ADVANCES IN DEEPFAKE TECHNOLOGY

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

FIRST SESSION

NOVEMBER 8, 2023

Serial No. 118–74

Printed for the use of the Committee on Oversight and Accountability

Available on: *govinfo.gov*
oversight.house.gov or
docs.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE
54–071 PDF WASHINGTON : 2024

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

JAMES COMER, Kentucky, Chairman

JIM JORDAN, Ohio
MIKE TURNER, Ohio
PAUL GOSAR, Arizona
VIRGINIA FOXX, North Carolina
GLENN GROTHMAN, Wisconsin
GARY PALMER, Alabama
CLAY HIGGINS, Louisiana
PETE SESSIONS, Texas
ANDY BIGGS, Arizona
NANCY MACE, South Carolina
JAKE LATURNER, Kansas
PAT FALLON, Texas
BYRON DONALDS, Florida
KELLY ARMSTRONG, North Dakota
SCOTT PERRY, Pennsylvania
WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
LISA MCCLAIN, Michigan
LAUREN BOEBERT, Colorado
RUSSELL FRY, South Carolina
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri

JAMIE RASKIN, Maryland, *Ranking Minority Member*
ELEANOR HOLMES NORTON, District of Columbia
STEPHEN F. LYNCH, Massachusetts
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
RO KHANNA, California
KWEISI MFUME, Maryland
ALEXANDRIA OCASIO-CORTEZ, New York
KATIE PORTER, California
CORI BUSH, Missouri
JIMMY GOMEZ, California
SHONTEL BROWN, Ohio
MELANIE STANSBURY, New Mexico
ROBERT GARCIA, California
MAXWELL FROST, Florida
SUMMER LEE, Pennsylvania
GREG CASAR, Texas
JASMINE CROCKETT, Texas
DAN GOLDMAN, New York
JARED MOSKOWITZ, Florida
RASHIDA TLAIB, Michigan

MARK MARIN, Staff Director
JESSICA DONLON, Deputy Staff Director and General Counsel
RAJ BHARWANI, Senior Professional Staff Member
LAUREN LOMBARDO, Senior Policy Analyst
PETER WARREN, Senior Advisor
MALLORY COGAR, Deputy Director of Operations and Chief Clerk

CONTACT NUMBER: 202-225-5074

JULIE TAGEN, Minority Staff Director

CONTACT NUMBER: 202-225-5051

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

NANCY MACE, South Carolina, Chairwoman

WILLIAM TIMMONS, South Carolina
TIM BURCHETT, Tennessee
MARJORIE TAYLOR GREENE, Georgia
ANNA PAULINA LUNA, Florida
CHUCK EDWARDS, North Carolina
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
Vacancy

GERALD E. CONNOLLY, Virginia *Ranking Minority Member*
RO KHANNA, California
STEPHEN F. LYNCH, Massachusetts
KWEISI MFUME, Maryland
JIMMY GOMEZ, California
JARED MOSKOWITZ, Florida
Vacancy

C O N T E N T S

WITNESSES

INDEX OF DOCUMENTS

ADVANCES IN DEEPFAKE TECHNOLOGY

Wednesday, November 8, 2023

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY
SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION
Washington, D.C.

The Subcommittee met, pursuant to notice, at 3:41 p.m., in room 2154, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Timmons, Burchett, Langworthy, Burlison, and Connolly.

Ms. MACE. Good afternoon, everyone. The Subcommittee on Cybersecurity, Information Technology, and Government Innovation will come to order.

Welcome, everyone, and without objection, the Chair may declare a recess at any time.

I recognize myself for the purpose of making an opening statement.

Good afternoon, and welcome to this hearing of the Subcommittee on Cybersecurity, Information Technology, and Government Innovation.

The groundbreaking power of artificial intelligence is a double-edged sword. That is nowhere more evident than in AI's capacity to generate realistic-looking images, audio, and video. The latest AI algorithms can be used to make synthetic creations nearly indistinguishable from actual faces, voices, and events. These creations are referred to as deepfakes.

Deepfakes can be put to a variety of productive uses. They are used to enhance video games and other forms of entertainment, and they are being used to advance medical research as well, but deepfake technology can also be weaponized and cause great harm. It can be used to make people appear to say or do things that they have not said or done. It can be used to perpetuate various crimes, including financial fraud and intellectual property theft. It can also be used by anti-American actors to create national security threats, and these are not hypothetical harms.

It must be me today.

OK. A few weeks ago, AI-generated pornographic images of female students at a New Jersey high school were circulated by male classmates. A company that studies deepfakes found more than 90 percent of deepfake images are pornographic. Last month, the at-

torneys general of 54 states and territories wrote to congressional leaders urging they address how AI is being used to exploit children, specifically through the generation of child sexual abuse material, or CSAM, pronounced "Cee-Sam." They wrote, "AI can combine data from photographs of both abused and non-abused children to animate new and realistic sexualized images of children who do not exist but may resemble actual children. Creating these images is easier than ever," the letter states, "as anyone can download the AI tools to their computer and create images by simply typing in a short description of what the user wants to see."

Falsified videos and photos circulating on social media are also making it difficult to separate fact from fiction in conflicts taking place around the world. Videos purportedly taken from the ground in Israel, Gaza, and Ukraine have circulated rapidly around on social media, only to be proven inauthentic. One AI-generated clip showed the President of Ukraine urging troops to put down their arms. I am not interested in banning all synthetic images or videos that offend some people or make them feel uncomfortable, but if we cannot separate truth from fiction, we cannot ensure our laws are enforced or that our national security is preserved. And there is more insidious danger that the sheer volume of impersonations and false images we are exposed to on social media lead us to no longer recognize reality when it is staring us right in the face.

Bad actors are rewarded when people think everything is fake, thus called the liar's dividend. The classic case of the liar's dividend is the very real hunter Biden laptop, which many in the media and elsewhere falsely attributed to Russian disinformation, but the risk from deepfakes can be mitigated. We will hear about one such effort today being pursued by a partnership of tech companies interested in maintaining a flow of trusted content. Voluntary standards can enable creators to embed content provenance data into an image or video, allowing others to know if the content is computer generated or has been manipulated in any way.

Our witnesses today will be able to discuss these standards, along with other ideas, for addressing the potential harms caused by deepfakes. With that, I would like to yield to the Ranking Member of the Subcommittee, my friend, Mr. Connolly.

Mr. CONNOLLY. Thank you, Madam Chairwoman, and thank you for having this hearing. Very timely. I will begin by noting our disappointment on the Minority side, yet again, the lack of a hearing on the scorecard for implementation of FITARA. This Committee initiated that legislation, created that scorecard, has had 15 hearings—a record for Congress—and it has produced over $25 billion of savings. We believe strongly that we need to continue that oversight and continue to press the executive branch for progress. I would note that until now, that effort over the last 7 years has been completely bipartisan. I have worked with my colleagues on the other side of the aisle—Mr. Meadows, Mr. Issa, Mr. Hice, Mr. Hurd—to make this happen, and we have always collaborated in a bipartisan way to make it happen. So, I hope we can revisit that issue and continue to make progress and keep what I think is a very proud record by this Subcommittee and by the full Committee in holding the executive branch's feet to the fire when it comes to

IT modernization, updating cybersecurity encryption, and moving to the cloud.

[Slides shown]

Mr. CONNOLLY. With that, with respect to this hearing, when most people hear the term "deepfake," this image may jump to mind. While images like this, His Holiness, Pope Francis, in a puffy coat, seems innocuous, most are, as the Chairwoman just indicated, quite insidious. Take the AI-generated image, for example, the Gaza image on the screen. Since the armed conflict between Israel and Hamas first broke out, false images created by generative technology have proliferated throughout the internet. As a result, these synthetic images have created an algorithmically driven fog of war, making it significantly more difficult to differentiate between truth and fiction. Just last year, at the outset of Russia's invasion of Ukraine, a fabricated video of Ukrainian President Zelensky calling for Ukrainian soldiers to lay down their weapons, also referenced by the Chairwoman, circulated on social media very widely. It was a deepfake, but thanks to Ukraine's quick response to Russian disinformation, it was quickly debunked. Welcome to the new frontier of disinformation.

Politics are one realm of deepfakes, but let us look at some numbers. According to one study, 96 percent of deepfake videos are of non-consensual pornography—96 percent. Another report confirmed that deepfake pornography almost exclusively targets and harms young women. Knowing this, it should be no surprise that the very first deepfake ever created depicted the face of a famous female celebrity superimposed onto the body of an actor in a pornographic video. These kinds of manipulated videos are already affecting students in our schools. In one instance, a group of high school students in New Jersey used the images of a dozen female classmates to make AI pornography. This is wrong. It threatens lives and self-esteem among young people, and it needs to be stopped.

Earlier this year, Ranking Member, Joe Morelle, introduced a bill called the Preventing Deepfakes of Intimate Images Act. The bill bans non-consensual images. The order instructs the Secretary of Commerce—whoops, I am sorry—of sharing synthetic intimate images and creates additional legal courses of action for those who are affected. I am a co-sponsor of that legislation and urge all of my colleagues to join us in this important effort.

Congress must not shy away from preventing harmful proliferation of deepfake pornography, but it is not just deepfake videos that we have to worry about. With AI, scammers have the ability to easily create audio that mimics a person's voice, matching, age, gender, and tone. Thousands of Americans are scammed over the telephone every year using this very technology, and deepfake capabilities further exacerbate the problem. So, what can we do? AI image detecting tools are being developed and used to help verify the authenticity of machine-generated images. Other tools place watermarks on AI-generated media to indicate that the media is synthetically created.

While these tools improve and evolve, both the public and the private sector must cooperate to educate the public on where these tools are and how to use them. Government and the private sector must collaboratively highlight the dangers and consequences of

deepfakes and teach how to combat this misinformation and its abuse. Private developers must implement policies that preserve the integrity of truth and to provide transparency to users. That is why I joined the letter, led by Representative Kilmer and the New Democratic Coalition AI Working Group, that requests leaders of prominent, generative AI and social media platforms to provide information to Congress outlining efforts to monitor, identify, and disclose deceptive synthetic media content, and the public sector is already taking bold, consequential steps toward collaboration and comprehensive solutions.

I applaud the efforts of the Biden Administration to secure commitments from seven major AI companies to help users identify when content is, in fact, AI generated and when it is not. The Biden Administration took a resolute and unprecedented step last week when it issued its executive order on artificial intelligence. The sweeping executive order speaks directly to the issues we seek to examine today. It leans on tools, like watermarking, that can help people identify whether what they are looking at online is authentic as a government document or tool of disinformation. The order instructs the Secretary of Commerce to work enterprise-wide to develop standards and best practices for detecting fake content and tracking the provenance of authentic information. I trust this Subcommittee will conduct meaningful oversight of these efforts because we, as a Nation, need to get this right.

I am proud that the Administration has taken the first step in performing its role as a global leader in addressing generative technology. I also look forward to hearing more today about existing and evolving private sector solutions and suggestions. We already know Congress must continue to fund essential research programs that support the development of more advanced and effective deepfake detection tools. Funding for research through DARPA and the National Science Foundation is critical. That requires a fully funded government. I once again urge all of my colleagues on this and the other side of the aisle to fulfill our constitutional duty and work with us to pass a bipartisan, long-term funding agreement.

I thank the Chairwoman, Ms. Mace, for holding this hearing and emphasizing the harm of deepfakes and disinformation, and I look forward to any legislative action that may follow this endeavor. I yield back.

Ms. MACE. Thank you, Mr. Connolly. Today, I am pleased to introduce our witnesses for today's hearing. Our first witness is Mr. Mounir Ibrahim, Executive Vice President of Public Affairs and Impact at Truepic. I would like to next introduce Mr. Langworthy to introduce the second witness.

Mr. LANGWORTHY. Thank you very much, Madam Chair. I am pleased to have the opportunity to introduce our witness from Western New York. Dr. David Doermann is the interim Chair of the Department of Computer Science and Engineering at the State University of New York at Buffalo. He is also a professor of empire innovation and the Director of the Artificial Intelligence Institute at UB. Prior to UB, Dr. Doermann was a program manager at the Defense Advanced Research Projects Agency, or DARPA, where he developed and oversaw $150,000,000 in research funding in the areas of computer vision, human language, and voice analytics

technologies. Dr. Doermann is a leading researcher and innovative thinker in the areas of document image analysis and recognition. Welcome to the hearing, Dr. Doermann. We look forward to your testimony today, and I yield back.

Ms. MACE. Thank you. Our third witness is Mr. Sam Gregory, executive director of WITNESS, and our fourth witness today is Mr. Spencer Overton, professor of law at George Washington University School of Law. Welcome, everyone, and we are pleased to have you here this afternoon.

Pursuant to Committee Rule 9(g), the witnesses will please stand and raise your right hands.

Do you solemnly swear or affirm that the testimony you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

[A chorus of ayes.]

Ms. MACE. Let the record show the witnesses all answered in the affirmative. We appreciate all of you being here today and look forward to your testimony.

Let me remind the witnesses that we have read your written statements, and they will appear in full in the hearing record. Please limit your oral statements to 5 minutes. As a reminder, please press the button on the microphone in front of you so that it is on, and the Members can hear you. When you begin to speak, the light in front of you will turn green. After 4 minutes, the light will turn yellow. When the red light comes up, your 5 minutes has expired, and we would ask that you please wrap it up.

I would like to recognize Mr. Ibrahim to please begin his opening statement.

STATEMENT OF MOUNIR IBRAHIM
VICE PRESIDENT OF PUBLIC AFFAIRS AND IMPACT TRUEPIC

Mr. IBRAHIM. Thank you, Chairwoman Mace, Ranking Member Connolly, and Members of this Subcommittee for the opportunity to brief today. My name is Mounir Ibrahim, Executive Vice President for Truepic, a technology company that focuses on digital content transparency and authenticity. Prior to my time at Truepic, I was a Foreign Service officer with the U.S. Department of State. My time as a U.S. diplomat was one of the greatest honors of my life and led me to my work today.

I was posted at the U.S. Embassy in Damascus at the start of the Arab Spring. I saw protesters risk their lives, being beaten and attacked in front of me, as they attempted to document the violence with smartphones. It was there I saw the power of user-generated content. Later, as an advisor to two different U.S. permanent representatives to the United Nations, I saw similar images from conflict zones around the world enter into the U.N. Security Council, but regularly undermined by countries, critics, and bad actors that wanted to undermine reality by simply claiming those images were fake. Today, that strategy, as the Congresswoman noted, is referred to as the liar's dividend, and it is highly effective, simply claiming user-generated content is fake.

In my opinion, in addition to the horrible, non-consensual pornographic threat that we have from generative AI, the liar's dividend

is one of the biggest challenges we have because we have digitized our entire existence. Government, business, and people all rely on what we see and hear online to make decisions. We need transparency and authenticity in that content to make accurate decisions. There is no silver bullet to transparency or authenticity online, but there is growing consensus that adding transparency to digital content so that content consumers—the people who are seeing those images and videos—can tell what is authentic, what is edited, or what is synthetic, will help mitigate the challenges.

A lot of this work is taking place by a coalition of organizations known as the Coalition for Content Provenance and Authenticity, C2PA, by which Truepic is a proud member. The C2PA developed the world's first open standard for digital content provenance, which is often referred to as content credentials. The basic concept of provenance is attaching the fact or history of that image, that video, that audio that you are interacting with online to the file itself, so the content consumer is informed of the artifacts associated with that, like time, date, how it was created, how it was edited, et cetera. The standard is interoperable, which is critical, so digital content can flow from one platform, one device to another so as long as they align to the same standard.

Truepic supports the C2PA because we believe interoperability is critical to help mitigate the challenges that you all laid out today. Our technology and our approach boils down into two areas: we help secure what is, in fact, authentic and captured from a smartphone, and we help add transparency to a synthetic or generative piece that is created from a platform.

From the authentic side, we created a technology called Secure Controlled Capture. It is used by hundreds of businesses every day, ranging from Equifax to Ford Motor Company, to add transparency into their operations. It has also been used in 150 countries. We have deployed this technology on the ground in Ukraine with Microsoft to help USAID partners document destruction to cultural heritage and national infrastructure. On the generative AI side, the C2PA standard has been recognized by the Partnership for AI as one of the lead disclosure mechanisms for generative AI. We are also a proud supporter of the Partnership for AI, and we strive to work toward this goal.

In April, we worked with Nina Schick, an author, and Revel.ai, to launch the world's first transparent deepfake so when you actually see the video, you see the content credentials and know it is, in fact, generated by AI. This past month, we launched two other partnerships with Hugging Face to democratize these tools to add content credentials so anyone can use them on their open-source models, and with Qualcomm, the chipset manufacturer. We think that is a watershed innovation because generative AI is going to move to your smartphone, and this chipset has this transparency technology added to it. It is worth noting that it is not only Truepic working on this. Microsoft, Adobe, Stability AI have all either launched products or made commitments to add the same transparency. This is a growing ecosystem.

In closing, if possible, I would like to offer some thoughts on how government might help mitigate these AI challenges with transparency and authenticity in mind. First, government has a unique

platform, and I applaud you for having this hearing. Events like this will raise awareness and help educate the public and give an opportunity to ask the right questions. Second, legislation can be powerful. We have seen in the National Defense Authorization Act, the bipartisan Deepfake Task Force Act, and the recent Executive Order Section 4.5, all of which point to transparency and authenticity in digital content. We have also seen it abroad in the U.K. and the EU. Finally, government should consider how it can use content credentials to authenticate its own communications and prevent constituents from being deceived, and also reap the same benefits that the private sector does in cost reductions, risk reductions, and fraud reductions.

Thank you for your time, and I welcome any questions.

Ms. MACE. Thank you. I now recognize Mr. Doermann to please begin his opening statement.

STATEMENT OF DR. DAVID DOERMANN
INTERIM CHAIR
COMPUTER SCIENCE AND ENGINEERING
STATE UNIVERSITY OF NEW YORK AT BUFFALO

Mr. DOERMANN. Chairwoman Mace, Ranking Member Connolly, and honorable Members of Congress, I appreciate the opportunity to testify before you today on the pressing issue of deepfake technology, creating and distributing computer-generated images, and voice cloning.

In 2014, only a decade ago, when DARPA began the Media Forensics Program, commonly known as MediFor, the primary goal was to detect and characterize image manipulation at scale. This was consistent with DARPA's mission of preventing strategic surprise. Although we imagined a world where our adversaries would become better at manipulating images, few imagined the pace at which automated manipulation would develop and the impact the technology would have on our society as a whole. The introduction of generative adversarial networks, or GANs, kicked off a plethora of tools that can generate images of people and objects that do not exist, synthesize speech that clones voices of others, implements real-time puppeteering to control talking heads, and, as we hear most, the ability to generate deepfake videos. The surprise we missed perhaps is the automated tools that are becoming more accessible and user friendly. They require a lot less data and a lot less technical expertise. Open-source software can be downloaded today and run by any one of us on a commodity laptop.

As these technologies advance at an unprecedented rate, it is crucial to recognize the potential for both positive and negative implications. We hear its use at both ends of the spectrum every week. This week we heard about AI being used to finish a new Beatles song and, as we have heard from the Ranking Member and Chairwoman, that a group of students in a New Jersey high school used it to generate pornographic videos of their classmates. Despite the President's executive order and the testimony of our thought leaders and business leaders, we are not moving fast enough to curtail the continued damage this technology is doing and will do as it evolves. Not only has it been used for non-consensual pornography, cyberbullying, and harassment, causing great harm to indi-

viduals, but the potential for national security implications are grave. Deepfakes can be used to impersonate government officials, military personnel, or law enforcement, and, in general, lead to misinformation and potentially dangerous situations.

Today, this is no longer a problem that can be solved by simply detecting and removing generated content from our social media and content provider sites. I urge you to consider legislation and regulation to address the misuse of deepfake technology as a whole.

Striking the right balance between free speech and safeguards to protect against malicious uses of deepfakes is essential. First and foremost, public awareness and digital literacy programs are vital to helping individuals learn about the existence of deepfakes and how to ensure that they do not propagate this type of misinformation. It may seem obvious that people want to know what type of information is being generated, and you would hope that they would be able to hold it upon themselves not to spread it, but we find that that is not the case. We should consider including school media literacy education and promote critical thinking.

Collaboration between Congress and technology companies is essential, and I am glad to see that that is happening to address the challenges posed by deepfakes. Tech companies should be responsible for developing and implementing the policies to detect and mitigate this type of content, including what we were hearing today, on their platforms and sharing, most importantly, what they learn with others. We have addressed this type of a problem with our cybersecurity, and we should be doing that same thing with our misinformation. More robust privacy and consent laws are needed to protect individuals from using their likeness and voice in deepfake content without their permission, and continued research and development in AI deepfake technology are necessary, as is funding to counter deepfake misuse.

We have created these problems, but I have no doubt that if we work together, we are smart enough to figure out how to solve them. I look forward to taking your questions.

Ms. MACE. Thank you. I now recognize Mr. Gregory to please begin his opening statement.

STATEMENT OF SAM GREGORY
EXECUTIVE DIRECTOR
WITNESS

Mr. GREGORY. Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, I am Sam Gregory, Executive Director of the human rights organization, WITNESS. Since 2018, WITNESS has led a global effort—Prepare, Don't Panic—to inclusively prepare for deepfake and related synthetic media and generative AI technologies. The capabilities and uses of deepfakes have often been overhyped, but with recent shifts, the moment to address them more comprehensively has come. First, I will cover technological advances.

Commercialization and accessibility characterized changes in the last year. Deepfake technologies are now available in widely used consumer tools, not just niche apps. Furthermore, they are easy to use and, particularly for audio and image, can be instructed with plain language and require no coding skills. Realistic image genera-

tion has improved dramatically in its quality and customization in a year. With widely available audio cloning tools, 1 minute of audio is enough to fake a voice. While video remains harder to do in complex real-world scenarios, consumer apps can swap an individual's face onto another's body, strip the clothing from a woman's body. Matching lip movements to a new audio track in a video is being demoed by Google, and live deepfakes are feasible. As a result, we are seeing an increased volume and ease in creating variations of realistic synthetic photos, audio, and, eventually, video of specific real individuals and contexts.

I would like to flag four future trends. These are increasing ease in instructing these tools in plain language; two, more ability to tailor outputs; three, more realistic outputs; and four, eventually similar advances in video to what we now see in audio and images.

Moving on to the risks and harms, deepfakes are causing harms in the U.S. and globally, with disproportionate impacts on groups already at risk of discrimination or vulnerable to offline harms. Women and girls are widely targeted with nonconsensual sexual images, and this problem is escalating. AI-generated child sexual abuse material, CSAM, is increasing. Simulated audio scams are proliferating, as are misuses of AI audio in political contexts. My organization frequently sees claims of AI generation used to muddy the waters and dismiss critical real content, while actors and others have their likenesses stolen to use in non-satirical commercial contexts.

Political processes are likely to be impacted by deepfakes, and recent polls find the American public is fearful of their impact. However, it is unreasonable to expect individuals to spot deceptive, yet realistic, deepfake imagery and voices. Guidance to look for the six-fingered hand or inspect visual errors in a pope in a puffer jacket does not help in the long run. Meanwhile, under resourced newsrooms and community leaders across the political spectrum are under pressure and do not have access to reliable tools that can detect deepfakes. That is because deepfake detection efforts are not yet reliable at scale or across multiple different ways of creating deepfakes, nor are there widely shared methods to clearly indicate how AI was used in creating content.

This leads me to what Congress should consider, to address these advances in technology and accompanying misuses. First, enact Federal legislation around existing harms, including nonconsensual sexual content and the growing use of generative AI and CSAM. Incorporating broad consultation with groups working on these existing harms while safeguarding constitutional and human rights would help you craft appropriate steps. Second, since people will not be able to spot deepfake content with their eyes or ears, we need solutions to proactively add and show the provenance of AI content and, if desired and under certain circumstances, human-generated content. Provenance, such as the C2PA standard mentioned before, means showing people how content and communications were made, edited, and distributed, as well as other information that explains the recipe. The best choices here will go beyond binary "yes"/"no" labels.

Overall, these transparency approaches provide a signal of AI usage, but they do not, per se, indicate deception and must be ac-

companied by public education. Critically, these approaches should protect privacy and not collect, by default, personally identifiable information. For content that is not AI generated, we should be wary of how any provenance approach can be misused for surveillance and stifling freedom of speech.

My third recommendation is on detection. Alongside indicating how the content we consume was made, there is a continuing need for after-the-fact detection for content believed to be AI generated. From witnesses' experience, the skills and tools to detect AI-generated media remain unavailable to the people who need them the most, including journalists, rights defenders, and election officials domestically and globally. It remains critical to support Federal research and investment in this area to improve detection overall and to close this gap. It should be noted that both provenance and detection are not as relevant to nonconsensual sexual deepfakes where a real versus fake is often beside the point since the harm is caused in other ways. We need other responses to that.

As a general and final statement for both detection and provenance to be effective in helping the public to understand how deepfake technologies are used in the media we consume, we need a clear pipeline of responsibility that includes all the technology actors involved in the production of AI technologies more broadly, from the foundation models, to those designing and deploying software and apps, to the platforms that disseminate content. Thank you for the opportunity to testify.

Ms. MACE. Thank you. I will now recognize Mr. Overton to begin your opening statement.

STATEMENT OF SPENCER OVERTON
PROFESSOR OF LAW
GEORGE WASHINGTON SCHOOL OF LAW

Mr. OVERTON. Chairwoman Mace, Ranking Member Connolly, Subcommittee Members, thanks for inviting me to testify. My name is Spencer Overton. I am a professor at GW Law School and GW's Equity Institute. My research focuses on civil rights law, democracy, and disinformation.

Now, while deepfake technologies offer many benefits, they also threaten democratic values, and they produce harms disproportionately borne by women and communities of color. Nina Jankowitz, for example, is a 34-year-old researcher. She specializes in state-sponsored disinformation and gendered online abuse. Earlier this year, she found out she was featured in at least three synthetic videos that appear to show her engaging in sex acts. Now, she wrote about these videos.

She wrote, quote, and I will just use her words, "Although they may provide cheap thrills for the viewer, their deeper purpose is to humiliate, shame, and objectify women, especially women who have the temerity to speak out. Users can also easily find deepfake porn videos of the singer, Taylor Swift; the actress Emma Watson; and the former Fox News host, Megyn Kelly. Democratic officials, such as Kamala Harris, Nancy Pelosi, Alexandria Ocasio-Cortez, and Republicans Nikki Haley and Elise Stefanik, and countless other prominent women. By simply existing as women in public life, we have all become targets, stripped of our accomplishments,

our intellect, and our activism, and reduced to sex objects for the pleasure of millions of anonymous eyes."

Deepfake pornography accounts for, as you all said, over 90 percent of all deepfake videos online. Women are featured as the primary subjects of 99 percent of deepfake pornography, while men are the primary subjects in only 1 percent. Nonconsensual deepfake pornography does not simply hurt women's feelings. It is an antidemocratic form of harassment designed to silence and undermine public confidence in women as legitimate public policy leaders. Deepfake technology is also fueling racial harassment. Earlier this year, a deepfake video showed a middle school principal saying that Black students should be sent back to Africa, calling them monkeys and the "N" word, and threatening gun violence. Userfriendly and affordable, deepfake technology could allow bad actors to be even more effective in dividing Americans and undermining democracy.

So, when we think back to 2016, the Russians, we know, set up social media accounts pretending to be Black Americans. They posted calls for racial justice, developed a following, and then, just before Election Day, they targeted ads at Black users, encouraging them to boycott the election and not vote. Now today, in this world, the Russians or domestic bad actors could spark social upheaval by creating deepfake videos of a white police officer shooting an unarmed Black person. Indeed, earlier this year, just before Chicago's mayoral election, a deepfake video went viral of a candidate casually suggesting that regular police killings of civilians was normal, and that candidate lost. Now, the private sector is definitely important, but the market alone will not solve all of these problems. Initial studies, for example, show that deepfake detection systems have higher error rates for videos showing people of color.

In conclusion, as deepfake technology becomes more common, women and communities of color bear increasing burdens. Members of Congress should come together, understand these emerging challenges, and really take action to protect all Americans and our democracy from the harms. Thank you.

Ms. MACE. Thank you. I would now like to recognize myself for 5 minutes for questioning, and my first question is for every member of the panel. So, let us not do 5 minutes each because we only have 5 minutes today, so if you could just keep it brief.

I am very concerned about deepfake technology being weaponized against women and children. Mr. Overton, as you made your point, the overwhelming majority of deepfakes circulating are pornographic. Most of these involve images of women. Some are images of children. As a woman in a public position and the mother of a teenage daughter, it is alarming to me how easy it has become to create and distribute realistic pornographic images of actual women and girls. These images can cause lifelong and lasting humiliation and harm to that woman or girl. So, what can we do to protect women and children from being abused in this manner? Mr. Ibraham, and we will just go across the panel.

Mr. IBRAHIM. Thank you, Congresswoman. Indeed, this is, as everyone noted, the main issue right now with generative AI, and there are no immediate silver bullets. So, several colleagues have noted media literacy and education and awareness. Also, a lot of

these nonconsensual pornographic images are made from open-source models. There are ways in which open-source models can potentially leverage things, like provenance and watermarking——

Ms. MACE. Mm-hmm.

Mr. IBRAHIM [continuing]. So that the outputs of those models will have those marks, and law enforcement can better detect, better trace down and take down such images. Those are just some thoughts to begin with.

Ms. MACE. Thank you. Mr. Doermann?

Mr. DOERMANN. One of the challenges that we have is that we do not have a culture where a lot of these things are unacceptable. In the case of New Jersey, I understand that there were parents even that said boys will be boys. These are not the kinds of things that we have today that should allow these types of things to progress from a technology point of view. We do have the ability to do partial image search. As another panelist here said, we have the original source material, and we could check that something has been manipulated in that way. It just requires that we do it at scale. It is not an easy solution, but those are the types of things that we have to think sort of outside the box.

Ms. MACE. Mr. Gregory? Microphone.

Mr. GREGORY. There is a patchwork of state laws at the moment. There is no Federal law at the moment that would protect women and girls. We need to make it clearer where there is individual liability that can be applied here. I should also note that recent research indicates how easy it is to find these deepfakes on search engines. Just type in a name plus "deepfakes," and you will come up with a deepfake of a public figure. So, addressing the responsibility of platforms within to make sure that, it is less easy to do that because at the moment, it is very hard for individuals to chase down all the examples of their deepfakes online with individual requests.

Ms. MACE. Mr. Overton?

Mr. OVERTON. The proposed Preventing Deepfakes of Intimate Images Act is a good start. Having both criminal and civil penalties is important. Not having overly burdensome intent requirements to establish a violation and also focusing on both creators and distributors, those are some important factors.

Ms. MACE. Thank you. My next question is about laws. Do we need changes in law enforcement practice? And there are revenge porn laws, as an example, that do not cover deepfakes necessarily. On the Federal level, 15 U.S. Code, Section 6851—I happened to be reading about it today

-is civil action related to intimate images and videos, but it relates to real images and videos, not to deepfakes. And so, I see a huge gap in law and even law enforcement practice, and what are your thoughts on that? Mm-hmm. We have a minute, so everybody gets, like, 20 seconds.

Mr. IBRAHIM. I would encourage examination of laws and what generative AI platforms and models can do——

Ms. MACE. Mm-hmm.

Mr. IBRAHIM [continuing]. To pre-mark their content output so that we can better effectively take things down and track them.

Mr. DOERMANN. I think I am not a legal scholar, but, you know, it is my understanding that, you know, the same way as our first generative algorithms targeted very high-level individuals, it might not be just pornographic. It might be just showing somebody in another type of compromising situation.

Ms. MACE. Mm-hmm.

Mr. DOERMANN. We need comprehensive laws to address these things.

Ms. MACE. Mr. Gregory.

Mr. GREGORY. Extending Federal law to cover synthetic content——

Ms. MACE. Mm-hmm.

Mr. GREGORY [continuing]. That fulfills the same purpose as a revenge porn and making sure it is accessible globally. We encounter cases of this all over the world.

Ms. MACE. Thank you. Mr. Overton?

Mr. OVERTON. Yes. I concur with Mr. Gregory.

Ms. MACE. That was easy. All right. Thank you, and I will yield for 5 minutes to my colleague, Mr. Connolly.

Mr. CONNOLLY. Thank you, Madam Chairwoman. You know, it seems to me that this is not as simple as it seems. Let us take AI for pornography. So, if somebody is a caricaturist and uses AI, and they want to make fun of a political figure and they make him to be the emperor with no clothes, crown on the head, and he is walking around with no clothes to make the point that he is empty, he is without merit or politically lost, now that is not pornography. It is AI-generative technology. It is not the real thing, but the parameters of the law, being a public official, you have got to put up with a fair amount. On the other hand, if somebody took that same individual and used it clearly as, not a caricature, not fun, but in a pornographic AI-generative technology, has he crossed a line in terms of the law, Professor Overton?

Mr. OVERTON. So, I think the answer is yes. Obviously, we have got to be very sensitive in terms of these First Amendment issues, including satire and parody, that type of thing. I would say, though, that even if we have disclosure in terms of deepfakes, this targeting of women who are political figures, even if it is satire, I think that it is a problem and something that we really need to hone in on.

Mr. CONNOLLY. I agree with you, but you are the professor of law, not me. Surely you appreciate the delicacy of that——

Mr. OVERTON. Right.

Mr. CONNOLLY [continuing]. However, under our constitutional system.

Mr. OVERTON. Correct.

Mr. CONNOLLY. We have limits for public officials to be able to seek redress in terms of libel.

Mr. OVERTON. That is right.

Mr. DOERMANN. You can defame us——

Mr. OVERTON. *New York Times v. Sullivan*.

Mr. CONNOLLY. Yes. You can defame us in a way you cannot defame some other citizens, *New York Times v. Sullivan*, so we have high standards for public officials.

Mr. OVERTON. Yes.

Mr. CONNOLLY. So, I put that as a category of complexity.
Mr. OVERTON. Right.
Mr. CONNOLLY. Not so simple in terms of regulating.
Mr. OVERTON. It is something we have got to grapple with. I really refer you to Mary Anne Franks, my colleague at GW, did a great Law Review article in 2019 where she really chronicled these harms as not really contributing to free speech and the marketplace of ideas and truth. And so, there is something else that is here, and we have got to really grapple with it.
Mr. CONNOLLY. Right. I agree with you. I do not think it is as simple——
Mr. OVERTON. Right.
Mr. CONNOLLY [continuing]. As we would all like.
Mr. OVERTON. Yep.
Mr. CONNOLLY. Now, that is public officials.
Mr. OVERTON. Mm-hmm.
Mr. CONNOLLY. Private individuals, such as the girls we talked about in New Jersey, are pure victims of somebody else's perverse sense of fun or pleasure, and they suffer real harm. Legally, what is their protection? What is their redress right now?
Mr. OVERTON. Yes. Right now, the problem is a lot of law does not cover this, and some states have laws with regard to deepfakes, but many states do not. Even though almost all states have revenge porn laws, this activity does not clearly fall under that, so often, there is no recourse.
Mr. CONNOLLY. So, we could maybe use the sort of underage piece of law to get at this if these victims are under a certain age.
Mr. OVERTON. I think that that is correct, but even the CSAM issue that we talked about before is not always clearly covered here in terms of existing laws with regard to child pornography. So, you know, we have got some real holes in the law.
Mr. CONNOLLY. Yes. OK. Well, I think that is really worthy of an explanation, not only by us up here, but by your profession and by the academic community. Dr. Doermann, let us send you back in time. You are back at DARPA, and you are in charge of all AI research and projects. What are we not doing that you want to see funded? You know, pick two or three that we really ought to be doing right now because it could have a beneficial effect if we plow this ground in terms of its promise in protecting ourselves from deepfakes.
Mr. DOERMANN. Absolutely. It is not just deepfakes, you are right. It is AI in general. We have gotten to the point where these large language models, where these models that we have are completely unexplainable. People believe that AI is somehow an answer, and everything is always right that comes out of these systems. We cannot converse with these systems, and they cannot explain why they made a decision or how they made things, I think the explainability issues. And these are things that DARPA is looking at now, but we need to have the trust and the safety aspects explored at the grassroots level for all of these things.
Mr. CONNOLLY. I would just say, Madam Chair, my time is up, but I think there is a huge difference between the pope in a puffery jacket, which does not do much harm, and the example of Ukraine, where deepfakes has him saying we are putting down our arms

and surrendering. You know, that can cause or end a conflict in an undesirable way, and so clearly protecting ourselves and being able to counter that disinformation in a very expeditious way, if not preventing it to begin with, I think is kind of the goal. I thank you.

Ms. MACE. Thank you, Mr. Connolly. I now recognize Mr. Timmons for 5 minutes.

Mr. TIMMONS. Thank you, Madam Chair. It seems we have two main issues here. One is attribution—a lot of people would see a deepfake video and not know whether it was fake or real—and the next issue is updating our legal structures to address the core purpose of them. We have revenge porn laws in many states. The update to the Violence Against Women Act that Chairwoman Mace just mentioned gives a civil cause of action for $150,000. The purpose of that was to address this issue, and the legislative intent did not really keep in mind the possibility of a deepfake. If you cannot distinguish it, there is no difference.

So, I guess my first question, Dr. Doermann, is there any way that we can, one, mandate identification to show that it is an altered image or a fake image, and then, two, is there a way to mandate that in the Code? Just like a photo on my iPhone says where it is and the GPS location it was taken, could you do the same thing with an IP address, and a location, and a time, and a date stamp on the video, and mandate that and make it illegal to create images using this technology without the attribution component? Does my question make sense?

Mr. DOERMANN. Yes. I think you actually have two parts there. Well, first of all, you know, if you mandate creating content or creating things that require you to disclose, for example, that it is a deepfake, the adversaries and the people that are doing these bad things in the first place, they are not going to follow those rules anyway. I mean, that is a much lower bar than actually creating pornographic images.

Mr. TIMMONS. Well, we got to take the first step of U.S. citizens within our jurisdiction.

Mr. DOERMANN. We can, yes.

Mr. TIMMONS. So, I mean, we could easily say if you create this, there is a civil penalty that is available, and that if you do this, there is a criminal penalty, just like states have done with revenge porn.

Mr. DOERMANN. Again, there is also a continuum between the things that are used for good and the things that it is used for bad, so just saying that you are going to, you know, identify it.

Mr. TIMMONS. OK. Deepfake porn, we could literally use AI to say whether something is considered porn or not and then whether that is——

Mr. DOERMANN. I am not sure about that. I think we will have a continuum of these——

Mr. TIMMONS. Well, you are going to have to take a photo of somebody initially of their face or their likeness to then give the AI the ability to create something that is resembling the original human, and you could then——

Mr. DOERMANN. Well, the face is, but the original content can come from a legal pornographic film, for example, and that is what is happening.

Mr. TIMMONS. But you are putting someone's face on it that is not the same face——

Mr. DOERMANN. That is——

Mr. TIMMONS [continuing]. To make it look like them in an attempt to do the same thing that we have revenge porn laws to do.

Mr. DOERMANN. That is what my colleagues here are saying, that there are holes in these laws that do not necessarily allow you to do that, those——

Mr. TIMMONS. Mr. Overton, is there any argument that you could use the existing statute to file a Federal lawsuit against somebody for sharing a deepfake?

Mr. OVERTON. There is an argument. I think the question is, does it hold water.

Mr. TIMMONS. We have got some judges in this country that do just about anything. All right.

Mr. OVERTON. Right, but, you know, we want certainly some consistency in enforcement of law.

Mr. TIMMONS. Sure. We could also maybe expand the Code section, too, but, I mean, I guess then it becomes the whole purpose of revenge porn law is, theoretically, you were complicit in the initial video but not complicit in the sharing, and it has to be done for retribution of some kind. So, I guess it becomes a lot more complicated when you are talking about celebrities and whatnot, but they also deserve the same degree of privacy and respect that we are seeking for everyone else. OK. Let us go back. I mean, I——

Mr. OVERTON. Well, let me just followup here. Disclosure under the court is much more acceptable than complete restrictions here, you know, in terms of the First Amendment.

Mr. TIMMONS. OK. And I guess, Dr. Doermann, back to the attribution issue. I mean, it is not unreasonable to try to create a legal framework through which a photo that is taken on my iPhone has all of this metadata. I mean, theoretically, if that metadata is not present in a video, then we would know that it is a malicious and does that——

Mr. DOERMANN. Yes. Yes. In theory, yes. The problem comes, again, with enforcing this because you now are forcing individuals to mark their content. It is a——

Mr. TIMMONS. Could we use AI to seek out and automatically delete videos that do not have the——

Mr. DOERMANN. Absolutely, and you could forge this type of stuff as well. Even camera fingerprints, these things can be forged, so we just have to be careful about what we rely on, and we make sure that everybody is playing by the same rules in being able to enforce those types of things.

Mr. TIMMONS. Theoretically, we could mandate certain websites to use AI to identify deepfakes and automatically delete them if they are deemed pornographic. Theoretically.

Mr. DOERMANN. Theoretically.

Mr. TIMMONS. OK. All right. Sorry, Madam Chair. Thank you. I yield back.

Ms. MACE. No. Thank you. I will now recognize Mr. Burchett for 5 minutes.

Mr. BURCHETT. Thank you, Chairlady. Several questions. I am just going to ramble, if it is all right with you all. This is a question

to all of you all, and I would like to discuss how criminals are using this deepfake technology to produce child sex abuse material, just child porn. And when these criminals use this deepfake technology to make this material of children, rather than alter the images that already exist, how can law enforcement agencies determine the age of the subject in the material?

Mr. IBRAHIM. Yes, sir. We have seen a rising amount of cases. The New Jersey one was noted. There was also a recent case in Spain in which these models were used for underage young girls. In terms of how can law enforcement potentially use that information and detect, there is some growing thinking that if the models themselves add some watermark or provenance to everything——

Mr. BURCHETT. And explain to me the watermark. What is that?

Mr. IBRAHIM. So, it——

Mr. BURCHETT. I know what it means, but maybe explain it.

Mr. IBRAHIM. It would be an invisible algorithm that is attached to every image that is spit out of the generator, whether it is a benign or malicious image, and which could be decoded by a law enforcement agency or has some sort of chain of custody, that could potentially be useful. That is something that a variety of organizations are looking at.

Mr. BURCHETT. All right.

Mr. DOERMANN. We also have to educate our legal system on how to use these things. I was on a panel at AAAS about a month ago, and very simple things such as the use of face recognition as an AI tool, which we know has been controversial, to say the least. So, we just have to make sure that our content providers or service providers are on board and that they are sharing this type of information with each other, and that is definitely something that is doable.

Mr. GREGORY. The problem this is creating in CSAM has similarities to other problems. It is a volume problem where you then have a triage problem for the people who have to do the investigation because of creating synthesized images and adapting existing images. So, investing in tools that are available to law enforcement as well as others who have to do that triage work would be a critical next step.

Mr. OVERTON. I just would note these evidentiary issues are very challenging for law enforcement.

Mr. BURCHETT. Yes. I think the court cases are that if they just generate, like, a fake face, that they cannot be held for child porn. Is that correct?

Mr. DOERMANN. It is my understanding that those laws are changing, but the previous laws—again, I am not a legal scholar—required a victim, and that was really the loophole there.

Mr. BURCHETT. Yes.

Mr. DOERMANN. But they are closing those.

Mr. BURCHETT. OK. Well, how can we prevent this technology from being used to create child sex abuse material? Mr. Overton, we will start with you first, brother.

Mr. OVERTON. I think that legislation is very important that directly deals with the CSAM issue.

Mr. GREGORY. I will agree with Mr. Overton. It is legislation around CSAM. There are clear reasons to legislate and include this alongside non-synthetic images.

Mr. DOERMANN. And I will just emphasize from the technology point of view, this is a genie that is out of the bottle. We are not going to put it back in.

Mr. BURCHETT. Yes.

Mr. DOERMANN. These types of technologies are out there. They could use it on adults, consenting adults, the same way, and it is going to be difficult to legislate those, but the technology is there. It is on the laptops of anyone that wants to download it from the internet, and so the legislation part is the best approach.

Mr. IBRAHIM. I echo my colleagues, and I would just note the majority of these materials are often done through open-source models. So, the more models you can get to sign up to frameworks and guardrails, pushing bad actors into other models that are harder to use would be beneficial.

Mr. BURCHETT. Do you all agree that these AI-generated images of children, real or not, should be illegal?

Mr. IBRAHIM. I do.

Mr. DOERMANN. Absolutely.

Mr. GREGORY. Yes.

Mr. OVERTON. Yes. We assume they are not hurting children. They are, yes.

Mr. BURCHETT. Yes. You know, I sponsored some legislation in Tennessee where actually people that abused children were given the death penalty, and my statement was that they had given these kids a lifetime sentence, and there is no coming back from that. It is a lifetime of guilt, and you see a lot of the kids self-inflict wounds and take their own lives, and it is just brutal. So anyway, thank you all. Chairlady?

Ms. MACE. Yes, thank you. I will now recognize Mr. Burlison for 5 minutes.

Mr. BURLISON. Thank you. I will begin with Mr. Doermann. Can we talk about the technology that is possibly available to recognize or identify AI and how that might be applied in a commercial setting?

Mr. DOERMANN. Well, the biggest challenge of any of these technologies is the scale. Even if you have an algorithm that works at 99.9 percent, the amount of data that we have at scale that run through our major service providers makes the false alarm rates almost prohibitive. We need to have a business model that our service providers, our content providers have that makes them want to take these things down. If they get clicks, that is what is selling ads now, and if it is not illegal, if we cannot hold them responsible in any way, it makes it very difficult to convince them to do anything.

Mr. BURLISON. Given that currently, today, there is the ability to identify graphic content, violent content, and then to often block it or require a person to take some action to basically break the glass and go through and see that content, can that not be applied to deepfake images or things that are created with it? That way, the individual would at least know that there is no truth to this image.

Mr. DOERMANN. Absolutely, I mean, but the places that this content is showing up are on those pay sites or onsites where it is mixed in with other type of content, so just detecting it is not necessarily the issue.

Mr. BURLISON. And they do not have a self-interest, a financial interest in identifying the deepfakes.

Mr. DOERMANN. Correct.

Mr. BURLISON. OK. I understand what you are saying. So let me ask, the technology is capable. We just need to identify——

Mr. DOERMANN. Not necessarily the deepfake part. If you do a reverse image search, for example, in a number of different sites, you can do it for the entire image, but if you take just the face of an individual, that is what we really need. We need to be able to say, OK, we are not going to look at the entire video because this video is not real, right? Well, part of it is real. The video part of the nude body is real, and the face is generated. So, if we could identify those people, make sure that we have that consent before it gets spread, that might be one thing, but, you know, just to detect something as being pornographic, we are still not detecting the fact that it was generated with a fake.

Mr. BURLISON. The deepfake. You are saying that there is technology, AI, that can view videos and images and ascertain whether it is a deepfake?

Mr. DOERMANN. Not reliably enough.

Mr. BURLISON. There currently is not any.

Mr. DOERMANN. This is 85 percent maybe, and every time we release a tool that detects this, our adversaries can use AI to cover up that trace evidence. So, no, that is why I said in my opening statement that detection and trying to pull this stuff down is no longer a solution. We need to have a much bigger solution.

Mr. BURLISON. Mr. Gregory, how do we authenticate the content without creating a surveillance state or suppressing free expression?

Mr. GREGORY. The first thing I would say is, as we are looking at authenticity and provenance measures, ways that you can show how something was made with AI and perhaps with human inputs, and I think we should recognize that the future of media production is complex. It will not just be a yes or no of AI. It will be, yes, AI was used here, no, AI was not, here is a human. So, it is really important that we actually focus this on the how media was made, not the who, right? So, you should know, for example, that a piece of media was made with an AI tool, was altered perhaps to change an element of it, and that might be the critical information rather than a political satirist made this piece of media, which, you know, certainly would not be something we would want to see here in the U.S. and globally when you look at how that could be misused.

So, I think we are entering a complicated scenario where it is both the authenticity tools and also detection tools, my experience, of a very messy reality where we need to focus on both, but we have got to do it with civil liberties and privacy at heart.

Mr. BURLISON. OK. As I understand it, there is—and this is a question for Mr. Ibrahim. What is the difference between detecting deepfakes and content authentication?

Mr. IBRAHIM. Detecting deepfakes would be something you do after the fact. It would be a system that would look at a video and try to spit out a binary or results-based response. Content authentication or provenance does it while it is being created. That is what Truepic does. So, as the image is being captured from a phone or a smartphone or a piece of hardware, you are attaching and cryptographically hashing the time, the date, the location, et cetera, into the media file while it is being created, so it is a proactive measure versus a reactive measure.

Mr. BURLISON. My time has expired.

Ms. MACE. Thank you. I want to thank all of our witnesses for being here today. In closing, I want to thank you for your testimony again.

So, with that, and without objection, all Members will have 5 legislative of days within which to submit materials and to submit additional written questions for the witnesses, which will be forwarded to the witnesses for their response.

Ms. MACE. So, if there is no further business, without objection, the Subcommittee stands adjourned.

[Whereupon, at 4:43 p.m., the Subcommittee was adjourned.]