, mandatory risk assessments, obligations for companies to minimize data, prohibitions against the use of discriminatory algorithms, fining authority for the FTC, and protections against targeted advertising to minors 17 and under.

So as you begin to consider the regulatory metes and bounds for AI, let me urge you to keep in mind your groundbreaking work on privacy legislation last Congress.

Even if enacting such a law requires some complicated negotiations and a few difficult votes -- which it will -- you will have done something meaningful for American consumers if you succeed. You will enhance American competitiveness if you succeed,

and you will have laid the groundwork for legislation making AI safe and effective.

Thank you.

[The prepared statement of Mr. Leibowitz follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. Thank you. I appreciate that. And I agree. And I will begin with the questioning.

Now, we are going to try to get as many members as possible to ask questions before we recess.

So I will start again with Mr. Leibowitz.

You have an extensive amount of experience, sir, from chairing the FTC to serving in civil society groups and even staffing Senators. There is a lot of interest right now about what to do, as you know, obviously, what to do about AI. But despite years of trying, we have no foundation for how consumer data is collected, used, and properly secured. We need to get the fundamentals in place.

You mention in your testimony the legislation this committee passed, nearly unanimously, was stronger than any State law. And I appreciate you emphasizing that, sir, today.

Can you expand on that and speak to how important it is for us to have a preemptive national standard to ensure data privacy and security for our constituents and for American leadership on AI. I know you did talk about it, but, please, if you can, if you have anything more to say, I want to give you the time.

Mr. Leibowitz. Thank you, Mr. Chairman.

And I guess I would make this point: Data travels in interstate commerce. It is not contained in a particular State. And consumers deserve a very high level of privacy protection -- this committee knows that better than anyone else -- wherever they live, wherever they work, wherever they travel. And that is what a comprehensive privacy law would do.

And look, we should give Californians, the California Legislature a lot of credit, because they were the first State legislature to show us that lawmakers can pass a law that protects consumer privacy.

But your data minimization isn't in the California law. Your limits on sensitive data, by default, not in the California law. The prohibitions on discriminatory use of algorithms, not in the California law. The prohibition on targeted advertising to children, not in the California law.

So it is almost like we are comparing apples and oranges. We need a Federal law. Your Federal law is stronger than any State law -- or your Federal proposal. And I would just urge you to move forward with it, as I know you want to.

Mr. Bilirakis. Thank you very much, sir. I appreciate it very much. Couldn't agree more.

Mr. Gregg, I appreciate you traveling across the country to be here. Your testimony on the collection and use of what is fundamentally your data is insightful, not just as a Hollywood creator but also as an everyday American.

I would like to discuss another important element of your efforts, which is the need for better security of our data.

We know these large AI systems harvest and scrape the internet for data, and that includes personal information due to the data breaches and hacking, amongst other causes. This can be used for deepfakes and other scams that I will call digitized fraud.

And the question is, how have you and the general public been harmed by this data being exploited and used for purposes that it wasn't intended for because there wasn't enough security around it? And I know you gave some examples, but if you could elaborate on that, sir, I would appreciate it.

Mr. Gregg. Thank you. Thank you, Mr. Chairman. It is an honor to be here.

Mr. Bilirakis. Your mike.

Mr. Gregg. I am new. I am new to this.

Like so many Americans, I am a consumer, I am a human, I have a family, in addition to being a performer. I shared some of the ways that your image will show up in ways that you never agreed to, some that are quite offensive. And I never signed off on that. And it is only a matter of time till those start to show up in video form that become, as AI expands exponentially, more and more lifelike.

As I said, that is a violation of the ultimate freedom, is my right to free speech, my right to privacy, my right to exist as an entity that makes my own decisions.

But I think what is most disturbing about this, as I have studied it and been very interested in it, because, as I said, the ramifications both for writers and filmmakers and actors are huge, and they are being fought right now.

One of the honors about being on the picket lines for us is that we feel that we are in an inflection point that is coming all around the Nation. We just happen to be in a visual, visible union.

But what I am struck by is the way that the CEOs themselves who run these corporations, they have all signed a letter saying that the threat is equal to or greater than thermonuclear war. The experts on AI, they can't even really quite tell you what it is going to become.

And so I think, to answer your question, we don't quite know what this is going to be. And in my experience and probably yours, when there is technology that can generate a profit, very often the profit is what drives the pace, not what is best for humans.

And machines, when we first picked up a stick the concept was that they would work for us. And what it feels like to me -- and I admit I watch too much sci-fi -- it feels like we are on a fast track to be working for them.

Mr. Bilirakis. Thank you very much. I appreciate that very much. And I have other questions, but I will submit them for the record.

Now I will recognize the ranking member of the subcommittee, Ms. Schakowsky, for her 5 minutes of questioning.

Ms. Schakowsky. First of all, let me just say how much I appreciate that pretty much to a person all of your witnesses have now said that we need a comprehensive privacy bill. And we were well on our way. So we need to continue that.

Ms. Kak, I wanted to ask you, you mentioned in your testimony right at the front that many of the tools that are needed to protect consumers from AI are already in place. Are you saying that we could move ahead right now because there are mechanisms that we have? And what are they?

Ms. Kak. Thank you, Ranking Member Schakowsky.

I think the recent joint statement of our Nation's enforcers said it eloquently, which is there is no AI-shaped exemption to the laws on the books.

And so the moment we are at right now I think is to first and foremost clarify and strengthen the laws on the books to apply to AI. The FTC has already opened an investigation against OpenAI, based on its deception authorities. The EEOC and the CFPB have also issued guidance in their particular domains. And the Chair of the SEC, Gary Gensler, recently said that he is worried and looking into the fact that the lack of diversity and competitiveness in AI models is really a financial stability risk.

So that is one. I think we really need to adequately resource these agencies

commensurate to the growing scale of the problem.

But second -- and we have all said this -- there are laws in waiting. We have the ADPPA. We have done the hard work of distilling a globally leading privacy standard.

So I guess my simple point today is that we shouldn't be reinventing the wheel. We have the tools. It is the time to act.

Ms. Schakowsky. Thank you so much.

Mr. Gregg, first of all, I know that your industry right now, we all love our actors and the opportunity to see them, have been on strike now for 6 months. I am sure some of those issues, as a supporter of labor, are more traditional labor issues. But I know that AI is one of those and you have been talking about that.

What would you say is the biggest concern now of workers, actors, that really threatens your business and their livelihood?

Mr. Gregg. Thank you so much.

Every time I think that I have done everything that could possibly make a human nervous, they come up with something else.

Thank you so much for your question.

Our concerns, as I expressed, can be far-reaching and existential, but they are also very simple in that we have an example in that 15 years ago, as a member of the Writers Guild, we were on strike about compensation, the things that we have to survive in a business where you are essentially an independent contractor.

We got through strikes. We got health insurance that way. We got residuals so that you have some chance to make some monetization of the work you do.

When that happened 15 years ago the thinking was, well, listen, we can't really give you any real protections in streaming, the internet, that is not a thing. The day

after the strike was resolved, Hulu was announced.

And so when things moved to streaming, our compensation models, without really our consent, suddenly changed. And all of a sudden -- perhaps it is a coincidence -- all of the content moved, all the stories all moved to streaming, and our compensation drastically trailed off.

And so while we have the existential concerns about committing our lives to telling stories and bringing the human soul to a collective medium, we also have survival issues. And that is that we need to have -- I am going to get the three C's from my colleague.

Okay, good. Thanks.

I should know these. I know what they mean. Consent, compensation, and credit, just to have our image, the work we have done.

I heard a really amazing AI researcher speaking about this last night, that what AI does is it takes human cognitive labor, which is something, it is different than minerals, and it harvests it, essentially.

So our work is something that is harvestable, and we need to be credited, compensated, and we need to have control over the way ourselves are used.

Thank you.

Ms. Schakowsky. Thank you so much.

I know I am out of time. Let me just say that I am going to want to talk to all of you as we move forward, working on legislation that we can do on privacy and on AI. So thank you very much for your testimony.

Mr. Bilirakis. I welcome that as well.

The gentlelady yields back.

Now I will recognize the chairman of the full committee, Mrs. Rodgers, for her 5 minutes.

RPTR SINKFIELD

EDTR HUMKE

[12:02 p.m.]

The Chair. Thank you, Mr. Chairman. It is the first in a series of AI hearings from our committee. It is the seventh in terms of data privacy. And just let me add that the importance of protecting our kids runs throughout. Chairman Bilirakis highlighted security. We have worked on data minimization. We have had multiple layers that provide even more protections with national standard for data privacy. The legislation isn't just about one provision. It is about all the provisions working together to achieve the strongest protections possible for everyone, including kids.

I would like to start with Ms. Espinel. Can you tell me how conducting impact assessments and calculating risks will serve us well in data privacy legislation and prevent harms in AI.

Ms. Espinel. Yeah, thank you very much. So impact assessments are a very important tool in terms of assuring that there is accountability; in terms of assuring that companies are acting responsibly. I want to start off by saying we believe it is important in privacy and in AI that impact assessments applied both to -- would often control processors and privacy law, but also developers and deployers in AI.

Those that are creating the AI systems and the companies that are using AI systems both should have obligations to conduct impact assessments. Those impact assessments would be slightly different because those companies are doing different things. They have access to different data, and they can do -- they could take different steps in order to mitigate risks.

And so the obligations and the impact assessments should mirror that. They should reflect that. But you can think of an impact assessment in a way like a report card.

The Chair. Okay.

Ms. Espinel. For a developer, someone creating an AI system, they need to have an impact assessment that looks like what is the purpose of that AI system, and what were the limits on that AI system? In other words, what should that AI system not do?

The Chair. Thank you. That is great. I know there is a lot more. I have a couple more questions, though, but thank you.

Mr. Krikorian, I appreciate the way you distilled potential AI harms. Mr. Gregg's points on sophisticated technology can be it underscores our concerns of how adversarial nations, including China with TikTok could access and train AI models using our data to cause harm and manipulate us. So very briefly, would a data privacy, comprehensive data privacy security bill similar to ours from last year, that restrict data brokers in Big Tech counter this threat to our security?

Mr. Krikorian. Thank you for that question. I believe it would for portions of it. I think that giving people transparency to where their data is going and giving them consent on how to access control is extremely important. I do highlight that I think there is some concern around these public spaces, these digital public spaces that people are voluntarily surrendering their data into, unknowingly and at large volumes.

And it is unclear whether or not those could be fully covered because those are simply scrapeable and downloadable by different parties. But I think from the explicit data collection standpoint, yes, I do believe that some form of this act would prevent those harms.

The Chair. Okay. Thank you. Mr. Gregg, my kids would be disappointed if I didn't let you get away without a question, not to mention quopping one of your lines. So, you know, we focused a lot on the importance of foundational protections and data privacy for also being important for trustworthy AI. It is a massive undertaking with concessions from all parties and stakeholders.

So would you agree this is never going to work if we don't have something to unite behind, and that enacting data privacy legislation is important this Congress.

Mr. Gregg. First of all, thank you, and my greetings to your kids. And I am really impressed that they remembered that line from an episode that I loved. Yeah, absolutely. I think what was just said about voluntary means that you put. And I see all these things popping up in California now.

You know, which part of your data do you -- I don't know. I don't know. I am busy. I want it -- I don't like that I think of something, and 2 days later I get an ad for it. It is creepy. Pardon me. I don't know if that is -- but I guess I can say creepy. But I think that we are depending, we are depending on guardrails to come from you.

As was said, this is a national -- the borders don't exist here. This is all happening around the planet in microseconds. We depend on the guardrails that can be put in place nationally. This committee is so important to me; to protect us as we figure out what this even is and what the ramifications are. Because clearly most of us don't. Thank you.

The Chair. Thank you. I really appreciate everyone being here. This has been a great panel. We do have more questions, but I have to yield back right now. I am out of time. Thank you, Mr. Chairman.

Mr. Bilirakis. Thank you. I thank the gentlelady. And now I will recognize my

friend from New Jersey, ranking member of the full committee, Mr. Pallone, for his 5 minutes of questioning.

Mr. Pallone. Thank you, Chairman Bilirakis. Last Congress I was proud to chair this committee as we advanced the strong, comprehensive, and bipartisan American Data Privacy and Protection Act.

And this bill put consumers back in control of their data, stopped aggressive and abusive data collection by Big Tech, and rejected the failed notice and consent regime. It also required data minimization and algorithmic accountability in order to ensure companies collect only the data they need to serve their customers.

So my questions are of Ms. Kak. Do you believe that notice and consent is a sufficient mechanism to protect consumers and their data from the harmful and abusive practices of tech companies?

Mr. Krikorian. Thank you, Mr. Pallone. The short answer is no notice and consent mechanisms are necessary, but they are far from sufficient.

So can they be a powerful believer? Yes. And I think the best example we have of this is Illinois' BIPA law where consent has actually been leveraged to shut down some of the most concerning users of AI, for example. Clear-view AI. But even there it is buttressed by a bright-line prohibition which prevents companies from profiting off the sale of biometric information. Now the core weakness of consent, of course, is that it completely breaks down any time there is stock power asymmetry. It breaks down in the workplace. It breaks down in schools.

But as Mr. Gregg just pointed out, arguably that power of asymmetry affects all of us and is all pervasive. And that is particularly why the ADPPA is so strong because it has the whole suite. It has consent. It has data rights. But crucially it is setting the

rules of the road so that these rules of the road apply regardless of what the consumer so calls chooses.

Mr. Pallone. All right. Thank you. Now how does the rapid growth of AI impact the urgency implementing strong comprehensive federal data privacy legislation that implements clear rules about or around data minimization and algorithmic accountability?

Mr. Krikorian. Thank you, Mr. Pallone. I would argue that data privacy has been an urgent priority for the last decade in the United States. But the events of the last 2 years, and maybe particularly if of the last few months, only reinvigorate calls for urgency. There are three main reasons that AI makes the passage of a data minimization mandate crucial. The first is the obvious one which is privacy. We are seeing new privacy threats emerge from AI systems. We talked about the future threats and how we don't know where AI is going to go, but we absolutely do know what harms they are already causing. They are leaking personal information.

They could potentially be leaking patient data and healthcare contacts. These privacy risks are not abstract even if the technologies are portrayed as these abstract magical systems. The harms are very, very real.

The second is competition. As I mentioned in my testimony, this is very, very crucial because we are at a moment where unchecked commercial surveillance is being incentivize by AI system. And unless we have rules of the road, we are going to end up in a situation where this is -- where the kind of state of play against consumers is entrenched.

And thirdly, this is crucial. Data privacy law is crucial for national security as well. We need security norms in place to make sure that, you know, the way we like to say it, is

that data is never collected is not at risk. Or data that is deleted after a reasonable period of time will no longer be at risk.

So we need to really minimize the surface area after that. And I think at the current moment in the absence of a federal privacy law we risk not only competitive and privacy threats, but I would argue national security threats as well.

Mr. Pallone. Well, I guess to my last question, Ms. Kak, in addition to protecting privacy, what other harms can be addressed with data minimization principles. For example, you mentioned doesn't it help address data security challenges and national security concerns.

Mr. Krikorian. Absolutely. The way we like to say it, Mr. Pallone, is that we are essentially creating gold mines for and honey pots really for cyber criminals of all varieties.

And this can be -- as Mr. Gregg and other pointed out -- we are actually incentivizing the creation of databases, including the databases of kids' information, that is kids' images and videos.

And we have an example of recently where it was reported that we have a large children's database that was created and was being sold by a company call Megaface. These kind of practices are going to become the norm, and AI is only supercharging existing incentives for unchecked and invasive data surveillance.

Mr. Pallone. All right. Thank you so much. Thank, you Mr. Chairman, I yield back.

Mr. Bilirakis. I thank the ranking member. And, you know, I think we just gaveled in, but out of respect to the witnesses and the audience, we are going to keep going as long as we possibly can. So I will recognize Dr. Bucshon for his 5 minutes of

questioning.

Mr. Bucshon. Thank you, Mr. Chairman, for calling today's important hearing on something that will play an even larger role in Americans' lives, AI.

With AI already being deployed in a multitude of economic sectors from healthcare to manufacturing, to defense, it is critical that Congress create an environment to foster innovative uses of such technology while also protecting Americans from possible harms. Enacting a national data privacy framework such that we passed through this committee last year with the ADPPA, to establish clear rules of the road for the U.S. is a key factor in deploying effective AI that will help U.S. innovators keep their edge against competitors abroad.

One of the goals of implementing a national data framework will be to provide some certainty to consumers. And as you mentioned in your testimony with the case of the deep fake Tom Cruise ad and the use of AI in generating such content, Mr. Leibowitz, do you think that regulation of AI content should or could include the use of something like a watermark or other indicators to consumers that content is AI generated?

Mr. Leibowitz. Yes, I absolutely do. I think a watermark is something you should strongly consider as you think through putting the right guardrails on AI and making sure that people are compensated for their work, and also that consumers know when something is generated by AI and when it is generated directly by a human brain.

But I would also say one more thing, which is that -- and as you heard from fellow panelists -- so much of what you want to do to regulate and to put into place appropriate standards for AI, it is in the privacy bill that you reported out last year. It is the requirements for data security. It is the restrictions on collecting data without consumer permission. It is the mandatory risk assessment that Ms. Espinel pointed out.

And so I would just encourage you -- and I know you want to do this -- not to kick the privacy can down the road. You are the committee that has shown leadership in the last Congress, and you can take it to the next level by enacting bipartisan legislation.

Mr. Bucshon. Thank you for that answer. And, I mean, you are a regulator. What are some of the challenges and then enforcement, enforcing such requirements, and what might you suggest for us to how we would address that?

Mr. Leibowitz. Well, I would say this. One challenge in the FTC -- as Ms. Kak knows because she was there, and Ms. Hone knows because she was there when I was there -- it has terrific lawyers. And they want to represent the public interest.

And they have some expertise in privacy in AI issues, and they are building it. I would say they will need more resources because this is a comprehensive and important piece of legislation, and you will want to give it to them. And I think -- when I was at the FTC, we started the Division of Privacy and Identity Protection because we thought privacy was a more important issue.

Mr. Bucshon. Sure.

Mr. Leibowitz. We had our first chief technologist brought in 2009 because we thought that was important. One of the things I like in your legislation is it would create a bureau bigger than a division on top of a division of privacy. And privacy is so important in America today that I think that would be -- I am a little surprised the FTC hasn't comprehensive done it unilaterally itself. But I think that is an important way to enhance and validate the importance of protecting consumer privacy.

Mr. Bucshon. Great. Thank you. I was a doctor before I was in Congress, so one specific sector I am excited to see AI make strides in is healthcare. I really believe technology is going to really advance us down the field in healthcare and also decrease

costs. And I know that already we are deploying apps in the healthcare systems.

Mr. Krikorian, what role do you think that enacting a national data privacy standard will have on the security and privacy of data for health information that's not explicitly covered by current HIPAA law.

Mr. Krikorian. Thank you for that question. I mean, I would contend that, especially with these machine-learning algorithms that require even more data that might be captured in order to make better predictions, that we need to expand this type of protections to beyond just healthcare information, whether it be perhaps information that is collected by different consumer applications, whether it be Apple, Health, or others might not be already covered, I think we need to extend those protections there.

I think HIPAA is a really good framework for us to think about what this could look like. SOC 2 might be another good framework on how may those be thought about. But an extension to what this consumer data realm looks like, so those could be also used as inputs into these deep models that would be quite important.

Mr. Bucshon. Yeah, it would be important to also continue to have researchers have the availability of the identified data if we are going to continue medical research. And that is one of the challenges of balancing that. So my time has expired, Mr. Chairman. Thank you very much. I yield back.

Mr. Bilirakis. Thank you, Doctor, I appreciate it. I went as long as I could, but we do have a vote on the floor. So we will recess for full activity. Of course, the subcommittee stands in recess subject to the call of the chair. So thank you very much for your cooperation and your patience. And we will be back.

[Recess.]

Mr. Bilirakis. Okay. We are going to reconvene. I know members are starting to come in, but we want to get started as soon as possible.

I want to thank y'all for, the witnesses, for your patience. We really appreciate it so much.

So with that, I am going to ask Chairman Castor, Acting Chairman Castor to ask her -- she is recognized for 5 minutes of questioning.

Ms. Castor. Well, thank you very much, Chairman Bilirakis, and thank you to our witnesses for bearing with us. Your opening statements were very persuasive. It is really refreshing to hear advocates like you pressing Congress to act. It is long overdue for the United States of America to adopt a basic fundamental privacy law online.

So as you raise your voices and encourage us to do that, it is very well received in the committee. Thank you for recognizing our bipartisan work on the ADPPA.

For many years I have had particular concern for the what Big Tech platforms do to exploit our children, to target them with advertising, to surveil them, even though we have a COPPA law, it still is not followed. It must be updated.

So when you think about AI and kids, it seems like all of the online harms directed towards children when it comes to AI would just be exacerbated, would be even more severe.

Ms. Kak, in your testimony, you raised a couple pf examples. Could you dive in deeper in AI and the special kind of considerations when it comes to young people.

Ms. Kak. Absolutely. Thank you, Ms. Castor, for that question and for raising this crucial issue. I think also lets start with the ADPPA which has been the subject of

today's discussion across the board. The ADPPA is we feel one of strongest ways of not just protecting everybody's privacy, but specifically protecting the privacy of children.

So kids data is sensitive data under the act, which affords it the highest and the strictest levels of protection. We have specific prohibitions against targeted advertising on children.

And I will stop there to say that these specific prohibitions and targeted advertising are essentially getting at the root of the business incentives for unfettered collection of data, right? They are fixing the business incentives. And what we have tried to emphasize today, what I have tried to emphasize is if you are attacking the business incentives, you are really future-proofing the law.

So when people ask what do we do about AI, we can point to the ADPPA and say it is structurally changing the business incentives so that companies whether it is AI, or it is the next big thing 5 years from now are structurally not incentivized for the responsible collection of data particularly when that data is of children.

And I think I would kind of, you know, moving away from this particular example of the latest AI fad which is generative AI, we can look at examples of the facial recognition systems absolutely proliferating across schools today. We are really happy just to hear that the New York State has actually banned the use of facial recognition systems in school.

Because speaking of notice and consent breaking down, the clearest example of that would be in a situation where you are at a school, where you have essentially minors that are in no position to consent, choose, or otherwise to these invasive face surveillance tools.

And I think the need of the hour is not just to put in place regulation, but

specifically to put in place bright-line rules against the kinds of data collection that we never think should be permissible.

Ms. Castor. It is kind of like the example that Mr. Gregg gave when comes to an actor and their personal privacy; the ability to control their own image.

So is what you are saying, Gosh, think about children who do not have the ability to consent when it comes to facial recognition, and that could be exploited by others when it comes to artificial intelligence.

Ms. Kak. Absolutely, Ms. Castor. And I don't think that these abstract or theoretical concerns. We already know that there are databases of children's images and videos that are being used in real time by AI companies to generate further material that is extremely sensitive and implicates these children's faces, among others things.

So, you know, again, we are not living in a moment we need to hypothesize about these risks are ever present. And a data privacy law, in particular, that protects everybody's privacy would be the best way to protect children's privacy as well.

Mr. Leibowitz. Yeah, and if I may add something.

Ms. Castor. Go ahead.

Mr. Leibowitz. You have been a leader on protecting kids. But as we know kids act impulsively. They are a vulnerable population. That is why Congress passed COPPA in the first place. And in the ADPPA and the bill you will reintroduce this year, there are going to be protections against minors 17 and under that we don't see anywhere else, not in a single state law.

So just coming back to one of the topics of this hearing I think it is critically important that you move that legislation. And you will be doing a -- you will be taking a major step forward if you can enactment the ADPPA or the ADPPA 2.0, it will be very

protective of children from abusive AI.

Ms. Castor. I agree. I don't think we have time to waste. I will look forward to the bipartisan bill coming back. I yield back. Thank you.

Mr. Bilirakis. Thank you. The gentlelady yields back. I now recognize the vice chairman of the subcommittee, my good friend, Mr. Walberg, from the great State of Michigan.

Mr. Walberg. Thank you, Mr. Chairman. Thanks panel for being here and staying here waiting around for us as well. Many of my colleagues know that protecting kids has been a top priority of mean while serving on this committee.

Although protections currently exist for some children, the scope is limited and doesn't cover the terrible harms we are hearing about in the news. We know the stories like the one in Marquette, Michigan, way up in the upper peninsular of Michigan. A very rural area. Very few people up in that are. Where scammers pretended to be another student and extorted a 17-year-old football player, a good guy who sadly took his own life after being blackmailed.

And another where innocent photos and personal information of ten middle schoolers, females, were turned into explicit images. These kids are met with harassment and extortion by vile actors scraping their data and threatening digital forgeries, explicit pictures to be given to their friends and family. This is abhorrent, and Congress must work to protect children from these evil actions.

I ask for unanimous consent to enter this article, Mr. Chairman, into the record: How AI makes it even harder to protect your team from sextortion online.

Mr. Bilirakis. Without objection, so ordered.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Walberg. Thank you. Mr. Leibowitz, how can the work of this committee in doing what we are doing on an acting and comprehensive data privacy and security law prevent these type of harms to our young people?

Mr. Leibowitz. Well, you have a number of provisions in the privacy legislation. This committee reported about 53 to two last year that really helped protect young people, vulnerable population from abusive AI. It is not the end of the -- it is not all the protections. You should keep on working on AI issues, but it is important.

So requirements for data security, restrictions on collecting data without consumer permission, mandatory risk assessments, obligations for companies to minimize data, finding authority for the FTC and states' attorneys general, the protections which we just talked about on minors 17 or under --

Mr. Walberg. And these will have the teeth to really do the job.

Mr. Leibowitz. Well, there is an absence of teeth now, right? And current law is inadequate. So I think this will take a really critical first step, an important step with not letting all of that information out of the barn --

Mr. Walberg. Okay.

Mr. Leibowitz. -- particularly as it hurts consumers. AND I just want to make one other point which is COPPA is 20 years now, and it needs to be updated. But it was really well written by Congress. So, for example, one thing you did was you allowed state AGs to also enforce the law.

Another thing is you gave the FTC rulemaking authority. So when I was at the FTC, we updated the COPPA rule to prohibit the collection of precise geolocation information. Now when COPPA was written, nobody knew what geolocation

information was. When I got to the FTC, I didn't know what geolocation information was. But we realized it was a big gap in COPPA, and we were able to fix it.

So I think you need to give some rulemaking authority possibility within guardrails. And I think you did that last year to the FTC to do some rulemaking because they have expertise in this area. Thank you.

Mr. Walberg. Okay. Thank you. Mr. Krikorian, I would be remiss if I didn't bring up your testimony on self-driving vehicles. Michigan's the auto capital of the world. An area that is of great priority to Republicans on this committee, that self-driving space.

I have had reservations in the past, especially to make sure how to use other roads users like motorcyclists remain safe. I do believe these vehicles can be made safe, but there are certainly limitations to where and under what parameters they can be tested. In order to become better and have greater chance to deploy broadly, self-driving vehicles need to collect, lots of data to improve. I think this is analogous to other areas that Chair Bilirakis discussed in his opening statement.

Good actors can use the data they collect to improve products and service, increase cybersecurity, or other improvements that they think is reasonable. Can you explain the harms that could arise if we limit this type of improvement in innovation.

Mr. Krikorian. Thank you for that question. If we don't do -- if the question is what happens if we don't do enough data collection in order to make things safe? Then we won't have enough data to power our algorithms. We won't have a enough data to power our simulations. And therefore we won't understand all the different complexities of what we might even encounter on the road.

We used to collect terabytes of information at Uber for every hour that we drove

on the road so we can properly analyze it after the fact and make sure that they are accounting for every single possible edge case that we might see on the road.

And if we didn't do that, then we would have a problem. Like we just wouldn't be able to understand all the situations, say a toddler running across the road, which happens maybe one in a million miles. But that one in a million miles is incredibly important.

So we don't capture all that data. It is incredibly important. But if we had major issues on the simulation and data validation side.

I will say, though, there are ways to capture this data and preserve privacy at the same time. You could be capturing data and scrubbing faces before it hits disks. You could be doing all these things that allows us to still get what we need from the information without violating say where a person is going or becoming a mass surveillance mechanism that is roving on the roads.

Mr. Walberg. Thank you. My time has expired. I yield back.

Mr. Bilirakis. Thank you. I recognize Representative Kelly for her 5 minutes of questioning.

Ms. Kelly. Before I started I wanted to yield a minute to Representative Cardenas.

Mr. Cardenas. Thank you for yielding, and thank you Mr. Chairman and ranking member for having this important hearing. The advancement of artificial intelligence brings massive opportunity for United States and the world. Through the development of AI, we will see unprecedented progress in research and innovation, improvements in the existing industries, and the creation of entirely new ones.

However, there are negative aspects as well that we could actually make better

with legislation through Congress. For example, artists deserve to be compensated when their work is used, and importantly they should not be competing in marketplaces with products that are artificially generated without AI-generated products and clearly labeled. This can and will vastly and drastically change the workplace not throughout America only, but throughout the world.

And I think that we can do a good job of legislating to make sure that we mitigate as much as we can.

With that, thank you so much for yielding time, Ms. Kelly.

Ms. Kelly. Thank you, Chair Bilirakis, and Ranking Member Schakowsky for holding this important hearing. As many of you know a few years ago, I had the pleasure of working with former Congressman Will Hurd of Texas in partnership with the bipartisan policy center to produce four white papers related to a national artificial intelligence or AI strategy.

As you such, I spent the past 2 years following the development of these technologies and systems. And I agree that AI has great potential to create new opportunities and greatly improve the lives of Illinoisans and all Americans. But we have already seen many ethical challenges that previously existed like bias, talked about privacy, and power, asymmetries evolve and can be greatly exacerbated by the emerging use of AI technologies and systems.

For these reasons, I strongly believe the issue of civil right and liberties must be front and center in discussions about the investment deployment and oversight of AI technologies. We must protect against the potential for these AI technologies and systems to harm Americans and reduce the ability of all communities to participate in the digital transformation of the economy.

Ms. Kak, ADPPA has strong provisions regarding the need for data, minimization, which I strongly support. Some critics have suggested that the principal of data minimization would hamper U.S. companies' ability to develop and deploy AI systems, leaving them at a competitive disadvantage of companies based in other countries. Do you agree with these concerns, or do you believe American companies can deploy AI while also having strong federal data privacy regulations?

Ms. Kak. Thank you, Ms. Kelly. I disagree with those statements because they are based on data minimization itself. I think this caricature presents data minimization is somehow stopped access to data wholesale where the truth is very far from that. We are simply setting guardrails on permissible purposes.

And we are kind of providing an antidote with data minimization to the otherwise incentives supercharged with AI, the incentive that exist to kind of hover up as much data about users and store it for as long as possible.

Now one other way to put this is that in America we want to be incentivizing the right kind of innovation. The whole premise of the AI race against China is that Democratic AI needs to beat out authoritarian AI. And the way we in which we do this is by sort of heightening the contradiction there. The way in which we establish U.S. global leadership on AI is by setting the precedent for what Democratic AI looks like. And I think a strong privacy law does that and is a very strong step in that direction.

Ms. Kelly. In your written testimony you talk about regulating the collection of certain kinds of sensitive material. How do the Illinois Biometric Information Privacy Act and other similar states laws limiting the use of biometric data protect Americans' privacy?

Ms. Kak. So the Illinois BIPA one of our favorite examples of a very strong data

minimization mandate for two reasons, right? Because although it has the lever of consent and that is very important, and it sets a high consent bar, it is at the same time drawing a bright line and saying no company should be able to profit from our biometric data. And it is because that line is drawn so very clearly in the sand that it has led to such successful litigation.

Most recently the fact that Clearview AI has now been permanently banned from selling its face database of millions of our faces to private industries for profit.

Ms. Kelly. And Ms. Espinel, would you please elaborate on why robust data protection is so critical.

Ms. Espinel. I think as AI becomes more powerful, privacy protections become more important. So we have already had a conversation about the risks, deep fakes, hackers' access to consumer data. These concerns are real. They are happening now. That makes the need for federal privacy legislation even more urgent.

But I would also say we need legislation on high-risk uses of AI as well. And I commend the committee for the bill that you developed last year that addresses both of those issues.

Ms. Kelly. Thank you so much. I yield back.

Mr. Bilirakis. The gentlelady yields back. And now I will recognize the representative from South Carolina, Mr. Duncan, for his 5 minutes of questioning.

Mr. Duncan. Thank you, Mr. Chairman, and a very timely hearing. We may have to tap into AI to figure out how to elect a Speaker of the House. We are going to have a hearing tomorrow on AI and the energy sector. I chair the Energy Subcommittee, so I look forward to that.

On July 13, 2023, the People's Republic if China issued final issues aimed at

regulating generative AI services such as ChatGPT to the Chinese public. Under these provisions, content providers must uphold state power and ensure the development of products aligning with the socialist agenda of the Chinese Communist Party. These actions, along with censorship and the CCP's growing control over the private sector have stifled domestic grown and innovation.

While this committee recognizes the need for a framework to address AI's potential risk to ensure responsible development and deployment, how do we also ensure that AI systems align with our own Democratic values while promoting a fair and open regulatory environment?

So for Ms. Espinel, you have talked about the different roles of companies in privacy and AI legislation, tell me more about those roles and why legislation should distinguish between them?

Ms. Espinel. So first I will say I think its very possible to have regulation that leads to responsible AI and takes a different approach than other countries. And I think the Unites States being a leader on what a regulatory approach to AI that reflects our values, I think that is critically important. One of the things that it also needs to do is recognize the different roles that you refer to. There are companies that develop AI. There are companies that use AI.

Our companies do both, and there should be obligations on both. They should reflect the fact that whether you are training a system, creating a system, or using a system, you are going to have access to different information, and importantly you are going to be able to take different kinds of steps to identify risks, and then fix those risks.

So having obligations for both and having impact assessments that will give companies a tool to identify what the risks are and then importantly go out and fix those

risks is critically important.

Mr. Duncan. Thank you for that. Privacy laws around the world in the U.S. and the U.S. statues governing privacy and security of financial and health information distinguish between control or versus a process when we recognize different roles they play in the ecosystem and tailor responsibilities accordingly.

Why should Congress support maintaining this distinction in federal privacy legislation. That question is to you too.

Ms. Espinel. For the same reason because whether you are a service provider that is processing data -- so for example, if you are at a grocery store and you are collecting data by your consumers, you have and you should and be responsible for making decisions about how to limit use of that data, for example. If you are service provider that is processing that data, you often will not have access to it. And we don't want service providers to have access to it. That would undermine privacy.

So it is a practical example of why those distinctions which again this committee is recognized and has been recognized I think in 126 laws around the world is important. And so I commend you for the work on that.

Mr. Leibowitz. Yeah, and if I could add just one small point to that, and I agree with everything that Ms. Espinel said. But she works for an association of the best companies. And -- and they are.

Ms. Espinel. Let the record reflect.

Mr. Leibowitz. And fine. And if you don't have a standard or a floor, then the companies that aren't the best companies, sometimes even the companies that were almost the best companies, they go down to the bottom because they are at a competitive disadvantage.

And so at the FTC we want after a lot of scammers, and they would come into my office or companies that engage in deception. And they weren't bad companies, but they would say, yeah, I would like to protect consumer data this much. But if I did that, we couldn't earn money because everybody else is at a lower level. And that is why you need a privacy baseline. And that is one reason why we need --

Mr. Duncan. I have heard concerns about how AI generated content, taking, using, profiling from individuals image and voice without acquiring consent. While this committee has been focused on privacy and data security of sometime, we have also focused on NIL and how it impacts people such as college athletes.

To that end, I am curious if you see issues beyond privacy like property right protection, image protection, whatever, as an essential part of what Congress should be addressing when attacking AI policy. And I don't care who answers it. You have got 45 seconds.

Ms. Espinel. Well, I think there important issues that are raised here. I think one of the things that Congress could think about is whether or not the right of publicity at a federal level would be helpful here. There are rights of publicity at the state law, but again not all States have those laws.

There is not one sort of federal standard for that. So a suggestion would be that Congress consider creating a federal right of publicity to address some of those concerns.

Mr. Duncan. Mr. Chairman, I have seen some videos recently where an image of someone was taken, and AI generated content of that person speaking something that they never said.

And how that could be used in a political realm against adversaries for blackmail or other things, even putting college athletes and students in a bad positions where they

have got to say that wasn't me, it looked real, and it is scary. And with that we are always concerned about privacy of American citizens.

Mr. Bilirakis. Thanks for bringing that up. I appreciate it. Mr. Gregg, do you want to respond to that at all? Briefly. Yeah, please.

Mr. Gregg. Very briefly?

Mr. Bilirakas. Yeah.

Mr. Gregg. No.

Mr. Bilirakis. Okay. All right. Now, I will recognize my good friend from the State of Florida, Mr. Soto, for his 5 minutes of questioning. Thank you.

Mr. Soto. Thank you, Mr. Chairman. Thank you to your witnesses for being here and having patience as we had to interrupt the hearing for a little while. We know whether it is deep fakes or ChatGPT, looking at fraud by impersonation, or advanced manufacturing that AI is awe-inspiring, but it also be can disruptive. We see it is particularly being disruptive in professional services and entertainment, in various different parts of our economy.

Mr. Gregg, first, I want to unequivocally announce my support for the SAG-AFTRA and members who are striking for better wages, benefits and workplace rights. We have many of your members in Florida and really appreciate it. I represent the Orlando area, and we have many artists, working in our theme parks, as actors, as musicians, in production. And I know that you have already mentioned AI is being used increasingly to replicate well-known actors, things of that nature. It would be great to hear how you think it affects those who are in production, all those workers who are helping produce movies, and minor characters and extras and the vast majority of folks that are involved in this SAG-AFTRA union.

Mr. Gregg. Thank you so much for our union's activities. The question if I understand it is how AI and this issue affects the broader rank and file of the crews and the, I don't know what not movie stars, et cetera, who work in our business. For us, we were just talking moments ago. For us this is not a future concern.

This is already happening now. As said the move from streaming felt like a test case for us where, you know, because it was monetized in a different way. It was advantageous more to the corporations and disadvantaged the right rank and file actors and production people, we already saw a huge shift down for the workforce.

The median income of writers went down 14 percent during the time when obviously the cost of living has gone up. Of the entire rank and file of SAG actors, which is before this strike a lot people thought it was just, oh, that George Clooney or whoever's got a lot of money.

But what has been able to be communicated, in my opinion, is that the vast majority of people, whether they are IATSE crew members, or actors, or writers are in middle. There is a reason it is called the middle because everyone is there. And they were making -- 26 percent of actors at any given time at any given year make the minimum they need to just get basic health insurance.

So when you start to take our image, our work, our likeness and turn that into a product that is being made by counterfeits, by bad actors in terms of foreign entities and counterfeits, you are taking away what is left of a pie that is already being shrunk in the economy as it stands.

Mr. Soto. Thank you so much. Ms. Espinel, University of Central Florida has world-class digital twin program. We work in everything from helping doctors with surgery prep to training firefighters and cops, improving efficiency of factories and

distribution centers.

How does the lack of AI legislation right now limit innovation in digital twin technology and other simulation and training type of technology.

Ms. Espinel. There are a lot of exciting things that are happening in digital twins. You mentioned some of them surgeons using them. Urban planners using them so they can figure out what the impact of the design is going to be, reduce costs, increase sustainability.

But I agree with when I think is your premise that passing AI legislation will help increase adoption. I think it will help increase trust in technology and increase adoption of AI in ways that would be beneficial to our society in its --

Mr. Soto. And why do you think that.

Ms. Espinel. Because I think having the clarity and predictability of what the rules are. How companies should be either in terms of privacy protections or how companies should -- what they should be doing what there are high-risk uses of artificial intelligence will give companies clarity and predictability that they need to make investments. It will give consumers trust that the technology is being used in a way that is responsible.

All of that I think will lead to greater adoption and in greater benefits from the positive tools that we are seeing.

Mr. Soto. Thank you so much, Ms. Espinel. You know, Chair, I have seen them scan people's bodies and practice surgery before they are even starting. I have seen logistic centers improve by digital twins. We have seen firefighters trained and cops trained on how to approach a major disaster, like a block-long fire all because of the work that is being done in our areas.

So we want to continue to make it further our ground for this innovation to continue. Thanks and I yield back.

Mr. Bilirakis. Thank you very much. I thank the gentleman. He yields back. And now Dr. Dunn from Florida, a good friend of mine, I know he had some great questions. You are recognized, sir, for 5 minutes.

Mr. Dunn. In fact, thank you very much, Mr. Chairman. I think there have been some great points made here by my colleagues and of course the panel. And, you know, clearly we want responsible data privacy protection as AI moves forward. But what is also critical that we maintain a competitive edge if you will in acquiring and developing this technology in America.

AI has obvious major applications in defense national security systems. In the global economy, we are presented with the challenge of preserving free markets while simultaneously protecting trade secrets of individual privacies, and of course critical technology.

Recently, the Commerce Department issued rules that require U.S. chipmakers to attain a license in order to export AI chips. I believe this is on the right track, you know, protecting the United States from global adversaries is a bipartisan nonnegotiable issue. China has been using AI in its national strategy for a years.

As early as 2017 China announced a national AI strategy that describes a new focus of international competition in AI. And that was 2017. Six years ago. This begs the question of what incentives should we be considering to ensure that our companies won't sell products to China in a manner that deteriorates not only our competitive advantage but our national security.

I have a July article, the CSIS which reads: The reality of Chinese military

purchasers is not up for debate. It was openly published and unclassified Chinese military procurement contracts followed just between April and November of 2020. They followed over 21,000 such contracts that all specified specifically American chips had to be used in the contract. Not one single contract specified purchasing Chinese chips.

So, you know, corporate profits in America, shareholder earnings are a clear motivation for U.S.-based AI chip manufacturers to export AI technology, even to communist China, but we need corporate America's cooperation on this, and it is an extremely dangerous area.

Mr. Leibowitz, I know you have a lot of experience with the FTC, do you think these export controls, current as they exist, are they going far enough, or should it be tweaked?

Mr. Leibowitz. Well, I am no expert on export controls, but I do agree with everything you have said, and it makes sense to keep exploring this approach. I would say also that when it comes to sort of leadership on protecting a consumer privacy and ensuring the proper guardrails on AI, it would be much better if our companies didn't go looking to Brussels for rules but came to the United States, and we set our own rules that are helpful to American corporations.

Mr. Dunn. We look to you for ideas on these things of all of our panel members. On another date, the Bank of America noted that their prediction, AI will be driving 16 trillion with a "T" dollars worth of economic activity annually. That just impacts every sector. That is a vast opportunity for domestic markets, but wait until proceed intelligently.

The sheer size of the Big Tech companies often give them the advantage. You

alluded to that earlier. Obviously, with some. With all your experience, sir, do you think that is the large U.S. corporations, that they have an undue advantage in the market?

Mr. Leibowitz. I think large corporations sometimes do have an undue advantage in the market and in sometimes we look at this as the FTC, Congress has looked at this, do create sort of barriers to industry for small and medium-sized companies. It could be their competitors. I do think when you have a well-intentioned but not probably -- but not well-executed law.

Like for example, the GDPR, you exacerbate those problems. And so one of the things that I think is very positive about the legislation that came out of this committee last year is you strike a proper balance between making sure the consumers are protected and also making sure that there can be compliance with those laws by companies.

Mr. Dunn. I thank you very much for those comments, and I do hope that you will help us keep our balance. Mr. Chairman, I yield back.

Mr. Bilirakis. Thank you. The gentleman yields back. Now I recognize Ms. Clarke, excuse me, from the great State of New York.

Ms. Clarke. Thank you very much, Mr. Chairman. I thank our Ranking Member Schakowsky for holding this hearing today.

I would also like to thank our witnesses for first of all your indulgence for being here to testify on such a very important topic.

I would also like to take a moment to recognize the context in which this hearing is being held. Right now, the House is essentially paralyzed. Even if this committee were to finally approve bipartisan privacy and AI regulations, the House couldn't even vote on

it.

Republicans continue to demonstrate their inability not only to govern but just figure out who to lead them, all while we are marching closer to another Republican shutdown. Democrats remain committed to passing bipartisan legislation that meets the moment, whether that is a comprehensive privacy law or addressing the war in Ukraine and the escalating Israeli Hamas conflict.

I believe, as many of my colleagues do, that one of the best ways to protect consumers and promote responsible use of AI is by passing comprehensive data privacy legislation.

Having said that, Ms. Espinel, in your testimony you reference how impact assessments are already being used across the industry. What are AI companies currently doing to evaluate risks created by their systems before and after the systems are deployed?

Ms. Espinel. Thank you very much, and thank you for your long leadership on these issues. So our companies, I represent the enterprise facing part of the tech industry are doing -- are taking quite a few steps.

So sometimes that is testing their models, including doing red-teaming. That is often that is assessing the quality of the data that is going into it. But the specific steps that they are taking often fall into this framework of impact assessments that you refer to.

And having developers of AI and having deployers of AI do impact assessments at every step of the process is very important to make sure that companies are acting responsibly; to make sure that they are not cutting corners. So I like to think of the impact assessment as a report card that measures the intent of the system, whether or

not it is being used correctly, whether or not the data that has gone into it is the quality of data that it needs to be.

And then I think what is important is the impact assessment be part of a larger risk management program so that if the report card comes back and it shows that there are problems that the companies have steps that they can take to address them.

And the last thing I would say is that they publically certify, that they have done so we can, so we can assure that they --

Ms. Clarke. So this is already currently a industry practice, or are we at the pilot stage?

Ms. Espinel. It is a practice that many companies that I represent are undertaking. But thank you for saying that. I think what is really important is that we make it a law, not a practice that is required that companies do impact assessments and publicly certify that they have done so in cases of high-risk AI.

Ms. Clarke. Very well. Well, decisions where life-altering opportunities are at stake, whether it is in healthcare, education, employment, housing, or where untested and biased systems can do the most harm. It is essential for companies to evaluate and mitigate the potential risk of a system before it is released. We needs strong rules that prevent companies from releasing systems that replicate and amplify the harmful biases in our society.

I was so glad to see so many of my provisions from the Algorithmic Accountability Act included in the ADPPA last Congress.

Ms. Kak, based on your testimony, I believe you agree that impact assessments are essential to ensure algorithms in AI systems do not perpetuate and amplify bias. What are the most critical parts of such an impact assessment?

Ms. Kak. Thank you so much, Ms. Clarke. I think speaking of report cards, while we are absolutely in favor of impact assessments and the companies should be, of course, evaluating risks, we are worried about a situation where companies are essentially creating their own homework. So while we were in favor of impact assessments, we think for these impact assessments to have teeth and for them not devolve into some superficial checkbox exercise, we need to make sure that there is independent and third party scrutiny of these evaluations.

The question of when these impact evaluations happen are crucial. They need to happen before these systems are publicly released, not just during and after. And the event of the last few months only emphasize that. And, finally, we need to have consequences associated with any harm that are uncovered through these impact assessments, including crucially no path dependency to going ahead.

I think one of the options on the table with an impact assessment needs to be abandoned the system --

Ms. Clarke. So should performance metrics be part of the algorithmic impact assessment? And if so, what would what would those look like, and who should have the input and access to those performance metrics.

Ms. Kak. Absolutely, Ms. Clarke. I don't think I can answer what the performance metric should be in the next 15 seconds. But what I will say is that these performance metrics cannot be set by industry themselves.

And, in fact, there is a very high risk of industry capture when it comes auditing standards. We need to make sure that the terms of the debate are set by the public and not the industry.

Ms. Clarke. Thank you very much, Mr. Chairman, I yield back.

RPTR BRYANT

EDTR CRYSTAL

[2:17 p.m.]

Mr. Bilirakis. Thank you. Thanks for yielding back.

And now we will have Mr. Allen from the great State of Georgia.

You are recognized for 5 minutes of questioning, sir.

Mr. Allen. Thank you, Chair Bilirakis, for convening this hearing.

I want to thank the witnesses for your input today. It has been very informative and we have got a lot to do.

Over the past year we have witnessed a remarkable surge in the popularity of AI, and it has transitioned into the mainstream of America.

This transformation owes much of its success to the widespread adoption of large language models. This evolution is not only attributed to the organic expansion of the user base, but it is also strongly influenced by publicly traded companies leveraging buzzwords to enhance their stock value.

We must develop the ability to discern between marketing exaggerations and actual advancements in development. More than anything, we should use this opportunity to reinforce how important it is for the United States to have a national privacy standard.

Mr. Krikorian, what data are LLMs usually trained off of?

Mr. Krikorian. Thank you for that question.

I mean, LLMs generally are trained on large corpuses of data. Now, the question comes from, where do they get those data from?

Organizations such as OpenAI have used public crawl information, where they are

trained across the entirety of the internet or a decent subset of the internet that has been publicly available for them.

Other organizations, such as Anthropic and others, do a little bit better work when it comes to curating that data coming in under the notion of "garbage in, garbage out," so making sure that good data goes in so that you get good data outwards.

But the training set is usually defined purely by the developer themselves of their own choosing.

Mr. Allen. Do LLM companies pay publishers for using their data to train their models?

Mr. Krikorian. Currently -- and I am not a complete expert on this -- but there is currently a lot of debate, having advised a bunch of the publishers, such as The Atlantic and others. There is no current compensation going back to those publishers.

Those publishers have taken recourse in blocking what their data can be -- how their scrapers can access their data. But currently, as I understand it, no.

Mr. Allen. Mr. Leibowitz, should the owners of LLMs be required to recompense publishers for data their models are trained with?

Mr. Leibowitz. Well, I certainly think as you move forward on AI legislation that should be something that you explore. The perspective of the FTC is always protecting consumers, and certainly consumers need to be protected from abuses in AI.

But I also worked for the film industry for a short period of time, a brief period of time, and of course people need -- whether they are authors or whether they are -- and my wife is a journalist -- or whether they are creators, or whether they are artists -- they deserve some degree of compensation. And so I agree with the premise of the question for sure.

Mr. Allen. Does the FTC already have authority to require these companies to compensate the publishers for using their data?

Mr. Leibowitz. Well, no, the FTC doesn't. I mean, the FTC has -- I would say it has about 80 percent of the authority it needs to protect consumers from fraud and deception and unfairness.

But also the Supreme Court took away its equitable relief authority. So it no longer has the ability, for the most part, to get equitable relief to injured victims or to disgorge profits from corporations that violate the FTC Act.

Most companies try to be on the right side of that. But that would be a thing -- and I know your committee is working on it, giving the FTC equitable relief authority -- that is an important element of it being an effective law enforcement agency.

Mr. Allen. Thank you.

Ms. Kak, should transparency about publishers' content in training datasets be part of the conversation about ethical AI?

Ms. Kak. Absolutely. I think the landscape we are operating within today is that we don't have basic information about what datasets these models were trained on and what practices were taken care of to prevent risks.

And so I think the start of any conversation and basic consumer AI literacy demands that we have answers to these questions before we can move further, and I think a data privacy law would be a strong step in that direction.

Mr. Allen. Okay. I have got about 30 seconds left.

A key issue associated with generative AI systems is the risk they pose for proliferating harmful content, including fake news, misinformation, disinformation, and entrenching bias against conservatives.

Since I am out of time, if you would submit this for the record, and this is all of our panelists today. Do you think that one guardrail that can be attached to generative AI tools is requiring that outputs contain clear prominent sources so that consumers can evaluate an output's trustworthiness.

And if you would respond to that in writing. I am out of time.

And, Chairman, I yield back.

Mr. Leibowitz. But I would say yes.

Mr. Allen. Okay. Thank you.

Mr. Bilirakis. Thank you very much. Appreciate it. And the gentleman yields back.

Now I will recognize Mr. Fulcher for his 5 minutes of questioning.

Mr. Fulcher. Thank you, Mr. Chairman.

And to the panelists, thank you for your time and your expertise and sharing with us today. You probably are aware that some of us are bouncing in and out with multiple committees. So some of this could be repeat questions. And if that is the case, please be forgiving and know that we try not to cover ground twice, but sometimes it just happens.

Mr. Gregg, I am not familiar with your industry that well. In fact, I rarely get a chance even to see movies anymore. But occasionally I do.

And not long ago, I saw the most recent installment of the Indiana Jones series. And at the front end of that movie there is a very young Harrison Ford in there. And I am told that that is AI-generated deepfake recreation.

Whether it was or whether it wasn't, I am not too worried about Harrison. My feeling is he probably got paid and he probably got paid pretty well. But that may not

be the case with other people in your industry, or there might be some concerns.

I would like to ask you a two-point question. One would be, has that issue reached high priority within your industry? And two, what is the proper role of the Federal Government when it comes to regulating that activity, that regeneration or recreation activity?

Mr. Gregg. Thank you very much. That is an excellent question.

The first part, I saw that. I did a movie called "Captain Marvel" where they wanted to use a younger version of me. I would like to use a younger version of me, but they actually had the capability to do so, and they did it. And there was Sam Jackson and I both in the nineties in a blockbuster, anyway, which was a throwback, and that is weird.

But they are able to do it. If you ask me, at times it looked very realistic, at times it didn't. But these are the beginning moments of this. They have been working on it for a while. And the ramifications, as you point out, are terrifying. They are terrifying to us professionally, as I outlined a bit earlier.

But, for example, one of the issues that came up very quickly in the labor action that we are involved in was that there was a request on the part of the corporations that make our content that, for example, the people who -- they are called background performers.

You know a background performer when you see a bad one. Most of the time you don't notice them because they are excellent. They are professionals. They work long hours, and they bring a whole world to life. They make the least money. They work the hardest. And what they wanted to do was scan these people once and then use them in perpetuity in whatever movie they wanted to use them in.

And I think that is a fair jumping-off point. You get to see what -- I heard someone saying that if you want to know where this is going, look what gets incentivized. And it is a way that you can remove the human element of this, because it doesn't demand a new contract, it doesn't need insurance benefits.

And, unfortunately, this also goes to another question, which was, how does this allow us to still be competitive? What it feels like is that the companies that we work for are focused on satisfying growth models and Wall Street.

And since this technology, especially with AI involved, is advancing so quickly, by the time they realize -- my dad, who I lost recently, said a great thing. He said, if you don't get the first moment of truth right, you probably won't see the second one.

By the time they are able to do this and we realize that something terribly artificial has crept into this and that the quality is gone that made our film and television business the best in the world, it will be too late to do anything about it.

Mr. Fulcher. And that is a very good response, and thank you for that.

And just because time is running so short, the second part of that question is, do you have any counsel for us? What is the proper role of the Federal Government in trying to regulate some of that activity?

Mr. Gregg. Thank you.

Because every example I have heard, whether it is about protecting our children, which I have a 21-year-old daughter and I have watched her grow up trying to navigate social media, the algorithm -- and I think AI is just the algorithm on steroids.

Left to the devices of commerce, I don't think we can trust the safety of our children. I don't think we can trust the safety of our performance. We need guardrails, and we need them on the Federal level. As we said earlier this morning, this

takes place across all boundaries instantaneously.

Mr. Fulcher. Thank you.

And very quick, because I am just about out of time, Mr. Krikorian, you may be the best person to ask this question.

The industry Mr. Gregg is in is one thing, and that is terrifying in and of itself to me. Another more terrifying component is what if a person, the President of the United States or whatever, is shown or redepicted as making statements or even declarations that are not accurate.

In the industry, do you have the technology to readily recognize a deepfake or a recreation?

Mr. Krikorian. Thank you for that question.

It is an arms race right now. I can literally create a recreation on my laptop in a couple of hours, and someone can maybe detect it. And their tools are getting better. But without things such as watermarking, without ways of understanding data provenance and others, right now it is an arms race that we are in right now.

Mr. Fulcher. Thank you.

Mr. Chairman, I yield back.

Mr. Gregg. Can I add one last thing, sir?

Mr. Bilirakis. Yes, please, please.

Mr. Gregg. What I failed to answer in the second, what our union is asking for is consideration, compensation, and consent, that there are rights you have as an individual and a performer. Thank you.

Mr. Bilirakis. With regard, Mr. Gregg, when you talked about the 1990s, the deepfake or whatever you want to call it in that particular movie, did you give them

permission to use the 1990s image as opposed to the current image?

Mr. Gregg. Thank you, sir. That is a great question.

Yes. In that case, the question that was put to me -- and it was a fair question, but I think it is an interesting one to bring up -- was if you want to be in this movie then we would like to use -- we would like to de-age you. And we are going to put some spots on you. We are going to give you, thank God, a little bit more hair. And we are going to put you back in the nineties. Or we can cast someone.

So I think a lot of times performers will be in the position of if you want to work you are going to have to go along with these things. And sometimes what we are afraid of is that you will sign off on something that leaves you not protected as the scenarios evolve.

As I said, it was nice to look young again.

Mr. Bilirakis. Yeah. But you want to be compensated for it.

Mr. Gregg. Correct, exactly right. Thank you.

Mr. Bilirakis. Thank you.

The gentleman yields back.

And now I will recognize my friend from Florida. We are also very strong University of Florida football fans.

Mrs. Cammack. Go Gators.

Mr. Bilirakis. She is from Gainesville, Florida. Go Gators.

I recognize you for 5 minutes of questioning.

Mrs. Cammack. I appreciate it, Mr. Chairman.

As the Representative of the Gator Nation and home to the Nation's supercomputer at the University of Florida, this is an interesting topic for us, because we

are investing millions and millions and millions of dollars into R&D. And I think that we are a little bit behind the eight ball in terms of how we manage some of the issues we are coming across.

And I know we have talked at length today about digital twins. So I want to talk a little bit more about the dark side of digital twins. We see the tremendous opportunities for growth, for expediting supply chains, different mechanisms. But can we talk about some of the malicious and possibly deceptive digital twins, how that might be mitigated, detected, et cetera?

I am going to open this up to you, Ms. Espinel.

Ms. Espinel. So I think digital twins, like other forms of AI, can create significant risks. And when we are -- like some of the ones that you have just highlighted -- in high-risk scenarios, in scenarios where AI is either being developed or used in a way that it is having a consequential decision on someone's health, on their education, on their employment, on their civil rights, in those cases we believe that you should pass a law that requires companies to do impact assessments, identify those risks, and then mitigate those risks.

The bill that you passed out of committee last year does have provisions on impact assessments, and so I commend you for having thought that through.

But I think that is an important element of trying to identify and then eliminate and reduce the risks that you are referring to, is by requiring all companies to do those types of impact assessments and then certify that they have done the impact assessment, they have identified the risk, and mitigated that risk.

Mrs. Cammack. You don't think that it should be a third party?

Ms. Espinel. So I think there is a lot of discussion about that. I do think we

need to ensure that it is not a check-the-box exercise. I think we need to make sure they are effective.

Mrs. Cammack. The government is very good at that.

Ms. Espinel. The whole point is to work responsibly.

There are some pieces that are missing right now in order to have a system of third-party audits that would work effectively at the moment.

So, for example, there is no accredited body to do third parties. There are no commonly agreed standards. But there are also groups that are working on those. And we are looking forward to working with many members of the community as those discussions continue.

Ms. Kak. Can I?

Mrs. Cammack. Go ahead.

Ms. Kak. I just had one very quick point, which is that I think we have industry support in general for impact assessments, but some of that support falls away when we say that these impact assessments need to happen before these products are publicly released and if they are unable to mitigate the risks that they shouldn't be put on the market.

So I think that is where the rubber hits the road and why it is very, very important to structure audits or any assessment tools so that they are really kind of -- they have teeth and they are able to introduce reflexivity before the harm has already happened.

Mrs. Cammack. Absolutely.

Ms. Espinel. We believe impact assessments should be happening at all stages, including before products are released, from the companies that I represent.

Mr. Leibowitz. Yeah. And I do too. And I do think third parties is a good idea.

But they have to have teeth. They can't be third parties that are just sort of reinforcing the views of the corporation.

We put Facebook under order when I was at the Commission, and I think Ms. Hone was at the Commission too, and we required a third-party auditor. And what did that lead to? Cambridge Analytica. So you have to be very, very careful, and you have to make sure it has teeth.

The other point I would make is Ms. Espinel's companies are large, important companies that can do mandatory risk assessments, and that is a good thing. But if you don't have a law in place, you might well have a race to the bottom.

Mrs. Cammack. Yep.

Mr. Leibowitz. And a race to the bottom starts with bad actors and it brings good actors down.

Mrs. Cammack. Absolutely.

And staying with you, Mr. Leibowitz, we see the benefits of what a digital twin can do both in the medical space, supply chains, manufacturing, et cetera.

Can you talk about limitations, though?

Mr. Leibowitz. Mitigation?

Mrs. Cammack. Limitations.

Mr. Leibowitz. Oh, limitations.

Well, I mean, look, the current law and current regulatory and enforcement agencies, they are just not a good match for the problems created by AI.

And so you really need to craft a law. And I think that the bill that came out of your committee 53 to 2 last Congress is a really good first step. Not the end, but very much the end of the beginning or the beginning of the end.

Mrs. Cammack. I appreciate that.

And, Mr. Gregg, I have been trying to think of a way to incorporate "Agents of S.H.I.E.L.D." references in my testimony today. I am just not that quick on my feet today.

That being said, I was recently in India. And as I was catching television in and out of the hotel, it was a 24/7 anchor that was AI-generated. We are heading for some very scary times.

And as AI, as Mr. Altman has said, it is not designed to be a human experience. We are getting very close to that. And so I appreciate your efforts to be here and speak to the issue of creativity and talent and some of the issues that we are going to be facing in both the entertainment and news media world and beyond. So thank you.

Ms. Espinel. Could I just make one point?

So I represent the enterprise-facing part of the tech industry. I represent some companies that are big. I represent a number of companies that are quite small.

We believe that companies should be able to do impact assessments whether they are big or small and should be doing them in high-risk cases of AI, but I also would say we think there should be a law passed so it is not just our companies who are doing that voluntarily, but all companies in high-risk situations being required to do that.

Mrs. Cammack. Not to presume that anyone has bad intentions here, but it does seem a bit like the fox in the henhouse. I see government agencies that have to do their own impact assessments on regulations they are trying to force down people's throats, and they don't ever match what the reality is. So I think that a third-party system is probably in order.

Mr. Leibowitz. Yeah. And going back to your earlier point about limitations in

mitigation and what you witnessed in India, that is not commercial. So the FTC has no authority there.

And so that is another reason why you want to look really closely at creating obligations for companies here. And the burden should be on the companies. It shouldn't be on the consumers. That is the problem with certain notice and consent historically. So I can tell this committee is not kicking the can down the road.

Mr. Bilirakis. Mrs. Cammack, I know I can't show any favoritism.

Mrs. Cammack. I know.

Mr. Bilirakis. Even though you are a Florida Gator, I can't. I have got to give the Georgia Bulldog an opportunity.

So, with that, I will recognize the gentleman, Mr. Carter, from Georgia.

Mr. Carter. Well, thank you, Mr. Chairman.

If I may take just a personal moment and compliment my colleague to my left on her choice of red and black today. She looks very attractive in that and I find it to be very attractive. Thank you. Mistake, mistake.

Thank you all for being here. Obviously, this is extremely important. I will tell you this, next to who is going to be the next Speaker, the most prolific subject matter right now is AI on Capitol Hill. That is all anybody is talking about, AI, AI. It is the flavor of the month. It is really the topic of the month. So very important.

Thank you, Mr. Chairman, for allowing me to waive on and thank you for having this hearing, because we need to get this right.

I am real concerned. And the internet, we have still got a law on the books that was created in 1997. And think of everything that has happened between that time and now on the internet, and yet we are still going by 230. I mean, it is just -- we have got to

get this right and we have got to get it right as it evolves. So your help on this is extremely important.

Ms. Espinel, I want to ask you, professionally, I am a pharmacist, so healthcare is extremely important to me. And I have been especially interested in the promise of AI in healthcare.

However, there have been questions that have come about as a result of health data. For example, there are reports of chatbots giving medical diagnoses. I am real concerned about this. And just want to ask you, what kind of privacy gaps are there as it relates to health data?

Ms. Espinel. Well, I would just say, as the daughter and as the sister of doctors, I share that concern.

Now, I think in terms of -- that is a great example of a high-risk use of artificial intelligence. It is impacting someone's health. There are other high-risk uses, but there could not be a better example.

And I think when AI, like a chatbot, is being used, developed or used, and it is going to have an impact in a high-risk situation like someone's health, then there do need to be -- there need to be limitations on that. There need to be obligations to do impact assessments. And if it is going to create a risk, such as offering a diagnosis inappropriately, then that can't happen.

And the companies need to have processes in place where they are identifying that that could happen and then addressing it. And by addressing it, I mean trying to ensure that it does not happen.

Mr. Carter. Mr. Leibowitz, do you want to?

Mr. Leibowitz. Yeah. I was just going to add a couple of points.

So one is, the benefits in healthcare of artificial intelligence could be enormous in a variety of areas, but there is also, as you point out, a big gap.

We have HIPAA, but there is a lot of sensitive information that is outside of HIPAA. It is what you are looking at on the internet if you are trying to find a medical diagnosis. And companies shouldn't be collecting that information and marketing it and selling it and transferring it without your permission.

And so that is a sensitive category of information that your legislation on privacy would require affirmative express consent for. In other words, it can't be taken by consumers without clearly them authorizing it.

Mr. Carter. Well, I can see where it can be extremely beneficial.

Mr. Leibowitz. Yes.

Mr. Carter. But I can also see where it can be extremely dangerous.

Ms. Kak. Mr. Carter, to your question.

Mr. Carter. Yes, please.

Ms. Kak. I have a small point, because I think privacy and competition are actually two sides of the same coin. And another practice we are seeing in the healthcare space is we are seeing Big Tech companies shore up medical databases, particularly those that are rich in patient data.

And so one of the things that we are really concerned about is we think there needs to be stricter review of mergers in this space, because Big Tech is really at a perch where they can shore up --

Mr. Carter. God bless you. I have been on mergers in this space ever since I have been here. And thank you.

Ms. Kak. No, this is absolutely --

Mr. Carter. And that is something we have got to be concerned about.

Ms. Kak. Absolutely. And FTC Commissioners Slaughter and Bedoya have also sort of sounded the alarm in the Amazon One Medical case, that this is just going to lead to Big Tech entrenching their data advantage. And we think data minimization tools are a good antidote there as well.

Mr. Carter. Good. Good.

Anyone else? This is my area and where I am really interested. Any other comments?

Mr. Gregg?

Mr. Gregg. I haven't even played a doctor on TV.

Mr. Carter. Really? Well, let me ask you this. What are the effects of misleading and deceptive content on consumer protection in the entertainment industry? I know that is kind of what you are involved in. But what kind of misleading and deceptive content on consumer protection have we -- do we need to be aware of and need to be concerned with?

Mr. Gregg. I think I understand the question. Content in terms of fakes?

Mr. Carter. Yes, yes. Because I am such a trusting person, I don't know what the difference is and whether it is real or it is not.

Mr. Gregg. Yes. Well, fortunately for you, you weren't here earlier when I was talking about the terrifying inappropriate images that were sent to me of me doing things that, as far as I know of, I have never done and would never do. And that is disturbing to have out there, with a daughter who is online.

But it is just an example of -- I think this goes -- this is where my business transcends out into your business, which is, if they can make me appear doing something

that I would never do, it is very dangerous to think that they could make you, the Speaker if we ever get one, the President, to say things, especially in really tense moments as we are going through right now with what is going on in the Middle East.

The way things turn around so quickly, first of all, there is so much mistrust people will have -- if we tell them that wasn't real, they won't believe that either, that what is being eroded is truth.

So I have said the other things I think about it is taking the soul out of the art form that I perform in, but I also think the fingers of it reach way, way more broadly.

Mr. Carter. Right. And, again, Mr. Chairman, thank you for indulging with me.

But this is why this is so important. We need to get this right. And I think the role that we play in Congress is going to be extremely important, but the role that the private sector has is going to be even more important.

So thank you. Thank you all.

Mr. Bilirakis. I appreciate it very much.

I just want to thank you all, because I think we are going to make a good bill better due to your testimony and your input today.

Please don't hesitate to come to our offices and offer suggestions, okay? Again, we had a limited amount of time and I appreciate your patience today.

But, again, this is a very important issue. As my fellow SEC member -- I went to the University of Florida -- said, it is so important.

We have got a real chance against you. I don't know, Buddy, I think we got a shot. We will see. The way we played last week was very encouraging.

But, in any case, I want you all to know our door is open to you.

And so, with that, I am going to say I am going to ask unanimous consent to insert

in the record the documents included on the staff hearing documents today.

Without objection, so ordered.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Bilirakis. And I remind members that they have 10 business days to submit questions for the record. And I ask the witnesses to respond to the questions promptly. Members should submit their questions by the close of business day on November 1st.

So, without objection, the subcommittee is adjourned.

[Whereupon, at 2:45 p.m., the subcommittee was adjourned.]