ADDRESSING REAL HARM DONE BY DEEPFAKES

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

OF THE

COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

MARCH 12, 2024

Serial No. 118–94

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
55–181 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
MICHAEL CLOUD, Texas
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
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
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
MIKE WALTZ, Florida

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
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
AYANNA PRESSLEY, Massachesetts

MARK MARIN, Staff Director
JESSICA DONLON, Deputy Staff Director and General Counsel
PETER WARREN, Senior Advisor
LAUREN LOMBARDO, Deputy Policy Director
RAJ BHARWANI, Senior Professional Staff Member
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
NICK LANGWORTHY, New York
ERIC BURLISON, Missouri
Vacancy
Vacancy

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

C O N T E N T S

Page

Hearing held on March 12, 2024 1

WITNESSES

Mrs. Dorota Mani, Parent of Westfield (NJ) High School Student
Oral Statement 6

Mr. John Shehan, Sr. Vice President, Exploited Children Division & International Engagement, National Center for Missing & Exploited Children (NCMEC)
Oral Statement 7

Mr. Carl Szabo, Vice President & General Counsel, NetChoice
Oral Statement 9

Dr. Ari Ezra Waldman (Minority Witness), Professor of Law, University of California, Irvine School of Law
Oral Statement 11

Written opening statements and statements for the witnesses are available on the U.S. House of Representatives Document Repository at: docs.house.gov.

INDEX OF DOCUMENTS

* Article, *TechCrunch*, "Taylor Swift deepfake debacle was preventable"; submitted by Rep. Garcia.

* Statement for the Record, Dr. Mary Anne Franks - CCRI; submitted by Rep. Garcia.

* Letter from State AGs Urge Study of AI and Harmful Impacts on Children; submitted by Rep. Langworthy.

* CSAM Graphic; submitted by Rep. Luna.

* Article, *Post and Courier*, "Aiken Winter Colony member facing voyeurism charges"; submitted by Rep. Mace.

* Article, *People*, "Lawmaker Whose Son Died by Suicide After Sextortion"; submitted by Rep. Mace.

* Report, CDC, Youth Risk Behavior Survey; submitted by Rep. Pressley.

* Questions for the Record: to Mrs. Mani; submitted by Rep. Connolly.

* Questions for the Record: to Mr. Shehan; submitted by Rep. Langworthy.

* Questions for the Record: to Mr. Shehan; submitted by Rep. Connolly.

* Questions for the Record: to Mr. Szabo; submitted by Rep. Langworthy.

Documents are available at: docs.house.gov.

ADDRESSING REAL HARM DONE BY DEEPFAKES

Tuesday, March 12, 2024

U.S. 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 2:27 p.m., in room 2154, Rayburn House Office Building, Hon. Nancy Mace [Chairwoman of the Subcommittee] presiding.

Present: Representatives Mace, Timmons, Burchett, Luna, Langworthy, Connolly, Lynch, and Pressley.

Also present: Representatives Raskin, Garcia, and Morelle.

Ms. MACE. The Subcommittee on Cybersecurity, Information Technology, and Government Innovation will now come to order, and we welcome everyone who is here this afternoon.

Without objection, the Chair may declare a recess at any time.

And I do want to ask for unanimous consent at this time for Representative Morelle from New York to be waived on to the Subcommittee for today's hearing for the purposes of asking questions.

So, without objection, so ordered.

And thank you for being here today, and we have a few extra Members that will come in as well this afternoon.

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

First of all, I want to say thank you to all of our witnesses who are here today. AI deepfakes, nonconsensual photos/photography are only getting worse in this country and around the world because of the advent of technology, and we are very eager to hear from each and every one of you today. If you did not get a chance to watch ABC "This Week" on Sunday and see the way George Stephanopoulos handled the topic of rape, I would encourage everyone watching this today to go and watch it.

I have been working on women's issues for a very long time. The body of work that I have been working on is only becoming more extensive because of the advent of technology. I wanted to point out today for my constituents back home some of the legislation that I have been working on. For example, H.R. 5721, has to do with rape. Rape is an issue that I care about, near and dear to my heart. I do not believe in rape shaming rape victims, but I did a bill that would work on the backlog for rape kits in this country.

There are over 100,000 rape kits that are sitting on shelves today that law enforcement have not processed, and I want women to know here today and in the hearing, those that are watching, those around the country, to know that Congress cares. We care about victims of sexual crimes.

And another bill, most recently, there was a decision in Alabama about IVF, and I have sponsored a resolution, I guess 2 weeks ago, House Resolution 1043, that talks about IVF and my desire to make sure that we, one, condemn the Alabama ruling, but two, also we do everything we can to protect women and their access to IVF. And it is not just a women's issue. It is a family issue. It is men and women alike who want to start a family. And both sides of the aisle, I know that we both want to work to make sure that we protect women and men and their access to reproductive technology and the ability to have a family.

I recently rolled out last week a deepfake bill, an initiative that would take a look at it from a criminal perspective. You know, we have a lot of laws in this country. Some states talk about revenge porn. Some have, you know, obviously, peeping Tom laws, surreptitious recording laws, but really, the advent of deepfakes and technology and AI is really a new frontier, and we will hear from you all today about this. But I filed a bill with some of my colleagues last week that would take deepfakes, if they are in the likeness of a real person, and make it a crime. This is not a crime yet today, and when the FBI or when you are looking to charge someone or indict someone for criminal behavior, it has got to be under Title 18. So, we looked at Chapter 88, Title 18 of the Federal Code of laws and looked at how we can make it a crime. I also recently cosponsored a bill by Alexandria Ocasio-Cortez on deepfakes, but it was related to civil torts.

I have learned a lot in the last hundred days or so, due to some experiences that I have recently had, about our Nation's laws and how poor they are on nonconsensual recordings of people, whether they are real or whether they are deepfakes. I am going to be introducing a bill next week, I believe, on voyeurism, again, looking at Title 18. When the Violence against Women Act was done, there was a civil tort enabled for women who are victims of voyeurism at the Federal level, but there was no crime. Like, it is not a crime to do that at the Federal level, and I am, you know, sort of astonished that there is not. But those are just a smattering of things that I have been working on up here in Congress.

I did want to enter into the record this afternoon and wanted to ask unanimous consent to enter into the record two articles. One is out of *People* magazine. State House Rep. Brandon Guffey, his son committed suicide. His son was 17. The title of the article is, "His Son, 17, Was a Sextortion Victim, Then Died by Suicide. Now South Carolina Dad Protects Other Kids From the Same Fate." This is difficult for me to read, but Brandon Guffey was typing on his phone at his home in Rock Hill, South Carolina. All of a sudden, he heard a sound. It sounded like a bowling ball falling and crashing through shelves, Brandon told *People* magazine. He yelled for his son, Gavin Guffey, who was in the bathroom with the door locked. When the 17-year-old failed to answer, Brandon kicked in the door and found his oldest child lying on the floor bleeding. He

thought that he fell and hit his head. After the shouting from his wife, they called 9–1–1. Brandon said he could smell the gun and the taste of gunpowder.

Brandon's son committed suicide because of being shamed and blackmailed over photographs on Meta, on social media, and it is very hard for me as a mom to hear these stories that have had kids affected by online scammers on social media. But it gets worse because with the advent of deepfakes and AI and technology, it is not just real videos you have to be worried about. It is the fake ones now that can be easily created.

The second article I wanted to ask unanimous consent to be entered into the record is a recent article in the *Post and Courier* and the title of it is, "Member of Aiken Winter Colony Family Still Facing Voyeurism Charges." This guy had a hidden camera in an Airbnb, I guess, and under South Carolina State Law Section 16–17–470, where it is illegal to record anybody, this first-offense voyeurism is a misdemeanor. It is only a misdemeanor. The fine is $500, and you face only up to 3 years in jail. This guy, I believe, allegedly had thousands of videos of unsuspecting victims.

And recently and disturbingly, I learned of a real incident in my district where multiple women appeared to be recorded without their knowledge or their consent, over a dozen women in my district. And disturbingly, included in these videos and these photographs, that I have been made aware of, included sexual assault. As a rape victim, to learn about these things is deeply, deeply disturbing.

And as I just mentioned, these are the real stories of real women that are victims, but it is worse because with the advent of deepfakes and AI and technology, it is not the real videos. I mean, obviously we are worried about that, but now it can be created out of thin air, and that fake videos of real people are out there. We are going to hear your stories today, and some of you, I hope, will touch on legislative options, how do states address this, how does the Federal Government address this, how do we take care of this criminally, how do we take care of this civilly? Because women who are victims of such a disturbing thing, whether it is real or fake or deepfake, they ought to get justice in this country at the Federal and the state level. With AI technology moving forward very fast, here in this Subcommittee today, we are going to talk about this from policymakers and people and family and moms who have experienced this horrific thing called deepfake. We are going to hear about child pornography, something I cannot even talk about, what is happening in the deepfake and AI world with child porn. It is all deeply disturbing, and I look forward to hearing everyone's testimony today and how do we move forward from here and make sure that everyone who has been a victim has their voices heard and that they get justice when this happens.

Thank you, and I yield back to my colleague from Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you. Acknowledging the importance of this hearing during Women's History Month, I am grateful that we are gathered here today to highlight a sensitive but very deeply troubling subject. A 2023 study found that while 98 percent of all online deepfake videos were pornographic, women were the sub-

jects in 99 percent of them. Our hope is that today's discussion will underscore the need for policy solutions that end the production, proliferation, and distribution of malicious deepfakes.

Earlier this year, artificial intelligence generated pornographic images of American pop star Taylor Swift rapidly spread on social media. Formerly known as Twitter, X, that platform and that company, proved very slow to act, and the images received, as a result, more than 47 million views in a matter of hours before X finally got around to removing them. Despite the images' removal, the explicit defects of the singer remain elsewhere online, and no laws exist to stop other malicious actors from reposting that material again. The fact that Ms. Swift, a globally recognized icon who built a $1 billion empire, cannot remove all nonconsensual deepfakes of herself, emphasizes that no one is safe.

Deplorably, children have also become victims of deepfake pornography. Last December, the Stanford Internet Observatory published an investigation that identified hundreds of images of child sexual abuse material, also known as CSAM, in an open data set that AI developers use to train popular AI text-to-image generation models. While methods exist to minimize CSAM in such data sets, it remains challenging to completely clean or stop the distribution of open data sets as the data are gathered by automated systems from a broad cross-section of the web, and they lack a central authority or host. Therefore, tech companies, leaders, victims, advertisers, and policymakers must come together to build a solution and address the issue head on.

Mrs. Dorata Mani, thank you for coming here today and bravely sharing your family's story. You and your daughter, Francesca, have proven to be fierce advocates against the creation and proliferation of nonconsensual deepfake pornography. You are providing a stalwart voice for countless others victimized by AI-generated deepfakes. I know President Biden has heard your heartfelt request for help because during his State of the Union address just this last week, he explicitly called upon Congress to better protect our children online in the new age of AI.

I also want to thank my multiple Democratic colleagues who requested to waive onto the Subcommittee today to speak out against harmful deepfakes. One of those Members, Representative Morelle, introduced the Preventing Deepfakes of Intimate Images Act, which would prohibit the creation and dissemination of nonconsensual defects of intimate images. As a cosponsor of this bill, I see that legislation as a great first step to preventing future wrongs that echo the fight of your family, Mrs. Mani.

Recent technological advancements in artificial intelligence have opened the door for bad actors with very little technical knowledge to create deepfakes cheaply and easily. Deepfake perpetrators can simply download apps that undress a person or swap their face onto nude images. That is why, if we want to keep up with the rapid proliferation of deepfakes, we must support Federal research and development of new tools for the detection and elimination of deepfake content. In addition, digital media literacy programs, which educate the public about deepfakes, have demonstrated effectiveness in vesting individuals with skills to critically evaluate content they consume online.

But we cannot have a fulsome discussion without acknowledging that some of our colleagues, including Members of this very Committee, have actively worked against rooting out the creation and dissemination of deepfakes. This Congress, the House Judiciary Committee Select Committee on Weaponization of the Federal Government, has relentlessly targeted government agencies, nonprofits, and academic researchers who are on the front line of this very work. These Members have stifled efforts of individuals and advocacy organizations actively trying to combat deepfakes and disinformation. For example, the Select Subcommittee accused the Federal Cybersecurity and Infrastructure Security Agency, CISA, of "colluding with Big Tech to censor certain viewpoints." These members argued that CISA's work to ensure election integrity, which, in part, includes defending against deepfake threats, is censorship.

They have also attempted to undermine the National Science Foundation's efforts to research manipulated and synthesized media and develop new technologies to detect. Most recently, on February 26, Chairman Jordan subpoenaed the NSF for documents and information regarding its research projects to prevent and detect deepfakes and other inauthentic information sources. He issued this subpoena even though the directive originated from a 2019 Republican championed law. Chairman Jordan has also targeted many of the academic researchers across the country who provide valuable research findings to the public and policymakers, such as the Stanford Internet Observatory, which led the investigation into CSAM's very questionable inclusion in AI training data sets.

I am proud of the Biden-Harris Administration secured voluntary commitments from seven major tech companies promising to work together with us and with government to ensure AI technologies are developed responsibly, but we know our work is not done. I urge my colleagues on both sides of the aisle to set aside partisan fishing expeditions and redirect our focus toward crafting bipartisan solutions to stop the creation of and dissemination of harmful deepfakes. I look forward to the hearing today, and I yield back.

Ms. MACE. Thank you. I am pleased now to introduce our witnesses for today's hearing. Our first witness is Mrs. Dorata Mani, a mother whose high school daughter was a victim of deepfake technology. We appreciate you being here today, Ms. Mani, to share your and your daughter's experience and message with us. Our second witness is Mr. John Shehan, Senior Vice President of the Exploited Children Division and International Engagement at the National Center for Missing and Exploited Children. Our third witness is Mr. Carl Szabo, Vice President and General Counsel of Netchoice, and our fourth witness today is Dr. Ari Ezra Waldman, professor of law at the University of California's Irvine School of Law. We welcome to have you and pleased to have you all 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 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 arguments to 5 minutes. As a reminder, please press the button on the microphone in front of you so that it is on, and Members up here 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 on, your 5 minutes has expired, and we are going to ask you to wrap up, and I will use the gavel nicely.

So, now I would like to recognize Mrs. Mani to please begin her opening statement.

STATEMENT OF DORATA MANI
PARENT OF WESTFIELD (NJ) HIGH SCHOOL STUDENT

Ms. MANI. Thank you so much for having me here. On October 20, 2023, a deeply troubling incident occurred involving my daughter and the Westfield High School administration and its students. It was confirmed that my daughter was one of several victims involved in the creation and distribution of AI deepfake nudes by her classmates. This event left her feeling helpless and powerless, intensified by the lack of accountability for the boys involved and the absence of protective laws, AI school policies, or even adherence to the school's own code of conduct and cyber harassment policies. Since that day, my daughter and I have been tirelessly advocating for the establishment of AI laws, the implementation of AI school policies, and the promotion of education regarding AI.

Despite being told repeatedly that nothing could be done, we find ourselves addressing this esteemed Committee today, highlighting the urgency and significance of this issue. Our advocacy has brought to light similar incidents from individuals across the globe, including Texas, D.C., Washington, Wisconsin, Australia, London, Japan, Germany, Greece, Spain, Paris, and more, indicating a widespread and pressing concern. We have identified several loopholes in the handling of AI-related incidents that demand attention from government bodies, educational institutions, and the media. However, our greatest disappointment lies in the school's handling of the situation, which we believe is indicative of a broader issue across all schools, given the ease and allure of creating AI-generated content.

Here, I wish to outline the mishandling of the situation by Westfield High School. One, the school inappropriately announced the names of the female AI victims over the intercom, compromising their privacy. The boys responsible for creating the nude photos were discreetly removed from the classroom, their identities protected. Only one boy was called over the intercom. When my daughter sought the support of a counselor during a meeting with the vice principal who was questioning her, her request was denied. The administration claimed the AI photographs were deleted without having seen them, offering no proof of their deletion. My

attempts to communicate with the administration about the case have been constantly ignored.

A harassment, intimidation, and bullying report submitted in November 2023 has yet to yield a conclusive outcome which we should receive within 10 days of submission. The interviews, carried out at the school with underage suspects in the presence of police but without their parents, have made their statements inadmissible in court. Despite our submission of updated policies created by our lawyers at McCarter & English to the Westfield Board of Education, the school's cyber harassment policies and code of conduct remained outdated, referencing Walkmans, pagers, and beepers, with no mention of AI to this day. The school's communication focused on only one boy involved, ignoring the others. The accountability imposed for creating the AI deepfake nudes without girls' consent was a mere 1-day suspension for only one boy. This incident and the school's response underscores the urgent need for updated policies and a more responsible approach to handling AI-generated content and cyber harassment at schools.

In light of the recent incident at Beverly Hills Middle School from this month, Superintendent Bregy not only released a statement that the school's investigation is nearly completed 1 week after the incident, but also took crucial steps of contacting Congress to emphasize the urgency of prioritizing the safety of children in the United States, and today, I have learned from The Guardian that he expelled five students.

This proactive stance demonstrates a commendable commitment to facing uncomfortable truths head on, with a focus on educating and advocating for essential changes in how such incidents are handled. In contrast, my expectations for similar leadership and responsiveness from the principal at Westfield High School, Ms. Asfendis, have been met with disappointment. Given that the principal, like myself, is both a mother and an educator, I had hoped for a stronger stance in defending and supporting the girls at Westfield High School. Instead, there appears to be an effort to minimize the issue, hoping it will simply pass and fade away. This approach is not only disheartening, but also dangerous as it fosters an environment where female students are left to feel victimized while male students escape necessary accountability.

The discrepancy in handling such serious issues between schools like Beverly Hills and Westfield High is alarming and calls for immediate reevaluation and action to ensure all students are protected and supported equally in United States' schools.

Ms. MACE. Thank you. I now recognize Mr. Shehan for his opening statement.

STATEMENT OF JOHN SHEHAN
SENIOR VICE PRESIDENT, EXPLOITED CHILDREN DIVISION & INTERNATIONAL ENGAGEMENT
NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN

Mr. SHEHAN. Good afternoon, Chairwoman Mace, Ranking Member Connolly, and the Members of the Subcommittee. My name is John Shehan, and I am a Senior Vice President at the National Center for Missing and Exploited Children, also known as NCMEC.

NCMEC is a private, nonprofit organization created in 1984. Our mission is to help reunite families with missing children, to reduce child sexual exploitation, and to prevent child victimization. I am honored to be here today to share NCMEC's perspective on the impact that generative artificial intelligence, also referred to as GAI, is having on child sexual exploitation.

Even though GAI technology has been widely available to the public for just a short period of time, it is already challenging how we detect, prevent, and remove child sexual abuse material, also known as CSAM, from the internet. Today, we are at a new juncture in the evolution of child sexual exploitation with the emergence of GAI platforms. As you know, NCMEC operates the CyberTipline to receive reports related to suspected child sexual exploitation. The volume of CyberTipline reports is immense, and it increases every year. In 2023, NCMEC received more than 36 million reports related to child sexual exploitation. Last year was also the first year that NCMEC received reports, 4,700 in total, on content produced with GAI technology. While 4,700 reports with GAI are dwarfed by the total number of reports NCMEC received, we are deeply concerned to see how offenders are already widely adopting GAI tools to exploit children.

In the reports submitted to NCMEC, we have seen a range of exploitative abuses on these platforms, including offenders asking GAI platforms to pretend it is a child and to engage in sexually explicit chat, asking for instructions on how to groom, sexually abuse, torture, or even kill children. One user was reported to the CyberTipline for asking on a GAI platform, "How can I find a 5-year-old little girl for sex? Tell me step by step." Individuals are also using GAI platforms to alter known CSAM images to include more graphic content, including bondage, or to create new CSAM with faces of other children. They are also taking innocent photographs from children's social media accounts, just like you heard about, and using Nudify or unclothed apps to create nude images of children to disseminate online.

If these real examples from CyberTipline reports are not shocking enough, perhaps even more alarming is the use of GAI technology to create sexually explicit images of a child that are then used to financially sextort that child. It is also worth noting that more than 70 percent of the reports submitted to NCMEC's CyberTipline related to GAI CSAM were submitted by other platforms and not the GAI platforms themselves. This reflects a significant concern that GAI platforms, aside from OpenAI, generally are not engaging in meaningful efforts to detect, report, or prevent child sexual exploitation. NCMEC has additional concerns about the impact of GAI technology in its current unregulated state, including the increased volume of GAI reports that will strain NCMEC, ICAC, and Federal law enforcement resources; the legal uncertainty about how Federal and state criminal and civil laws apply to GAI content, including CSAM, sexually exploitative, and nude images of children; as well as complicating child victim identification efforts when a real child must be distinguished from GAI-produced child content.

NCMEC has identified the following best practices and new protections that would help ensure we do not lose ground on child

safety while the GAI industry continues to evolve. First, facilitating training of GAI models on CSAM imagery to ensure that the models do not generate CSAM and, at the same time, ensuring that GAI models are not trained on open-source image sets that often contain CSAM; considering liability for GAI platforms that facilitate the creation of CSAM; ensuring Federal and state criminal and civil laws apply to GAI CSAM and to sexually exploitative and nude images of children created by these tools; and finally, implementing prevention education in the schools so children understand the dangers of using GAI technology to create nude or sexually explicit images of their classmates.

In conclusion, I would like to thank you again for this opportunity to appear before the Subcommittee to discuss the dangers around GAI technology in its current unregulated state and what that presents to children online. NCMEC is eager to continue working with this Subcommittee and other Members of Congress to find solutions to these issues that I have shared with you today, and I look forward to your questions.

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

STATEMENT OF CARL SZABO
VICE PRESIDENT AND GENERAL COUNSEL
NETCHOICE

Mr. SZABO. Thank you. Madam Chair, Ranking Member Connolly, my name is Carl Szabo. I am Vice President and General Counsel of Netchoice. I am also an adjunct professor at George Mason Antonin Scalia Law School.

The stories that I have heard so far are horrible and terrifying, and it enrages me as a father of two that a principal is more willing to side with the perpetrators of a bad action than the victim. I think that is little outside what I am here to talk about, but fundamentally, we should support principals who enforce rules, not principals who try to escape responsibility.

Just kind of jumping in, I do want to kind of disagree a little with my colleague over here. AI is heavily regulated today. It is heavily regulated today. Every law that applies offline applies online. So, when it comes to harassment, we need to enforce harassment law. When it comes to fraud, we need to enforce fraud law. Good example is Sam Bankman-Fried went to prison not because of crypto, but because of fraud. So, the notion that AI is some escape clause for criminals, I think, is incorrect, and we need to do more law enforcement and more prosecution of bad actors.

Simple example, and I kind of outline this in my testimony, so, there was a famous situation this past couple of months where President Biden up in New Hampshire allegedly sent out a bunch of robocalls saying he was dropping out of the race. They used AI to generate the robocalls. Well, turns out that Pindrop, a company that detects AI-generated content, detected it, identified it was created by ElevenLabs, contacted them. Law enforcement then got the name of the perpetrator from ElevenLabs and arrested him. And they arrested him, not under any new law, but New Hampshire law, for example, makes it a crime to engage in such fraud. The Telecommunications Privacy Act, TCPA, makes it illegal. We have

Federal laws with prison sentences up to 20 years for such criminal activity. So, I do not care if you use a robot, or you do it yourself, or you get an impersonator from "Saturday Night Live," fraud is fraud, and we need to be willing to prosecute it.

But that is not saying that there are not gaps in the law. I think you are correct. When it comes to things like child sexual abuse material, there are existing gaps in law, and we have been working at Netchoice with lawmakers across the country to close those gaps. Under existing CSAM law, you actually require an actual photo, a real photograph of child sexual abuse material, to be prosecuted. So, bad actors are taking photographs of minors, using AI to modify them into sexually compromised positions, and then escaping the letter of the law. Not the purpose of the law, but the letter of the law. So, this is an example where legislation that is before Congress, that Chairwoman Mace has introduced and many others, can help fill those gaps and make sure that bad actors go to prison.

Looking to the issue of nonconsensual deepfakes, this is something we are also working with state lawmakers across the country to make sure that we enact laws. And one of the things that we did at Netchoice, we sat down, and we looked at First Amendment law because the last thing we want to do is create a law that does not hold up in court. We do not want a criminal to get prosecuted and then have a get-out-of-jail free card because we did not artfully address some of the constitutional challenges. So, when we sat down and drafted, and it is included in the back end of our testimony, some of our proposed recommendations, we identified the constitutional issues and then filled in those gaps.

Finally, when it comes to artificial intelligence, deepfakes, anything like that, we need to make sure we get the definitions correct. One of the challenges that we are seeing across the country, many states have introduced legislation, well intentioned, but, unfortunately, their definition of "artificial intelligence" is written so broadly, it would apply to a calculator or a refrigerator. And so, we need to make sure when we are drafting definitions and we are writing legislation, that we need to hit the target directly. Otherwise, we risk creating a law that is unconstitutional, and an unconstitutional law will protect no Americans.

Just to close out. The last thing that I will chime in on, and I am happy to answer your questions about what is going on at the state level, challenges we can address, but legislation must come from the legislative branch of government. One of the things that truly scares me is when we see executive overreach try to seize control of certain sectors of the government, and the fundamental problem is, like what we have seen in the latest executive order on AI, as well intentioned as it may or may not be, it will violate the major questions doctrine.

So, once again, unconstitutional laws will protect no one. Laws must be written by the legislature and enforced by the executive branch. And to that end, I fully welcome the opportunity to work with this legislature on creating laws that protect everyone from AI deepfakes.

Ms. MACE. Thank you. I will now recognize Dr. Waldman to begin your opening statement.

STATEMENT OF DR. ARI EZRA WALDMAN
PROFESSOR OF LAW
UNIVERSITY OF CALIFORNIA'S IRVINE SCHOOL OF LAW

Dr. WALDMAN. Thank you. Chairwoman Mace, Ranking Member Connolly, and Members of the Subcommittee, thank you for the opportunity to provide testimony about the dangers of and possible responses to deepfakes here today. My name is Ari Waldman, and I am a professor of law at the University of California at Irvine, where I research, among other things, the impact of new technologies on marginalized populations. Given my commitment to these issues and my own personal experience with image-based abuse, I also sit on the board of directors of the Cyber Civil Rights Initiative, or CCRI, the leading nonprofit organization dedicated to combating image-based sexual abuse and other technology-facilitated harms. Although I sit on the board of CCRI, I am here in my own capacity as an academic and as a researcher.

As we have already heard, AI means, in this context, we have a proliferation problem in which images that are fake images and synthetic images and videos about anyone, whether it is Taylor Swift or a young teenage girl, can be sent throughout the internet within moments. Technology, of course, did not create this problem, but it certainly made the problem bigger, harder to identify and dismiss, and vastly more common. But common does not mean that harm is evenly distributed.

Deepfakes cause unique harms that are disproportionately experienced by women, particularly those who are intersectionally marginalized, like Black women and trans women. So much of the history of modern technology begins with men wanting to objectify and sexualize women. It is no wonder that recent advances in deep-learning technology is reflecting our cultural and institutional biases against women. Even here, the story Mrs. Mani tells us about how a school is inappropriately ending up putting the female victim at risk reminds me of how so many schools approach the harassment of women, of trans women, of Black women and queer folk, generally.

The people who create, solicit, and distribute deepfake porn of women and girls have many motives, but what they all have in common is a refusal to see their victims as full and equal persons. Like other forms of sexual exploitation, deepfake porn is used to punish, silence, and humiliate mostly women, pushing them out of the public sphere and away from positions of power and influence. Let us be clear: this is not mere speech. This is not protected by the First Amendment. The harm caused by artificial, nonconsensual pornography is virtually indistinguishable from the harm caused by actual nonconsensual pornography: extreme psychological distress that can lead to self-harm and suicide; physical endangerment that include in-person stalking and harassment; and financial, professional, and reputational ruin.

There are new deepfake porn apps and web services that launch every month, and platforms do not seem willing to do anything about them. These services produce thousands of images every week, and those images are shared on websites that Google and other platforms list in their results and prominently do so. And as we know, deepfakes go viral, even for someone as famous as Taylor

Swift. It is always the last bastion of those who want a deregulatory agenda to say that we need to enforce current laws and we do not need any new laws, but we already know and have examples, and many examples, of current laws not even working. Simply enforcing the laws that we have is insufficient.

Although most of us around the world relate to Taylor Swift's music, almost none of us have the same resources at our disposal as she does. If digital forgeries of us get out there, we are often powerless. That is not just because we cannot all afford lawyers, nor is it just because we do not have lawmakers or platforms listening to us. It is because, just like with real nonconsensual pornography, it is extremely difficult to mitigate the harm of deepfakes after the fact. This means we need deterrence. We need to stop this, particularly nonconsensual deepfake pornography, before it starts, and that is where Congress can step in.

The First Amendment does not stand in the way of Congress acting. There is longstanding precedent in First Amendment law for regulating false harmful expression that is perceived by others to be true. While false expression that is clearly not harmful or likely to be mistaken for real depictions of individuals, such as parody or satire, enjoy considerable First Amendment protection, there is nothing about defamation and fraud that has been historically considered protected by the First Amendment. So, I am not sure what the deep, difficult conversation is here about trying to pass a law that passes First Amendment scrutiny because nothing that we are talking about here is protected by the First Amendment. There are criminal prohibitions against impersonation, against counterfeiting and forgery, and these have never raised serious constitutional concerns.

I would argue that the intentional distribution of sexually explicit, photorealistic visual material that appears to depict an actual, identifiable individual without that individual's consent should be prohibited. Civil penalties are a step forward toward deterrence but insufficient. Deepfakes offer a liar's dividend, as the legal scholars Danielle Citron and Bobby Chesney have argued. In a world where we cannot tell the difference between true and false, those that are lying have a leg up. Thank you.

Ms. MACE. Thank you all. I will now recognize myself for 5 minutes for questioning. And to piggyback on Dr. Waldman, yes, that Taylor Swift video got 45 million views before it was ever taken down, and there are people today who do not know that it was a deepfake, probably believe that it was still real because they do not know the difference and did not know it was taken down because it was a deepfake. So, I appreciate everyone's points today.

My first questions will go to Mrs. Mani, and first of all, I just want to say as a mom of a 14-year-old girl, it is horrifying to know what your daughter went through and the fact that they released the names. I did not have that detail, but it really pains me to hear that. I was raped at the age of 16 by a classmate of mine in high school. I dropped out of school shortly thereafter, and I can only imagine as a mom what my mom felt at the time. It is a deeply painful experience, and I am really sorry that it happened to you and any woman or young girl that has gone through this. I hate, you know, what they have felt and the shame that they have gone

through. And on that point, when George Stephanopoulos rape shamed me on Sunday on "ABC News This Week," I want to make sure that no woman or girl is ever treated that way, and I hope that we can put a stop to that.

So, first of all, my first question to you, in your written testimony about what was done to your daughter, you state this event left her feeling helpless and powerless. As a mom, can you talk to us a little bit about what this has done to your family?

Ms. MANI. Yes. So, I probably will not share what you want to hear, but the moment when Francesca was informed——

Ms. MANI. Mm-hmm.

Ms. MANI [continuing]. By her counselor and her vice principal that she was one of the AI victims, she did feel helpless and powerless.

Ms. MACE. Mm-hmm.

Ms. MANI. And then she went out from the office, and she has noticed group of boys making fun of group of girls that were very emotional in the hallway. In that second, she turned from sad to mad, and now, because of you, all of you, we feel very empowered because I think you guys are listening. And just like you pointed out, you are a father. I think we are all human beings, we all have children, and we all have brothers and sisters that we want to protect, and we should sit down together and figure out a way how to fix it.

And I am so sorry that Mr. Stephanopoulos shamed you. I think that is the narrative that must change in media. Besides upsetting, it is just irresponsible and dangerous. The narrative needs to be changed.

Ms. MACE. Mm-hmm.

Ms. MANI. And instead of talking about girls and how they feel as a victim, we should be talking about the boys and how are they being empowered by the people in power, especially, in my case, in education, by being left unaccountable, walking the hallways with the girls. My daughter does not mind. I do.

Ms. MACE. Right, and I want to thank you for your and your daughter's advocacy, too. Your voice is very important because this is so early on in terms of the technology and what laws we are looking at, at the Federal and the state level. It is very important to hear voices of moms and dads and parents and the kids who have been affected, quite frankly, because those voices have to be a part of the conversation, and I hope that your advocacy will help change the policies not just at her school, but at every school. So, we really admire and appreciate you being here today.

I have less than 2 minutes, and I did want to, while I have you, Mr. Szabo, talk about legislatively, policy wise, because I am very, very, very, very tuned in to, one, as a victim of sexual trauma and assault and then seeing, you know, the things that I have seen, especially over the last couple of months, the advent of technology and then nonconsensual pornographic images and videos, et cetera, and then digital forgeries. You know, at the Federal and the state level, just at the state level, how many states have updated their laws so far?

Mr. SZABO. So, right now, we have been working with states across the country. Wisconsin is about to enact the two recommended pieces.

Ms. MANI. Are they the first?

Mr. SZABO. I do not want to say they are the first——

Ms. MACE. Mm-hmm.

Mr. SZABO [continuing]. But they are definitely one of the leaders on this. They are going to actually enact both the recommended Stop Deepfake CSAM Act as well as the Stop Nonconsensual Artificially Generated Images Act. California right now, we are working with lawmakers out there to make sure that their introduced legislation does not get thrown out by a court when a bad actor gets arrested. And so, we are seeing many states across the country start to adopt this. To your home state of South Carolina, I would love to see——

Ms. MACE. That is what I was going to bring up—I have 40 seconds left—is talking about South Carolina's laws, and I am going to look up impersonations and forgeries. I am not quite as familiar with state law. Obviously, that is not my jurisdiction. But when I looked at what was going on, when I found out about these women in my district that had been recorded without their knowledge or consent, I looked at state law. State Law 16–17–470 is under peeping Tom voyeurism laws. A $500 fine and up to 3 years in jail for the first offense is offensive. It is not a felony until the second offense, but clearly it is not enough, but there is not digital. There is nothing that would include, I believe, deepfakes in there, so I would love to talk to you about and actually even work with our state legislature, who I know our state legislature is working on revenge porn laws, but I also want to strengthen state law in all ways with nonconsensual images and video. So, I would love to talk to you afterwards, so thank you. I am going to yield back to my colleague from Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you. Mr. Shehan, I just want you to know, you could not pay me a million dollars a month to have your job. I cannot imagine dealing every day with violence against, abuse against children. It is just horrifying and very hard to listen to or contemplate, and I salute you for doing what you are doing and protecting children.

Dr. Waldman, well, it is almost St. Patrick's Day, a little leprechaun on my shoulder. You will forgive this question, but is deepfakes mentioned in the Constitution of the United States?

Dr. WALDMAN. No.

Mr. CONNOLLY. No. So, according to Samuel Alito logic, we have no ability to regulate deepfakes because it is not mentioned in the Constitution. Isn't that kind of what he did in the Dobbs decision with respect to abortion?

Dr. WALDMAN. Yes. There is no history and tradition of regulating deepfake technology under his theory of interpretation.

Mr. CONNOLLY. Thank you. So much for originalism. Of course, we saw a lot of originalism with respect to the Fourteenth Amendment just recently. I think it is kind of outside the window, Antonin Scalia Law School being named after an originalist notwithstanding. Mr. Szabo, if I understood him correctly, was suggesting we do not really need a lot of new laws. There are some

gaps, but how about enforcing what we got both at the state level and the Federal level. What is your sense of that? I am addressing you, Dr. Waldman.

Dr. WALDMAN. Oh, sorry.

Mr. CONNOLLY. I mean, Congress is all about passing laws. Do we need to pass more laws? I mean, are there, in fact, some significant gaps that allow malign things to happen that we could perhaps prevent.

Dr. WALDMAN. Especially in this situation. We have seen it before with nonconsensual pornography. We needed new laws on the books because existing defamation or existing tort law had too many gaps, especially when victims originally allowed the image to be taken or video to be taken in the context of a consensual relationship but then distributed without their consent. So, we needed new laws, and we have seen some progress. My colleague at GW Law School, Mary Anne Franks, has been a leader in working with legislatures to pass legislation all across the country, so that is just one example. There are so many gaps here as well.

Mr. CONNOLLY. So, I invite you to provide us a list of those gaps because we would be glad to work on filling those legislative gaps.

I know my colleague and friend, Mr. Raskin, has to go to another committee. I yield the balance of my time to Mr. Raskin.

Mr. RASKIN. Well, thank you very much, Mr. Connolly. I just had one question for Mr. Waldman. Can you tell us what is the experience of deepfake regulatory legislation in the states and have they survived First Amendment attack, and what is the best model for creating a statute to deal with the problem?

Dr. WALDMAN. So, we do not have a lot of examples of state legislation focusing specifically on deepfakes, but we have examples of state legislation focusing on nonconsensual pornography that has gone to be challenged on First Amendment grounds, and they have been upheld. Minnesota is a really good example. The State Supreme Court handed down—and Illinois—handed down excellent decisions saying that, just as I discussed in my written testimony, there is no reason why this kind of nonconsensual harmful activity has ever been protected by the First Amendment. And Congressman Connolly, you are talking about history and tradition. Here, we have an example. There is no history and tradition of allowing this type of content, this type of behavior to be protected by the First Amendment.

Mr. RASKIN. Thank you very much. I yield back, and thank you, Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Raskin. Mr. Szabo, you know, I represent George Mason University, though I would never have named law schools the way it got named. It is a public university. But I invite you to do the same thing I have invited Dr. Waldman to do, which is, where there are gaps, or, for that matter, where there are enforcement issues, please alert us. You may want to comment.

Mr. SZABO. Yes, thank you. So, first of all, with respect to the gaps, I highly suggest we take a look at making sure that our laws clearly address AI deepfake CSAM, one such example. The other, when it comes to law enforcement. So, this is something that—there is a group called Stop Child Predators that put out a report

recently. Ninety-nine percent of reports of child sexual abuse material do not even get investigated. Yes, I know. Only one percent of reports of child sexual abuse material get investigated, and that is a lack of resource. So, there is currently legislation, both on the House and Senate side from both parties, called the Invest in Child Safety Act, which would give law enforcement more tools to put bad actors behind bars, and that is something I suggest taking a look at as well.

Mr. CONNOLLY. And I would just say in closing, when I was Chairman of Fairfax County, we had a police unit that looked at, you know, child predation and sex trafficking and crimes against children, but that was 15 years ago, and what has happened with technology has just exploded. And often, I think it just goes beyond the resources of local law enforcement to monitor, let alone entirely enforce, so I think that is something we are going to look at in terms of how can we find better ways of addressing the issue at that level. Thank you so much.

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

Mr. TIMMONS. Thank you, Madam Chair. Mr. Szabo, you said that we do not really need a lot of new laws, and, Dr. Waldman, you have taken a pretty different stance on that. I mean, it seems to me that there are, indeed, holes and there are gaps, whether it is revenge porn, nonconsensual porn, child porn. I mean, I think, Mr. Szabo, you would agree that we do need to address that. I mean, there is just a lot of gray area surrounding causes of action and ways to be made whole, whether it is using civil law to extract financial benefits or criminal law in certain circumstances. But you would agree that we do need to address the holes as it relates to those areas.

Mr. SZABO. Hundred percent. I mean, you have laws like FCRA, HIPAA, all these laws. Rohit Chopper is the director of the CFPB. He and I probably disagree on not much. Even he recognizes that you cannot hide behind a computer because existing laws apply, but here we do have gaps that do need to be filled.

Mr. TIMMONS. So, I guess to that, I mean, are you familiar with the Coalition for Content Provenance and Authenticity that Adobe has founded?

Mr. SZABO. Yes.

Mr. TIMMONS. OK. So, I mean, it seems that one of the big problems is that anybody can use the internet and create deepfakes of any kind, and there is no way of knowing who created it, and that is a big challenge.

Mr. SZABO. Exactly. So, what we need to do is better identify the perpetrators. I completely agree that it is a challenge, but you can reverse engineer. You can look at IP addresses. That is kind of what happened with the Biden deepfake call. Once they——

Mr. TIMMONS. I wanted to go to that.

Mr. SZABO. Yes.

Mr. TIMMONS. So, they were able to charge them because it was fraudulent in that he was not actually pulling out of the race, and there are all kind of laws associated with that. Would it be illegal if the same individual, instead of saying that the President was pulling out of the race, did dozens of videos of him falling upstairs

or stammering or stuttering? I mean, you know, those will have equally adverse impacts on a campaign. What law would apply if somebody did a video of him falling into Marine One or falling out of Marine one?

Mr. SZABO. Yes.

Mr. TIMMONS. I mean, is that illegal?

Mr. SZABO. It is a complex——

Mr. TIMMONS. The answer is no.

Mr. SZABO. Yes.

Mr. TIMMONS. I do not think it is.

Mr. SZABO. Well, "it depends," is kind of the problem because you have the public figure doctrine. You have satire. There is a lot that goes into that. States have tried to look at this by requiring campaign videos that use altered images to have a disclosure, but the challenge there, again, is in the definition. So, if a politician were standing in front of a green screen, that would be defined as an altered image, and all of a sudden you have to put at the bottom of your campaign ad, there are fake images in the campaign ad.

Mr. TIMMONS. Again, I mean, there are so many different bizarre media outlets. I mean, you could not put a video of a fake video of the President falling, which, again, there are many that exist that are not fake. But I mean, if you had a fake one, you could not put it on television because it gets vetted through legal. You could not theoretically run an ad on a radio that is fabricated because the radio station has liability if they are going to release an ad that is fake, I mean. But, again, the internet is such a wide area of media consumption, that none of these laws really have any enforcement mechanism. I mean, how would you address a deepfake that would be detrimental to someone's political campaign or life, short of nonconsensual pornography, but still is equally bad? We do not have laws for that.

Mr. SZABO. Well, so you could bring an action under existing tort law for defamation of character, misappropriation.

Mr. TIMMONS. Why is it defamation if you are falling over?

Mr. SZABO. Because if it is not a real image, it is a——

Mr. TIMMONS. What if I fell over in a different image?

Mr. SZABO. Well, so, I was going to say——

Mr. TIMMONS. Again, truth is the ultimate defense to defamation, so.

Mr. SZABO. Yes. So, when it comes to nonconsensual disclosures, for example, you have the *Hulk Hogan v. Gawker* example that played out under existing privacy law, so there is potential there. There are a lot of laws out there that can be enforced today, and to the extent that we do find gaps, we need to make sure that when we fill them, that we do so in a constitutional way.

Mr. TIMMONS. I agree with you on that, and I think one thing that we are not talking about is disparity of resources. Dr. Waldman, you touched on this. Taylor Swift has unlimited resources. She can sue whoever she wants. If a similar situation to Ms. Mani happened, technically, under the VAWA civil cause of action, you could probably allege that it was nonconsensual pornography, I mean, but it would cost tens of thousands of dollars, so, I mean, I like loser pays across the board. But could we look into some sort of loser pays funding mechanism to address civil causes

of action for revenge porn, nonconsensual porn, all of these things. Dr. Waldman, is that something——

Dr. WALDMAN. Yes, absolutely. I believe Chairwoman Mace's proposal includes a fee-shifting provision for civil damages that would, you know, it is found to be indeed nonconsensual, deepfake pornography, that the perpetrator would have to pay. But still, even Taylor Swift still has the problem of those images and videos are still out there, and even she cannot——

Mr. TIMMONS. Well, it also goes back to the provenance. Like, how do you know who did it? Anyways, OK. I am over. Thank you. I yield back.

Ms. MACE. Thank you, and I will recognize Ms. Pressley for 5 minutes.

Ms. PRESSLEY. Thank you to our witnesses for being here today, including Ms. Mani. As a survivor of intra-family childhood sexual abuse myself, I must say, I really do look forward to a day where families and children do not have to weaponize and relive their trauma in order to compel action from their government, but I am grateful for those who do it time and time again.

Frederick Douglass once said it is easier to build strong children than to repair broken men and women. That is why in the 116th Congress, as a freshman Member and serving on the Oversight Committee, I convened the first-ever hearing on childhood trauma in the history of this Committee. Children across the country and in my district, the Massachusetts 7th, are facing layered crises, shouldering unprecedented emotional burden from challenges in their homes, classrooms, and now, more than ever, online. Our young girls—our young girls, and we must see them as all of our children—our girls are targeted and victimized the most.

Just last year, the CDC released a report that teenage girls are experiencing record-high levels of violence, sadness, and suicide ideation. The trauma backpacks that they carry across the thresholds into our schools every day only grow heavier. I ask unanimous consent to enter this youth risk behavior survey into the record.

Ms. MACE. Without objection.

Ms. PRESSLEY. You know, as a Black woman who was once a Black young girl, I know intimately what it is for your body to be criminalized, your hair to be criminalized, for your body to be banned, objectified, and, as a survivor, violated. And as this report makes plain and this hearing has confirmed, our girls are being traumatized. I worry for my 15-year-old daughter, who will think that it is normal, a conflated part of her identity as a girl or a woman in this country, to experience these indignities and these violations. Professor Waldman, in what ways does nonconsensual, deepfake pornography contribute to the growing crises of childhood trauma?

Dr. WALDMAN. I need more than 2 1/2 minutes to describe all those ways, but very briefly, the nonconsensual, deepfake pornography does more than just nonconsensual pornography in that not only does it objectify and make someone at risk of, you know, someone who is always looking over their shoulder, every image, every social encounter that they engage in, which deters them from engaging with other people, which is necessary at any age of life, but also, it allows for this to happen even if you do not have any im-

ages out there, right, because these images can be created even with a simple instruction to an AI generator. Essentially, what it does is it creates perpetual trauma and perpetual risk of trauma.

Ms. PRESSLEY. That is right. Thank you. And further, a traumatized child certainly has a decreased readiness to learn. Advances in AI have made it easier for people to create sexual content that intimidates, degrades, dehumanizes, and traumatizes victims, and this technology is becoming more present in our K through 12 schools. Ms. Mani, can you describe what the psychological damage is for teenagers who are victims of this type of harassment? And once again, thank you for the courage you and your daughter continue to display in the face of these reprehensible acts.

Ms. MANI. [Off mic.]

Ms. MACE. Turn your microphone on or speak into it.

Ms. MANI. So, I am not trained to really talk about the repercussions of those images. All I can tell you is that we are not the majority. We took a stand and my daughter took back her dignity, but not many girls can be in the same position because of multiple of layers and factors. Most importantly, it is a shame that in 2024, we are still talking about consent, consent in regards to our body. Now that should be taught as a sentence, and our girls that are not empowered but rather falling through the cracks because of the educational system. Laws, they have to be put in place? Hundred percent. School policies? Hundred percent. And then we all should sit down and figure out ways of how to make it better without pointing fingers as well but, rather, because it is ethical and the right thing to do.

Ms. PRESSLEY. Absolutely. I think we should start with trauma-informed schools. Thank you.

Ms. MANI. Hundred percent.

Ms. MACE. I will now recognize Mr. Langworthy for 5 minutes.

Mr. LANGWORTHY. Thank you, Chairwoman Mace. It seems now every single week that goes by, we see another story about a bad actor using AI unethically. And while I strongly support innovation and will always work to make sure that this country does not lose its edge to China in the AI race, I think that we all must hold accountable unethical creators, criminal actors, and especially those who are creating child pornography and child sexual abuse material.

Emerging technology should always be used in ethical ways, and tech companies, alongside Congress, need to ensure that this happens. That is why I am very proud to be working on legislation with attorney generals [sic] from all 50 states and four territories that would create a commission examining generative AI safeguards, assess current statutes, and recommend legislative revisions to enhance law enforcement's ability to prosecute AI-related child exploitation crimes.

And I would like to enter into the record a letter signed by 54 attorneys general calling for this commission-based approach.

Ms. MACE. Without objection.

Mr. LANGWORTHY. I want to start today by talking about law enforcement's approach to generative AI. Mr. Shehan, how is law enforcement reacting to the uptick in AI-generated child sexual abuse material, CSAM? Has that approach been reactive as in waiting for

images to circulate, or are there ways law enforcement can be more proactive?

Mr. SHEHAN. Excellent question. In a lot of the scenarios, these are reactive because I outlined earlier that many of the generative AI technology companies, they are not taking proactive measures to identify and stop the creation of that material on the onset. It is often after the content has already made its way into the wild that you have social media companies and the such that are finding these types of material and reporting it into our CyberTipline, and we, in turn, provide that information to the Internet Crimes Against Children Task Force members who are actively investigating these cases.

One quick example, in the fourth quarter of last year, we had a report that came through—it was made by Facebook—regarding an adult male who was talking through Messenger to a minor using Stable Diffusion to create child sexual abuse content. Sent it to the minor. It was detected and reported. The Wisconsin ICAC investigated that case, found out not only was he creating content, possessed child sexual abuse material, and through the forensic interviews, also realized he was abusing his 5-year-old son. State and local law enforcement are having to deal with these issues because the technology companies are not taking the steps on the front end to build these tools with Safety By Design. We are getting this content out into the wild far too early, and something has to be done about this.

Mr. LANGWORTHY. It is chilling. Thank you. I would like to point out that the sheer volume of cyber tips has oftentimes prevented law enforcement from pursuing proactive investigation efforts that would efficiently target the most egregious offenders. In only a 3-month period from November 1, 2022 to February 1, 2023, there were over 99,000 IP addresses throughout the United States that distributed known CSAM, and only 782 were investigated. Currently, law enforcement, through no fault of their own, they just do not have the ability to investigate and prosecute the overwhelming number of these cases.

Mr. Szabo, there have been several bills introduced this Congress to address the current legal framework to protect those exploited by generative AI, and even more that look to combat deepfakes all at once. You know, while many of them are well intentioned, my concern is that the Department of Justice has not had much success in prosecuting a number of these cases because of the fine line that needs to be walked with the First Amendment rights. So, I wanted to ask you, what are the biggest gaps in the current legal framework that need to be filled?

Mr. SZABO. So, there is a case called *Ashcroft v. Freedom of Speech Coalition*, and basically what it got into is an overly broad law, well intentioned, to prohibit these types of activities, but it applied to non-actual victims of fake images, and the U.S. Supreme Court shot that down. They said it is a violation of the First Amendment. So, one of the gaps is the type of legislation that we have been talking about here, whether it is the Chairwoman's legislation as well as some of the other bills that have been proposed from all sides of the aisle, to kind of fill that gap and make crystal clear that AI-created content, if it has the image of an actual or

identifiable child, is CSAM material, as opposed to the way the laws are currently written, which requires an actual photo. So, we are seeing time and time again that bad actors are escaping justice. At the same time, the Invest in Child Safety Act, I think, is a really important one to give law enforcement the tools it needs.

One other thing to address is groups like NCMEC are taking on tons of information but not necessarily having enough time to process it, and they have a mandatory deletion time for content. So, giving them a bit more time to process and prosecute content that they receive and tips that they receive, I think would be helpful as well.

Mr. LANGWORTHY. Thank you very much, and I am out of time. Thank you, Chairwoman, for having this hearing, and I yield back.

Ms. MACE. Thank you. I will now recognize Mr. Garcia for 5 minutes.

Mr. GARCIA. Thank you very much, Madam Chair, and thank you for allowing me to waive on to the Committee today. I want to thank all of our witnesses, particularly to Ms. Mani. My heart goes out to you and everything that obviously you have experienced. I also want to just note a couple other cases I think are important.

A few weeks ago, fake images were circling online that put real students' faces on artificially generated nude bodies from Beverly Vista Middle School in Beverly Hills. We are talking about middle school students. We know that that is completely predatory and unacceptable. I know a lot of examples have been discussed today. Also, just weeks ago, AI-generated pornographic deepfake images of Taylor Swift were viewed more than 45 million times.

Now, media investigations showed how easy it was to get AI software guardrails to post these images and how platforms struggled to prevent people from sharing them.

Ms. MACE. Will the gentleman yield for 1 second? We need to waive you on. I ask unanimous consent to have Representative Garcia from California on the Subcommittee for today's hearing, and without objection so ordered.

Mr. GARCIA. Thank you. Now, I would like to ask unanimous consent to introduce this article entitled, "The Taylor Swift Deepfake Debacle Was Preventable," and these are all really serious issues.

Now, fortunately, someone like Taylor Swift had millions of fans that came out to defend her, to protect her online. They flooded social media with junk posts to bury abusive content. The phrase, "Protect Taylor Swift," was on 36,000 posts that were shared. But we know that Taylor Swift fans and Swifties cannot protect everyone and certainly not people that do not have that platform, and so Congress has a responsibility to act.

Now, deepfake pornography accounts for 98 percent of deepfake videos online, and 99 percent of all deepfake porn features women, while only 1 percent feature men. A 2019 study found that 96 percent of all deepfake videos were nonconsensual pornography, and it does not matter, of course, whether you are a billionaire, one of the most powerful women on earth, whether you are Taylor Swift, or a middle school student, deepfake pornography and the manipulation of images is deeply troubling and predatory, particularly to women across this country and girls.

Now, we know that deepfake images can also be used to intimidate, harass, and victimize people, and oftentimes, if you are targeted, there is nowhere to turn, and, Ms. Mani, I know in your situation you received little to no support. And I just wanted to ask you, did you feel you got any support from the actual school itself?

Ms. MANI. I received zero support, and it is disappointing that I have to sit down in here, and, you know, fighting for the girls of Westfield and other girls of United States because my school did not have the balls to do so. Also, in contrast, as you mentioned, the Beverly Hills incident, that principal or superintendent, you know, withdrew the boys from the school, completed HIB investigation within 10 days. He did the right thing. Was it an easy choice? No, but it was the right thing, and I think our girls should not be solo gladiators fighting for their rights. It is shameful that in 2024, we need to fight still for our rights.

Mr. GARCIA. That is exactly right, and I want to note that the Beverly Hills middle school case, I mean, students were actually expelled in that that case.

Ms. MANI. Correct.

Mr. GARCIA. The principal acted quickly.

Ms. MANI. That is right.

Mr. GARCIA. And it is important to note, I mean, all young girls deserve equal protection. That also happens to be a school that is very well resourced with parents that are constantly advocating. It is in Beverly Hills, and so it should not matter where the school is or the resources parents may have, but every girl deserves protection at every single school or any student, period.

Also, just, Professor Waldman, we know, also, just briefly, with the remainder of my time, we know that Russia and China and other hostile actors are targeting our elections. We have seen deepfakes already used to do that, whether it is targeting President Biden or other elections that are happening as well. Can you explain how what is happening right now is undermining our election security and as well as our national security?

Dr. WALDMAN. Sure. So, I think it can boil down to what deepfakes do is, as I said during my testimony, they create a liar's dividend, which means that when anything could be false, then everything is presumed to be false. Therefore, when we know that AI can be used by Russia and hostile countries to undermine our democracy, then we start disbelieving everything, right? We do not start just disbelieving the things that are actually false. We start then allowing people to say, well, how do I know that it is true? It could be a deepfake. And when we disagree on even just the basic things, democracy ceases to work.

Mr. GARCIA. And I appreciate that. I think obviously, deepfakes are oftentimes being used for entertainment purposes. I mean, look, I have seen deepfakes on funny videos, on things that could be entertaining, but it is also deeply troubling when it affects our elections and certainly when it is affecting people and young people in our country.

Before I close, I just want to introduce a written statement into the record from Dr. Mary Anne Franks. Dr. Franks is the President and Legislative Tech Policy Director of the Cyber Civil Rights Institute and Eugene L. and Barbara A. Bernard Professor of Intel-

lectual Property, Technology, and Civil Rights at George Washington Law. So, I would like to just——

Ms. MACE. Without objection, so ordered.

Mr. GARCIA. Thank you, and thank you all to our witnesses.

Ms. MACE. Right. I will now recognize Mrs. Luna for 5 minutes.

Mrs. LUNA. Chairwoman, if I could submit this poster into the record.

Ms. MACE. Without objection, so ordered.

Mrs. LUNA. So, there has been a lot of talk today on CSAM, but for those who might be tuning in that might not know what that is, it is the creation of child sexual abuse materials from lifelike images of children. This situation has not only perpetuated the occurrence of child sexual exploitation in this country, but has also created a new legal question about how to effectively crack down on the practice to protect our children. And I bring this up because this was actually something that the FBI, in talking to them about cybercrimes, asked us to specifically look at because they are having issues currently prosecuting these really, really gross, sick individuals because, technically, a child is not hurt in the process because it is a generated image.

According to recent reports, thousands of AI-generated child sex images have been found on forums across the dark web. Some of these forums have even been found to have instructions that detail how other pedophiles can create their own AI-generated sex images, and I just want to point to the poster behind me.

[Chart]

Mrs. LUNA. If you see "after COVID in 2020," and then you see this spike, this also, in my opinion, correlates with the rise and the, I think, evolution of AI getting better and better and better at generating these graphics and images, and you can see it is clearly not good for our kids. This has increased the speed and scale at which pedophiles create new CSAM. One report explained that in the creation of new images, pedophiles superimpose the face of children onto adult bodies using deepfakes and rapidly generate many images through one single command.

The importance of raising awareness of this problem speaks for itself. In one study of an online forum with over 3,000 members, over 80 percent of respondents stated that they would use or intended to use AI to create child sexual abuse images. This is concerning for child safety and makes law enforcement efforts to find victims and combat real world abuse much, much more important.

My first question is for Mr. John Shehan. You previously stated in a report of CSAM, online platforms grew from 32 million in 2022 to 36 million in 2023. What factors do you think have contributed to this trend?

Mr. SHEHAN. That is an excellent question, and much of it is around just the global scale and ability to create and disseminate child sexual abuse material. This is truly a global issue. The 36 million reports last year, more than 90 percent were outside the United States, individuals using U.S. servers, but we are also seeing a massive increase in the number of reports that we are receiving regarding the enticement of children for sexual acts.

In your chart there, you know, in 2021, we had about 80,000 reports regarding the online enticement of children. Last year, it

jumped up to 180,000 reports. Not even through the first quarter of this year, we are already over 100,000 reports regarding the enticement of children. Many of these cases are involving generative AI. Others are financial sextortion. So, there are individuals in countries like Nigeria and the Ivory Coast, and it is all about the money. They are blackmailing young boys to create a sexually explicit image, just that one image, and then they are after the money——

Mrs. LUNA. The deepfakes.

Mr. SHEHAN [continuing]. Significant amounts of money.

Mrs. LUNA. Just out of curiosity, because we have legislation. I know that I am cosponsoring Representative Mace's legislation in regard to deepfakes, but in regard to the No. 1 platform that you are finding that this is being circulated on, and I know that this has been a question of how do these online platforms moderate this content, what is the No. 1 platform that you are finding that is distributing this?

Mr. SHEHAN. Well, so GAI and deepfakes, it is a difficult question because some of the companies that are reporting the most are doing the most. I mentioned earlier OpenAI. They are setting the bar for what every single other generative AI company should be doing in this space. I also gave an example just a minute ago about Stable Diffusion, which is owned by Stability AI. They are not even registered to report to the CyberTipline. So, we have a huge gap in some of these providers who are enabling individuals to create child sexual abuse content, and they are not even set up to report. So, it is difficult to give a top provider when there are so many that are not even doing a bare minimum.

Mrs. LUNA. So, what would you say the bare minimums are?

Mr. SHEHAN. Well, certainly taking proactive steps that, if someone is trying to use these tools to create child sexual abuse material or modify it or text prompts to create, they should not be allowing that to happen. We started off this session, Ranking Member Connolly had mentioned the Stanford Internet Observatory research that was done that discovered that there was child sexual abuse material in the training set of these data that was given to the OpenAI models to train on. How did that even happen?

Mrs. LUNA. Yes.

Mr. SHEHAN. How is their child sexual abuse material in the content that they are training on? So, there are so many things that we work backward on to rectify the situation that we are in right now.

Mrs. LUNA. OK. Well, I know parents might be tuning in, so I just ask you, and I am sure you would agree, but maybe not post pictures of your children on the web because right now, it is kind of the Wild West out there, and they could be exploited.

Mr. SHEHAN. There certainly are situations where even the benign photos, the clothed photos, as you heard earlier, are being used, run through these tools, and turned into nudity and pornographic content. So, it is a troubling time to be posting content online with some of these tools that are not built Safety By Design.

Mrs. LUNA. Thank you for your time. Chairwoman, I yield my time.

Ms. MACE. OK. We will now, finally, Mr. Morelle, recognize you, and thank you for being here this afternoon. Thank you for waiting so patiently.

Mr. MORELLE. Thank you, Madam Chair, and let me start by thanking you for holding this incredibly important hearing. And thank Ranking Member Connolly and both of you for allowing me to participate in this conversation, as well as thanking our witnesses for sharing their perspectives on this fast-growing and very, very dangerous issue, an issue that has been noted overwhelmingly, disproportionately affects women.

And I also want to acknowledge some familiar faces on the witness panel. I, first of all, want to thank Dorata Mani, a mother, powerful advocate and partner in the war to help prevent innocent people from being harmed by nonconsensual deepfake images. I have had the pleasure of meeting both Dorata and her 14-year-old daughter, Francesca, several times, including here in Washington, where they both courageously participated in a conversation with myself and Congressman Tom Kean on this topic.

I also want to thank the Cyber Civil Rights Initiative, represented here by Dr. Waldman, for their assistance in the drafting of my legislation, the Preventing Deepfakes of Intimate Images Act, which was originally introduced in 2022, long before anyone heard of what happened to Taylor Swift, and we reintroduced the bill in May 2023. On this Subcommittee alone, Members Connolly, Lynch, Langworthy, and Moskowitz are cosponsors.

And as I listen and learn from our witnesses panel this afternoon, the need has been clearly demonstrated for a comprehensive, and what I hope will be a bipartisan, solution to address the unique pain caused by the distribution of nonconsensual, intimate deepfake images, and as has been said, and I think bears repeating, made so much easier today by advances in both generative AI as well as hardware and the capability of even laptops to be able to do this. You know, years ago, you would need to have some sophistication. Nowadays, frankly, I think teenagers will be able to do it with very little training and very little time and energy.

I agree with much of what has been said by my colleagues. Over 50 Members have already supported my legislation, which will make sharing these images - it is comprehensive in the sense that it creates sharing of the images a criminal offense and also creates a private right of action for victims to seek relief. And I hope others, not only on the Subcommittee, but other Members will consider joining as well as we look to perhaps work on all these different proposals and blend them together.

Having said that, in just a couple of minutes, I want to start with a question for you, Mrs. Mani, and thank you, again, for sharing your story and for your thoughtful notes and commentary on a comprehensive solution. And throughout your testimony and other comments you have made publicly, you called attention to the work that needs to be done at the local and state level, within our education system particularly, and also focusing on artificial intelligence companies and what they need to do and their responsibilities. So, based on your experience discussing your story and what you have learned, how do you think Congress can help ensure that

these entities are better prepared to combat the issue of nonconsensual deepfake pornography?

Ms. MANI. I actually think we should establish a roundtable without pointing fingers and ask them for solutions. They are the experts. They will teach us more than we can ever know. So, that is one. No. 2, create a coalition of companies, platforms that host the illegal content, like Google, Amazon, and few others, as well as the financial platforms that facilitate spread of that content, like Amex, Google, Visa, PayPal, et cetera, et cetera, to come to the table because it is the right thing to do.

You know, I have watched, just like every one of us watched, the Senate hearing, and every single platform said the same thing that you said today. We are fathers and we are mothers, and I think that is what we need to do. We need to sit down and figure out ways how to fix it without laws and legislations. Put laws and legislations in place, and then put accountability on the perpetrators or the bad actors.

Mr. MORELLE. Thank you. If I could ask you, Dr. Waldman, in the few seconds I have left, could you talk about the importance of a multipronged approach, civil and criminal, in whatever it is we ultimately decide to do here?

Dr. WALDMAN. Sure. I think a civil remedy approach is a step forward but insufficient for a couple of reasons. We cannot be sure that a simple threat of civil damages would be enough because so many of the perpetrators of this are, you know, the dude in the basement who is probably judgment proof, and so you will not be made whole by a civil remedy. Relying on a civil remedy alone puts the burden entirely on the victim, right, and civil litigation is really expensive, so when you are not Taylor Swift, as we said before, it is really hard to even start something like that. And then in certain situations, we have a history of under criminalizing bad things that happen to women, and intersectionally marginalized women, in particular.

So, while I think we need to be concerned about people in power misusing their power in certain situations, we want to make sure we criminalize this kind of behavior in other instances for important reasons, because it is so bad, because we need that deterrent effect. And I fear that without this comprehensive approach, including government organizations like CISA getting involved in helping platforms do what they should be doing on this, then we are going to leave victims without any recourse.

Mr. MORELLE. Thank you, Madam Chair, for your indulgence, and thanks for allowing me the opportunity to participate. I yield back.

Ms. MACE. Of course. Thank you. In closing, I want to thank our panelists once again for their testimony today, and I want to encourage you all, please stay in touch with this Committee, but with my office. I am deeply passionate about this issue. I come from a background in technology. When I got my first job, I was a programmer, and I have since been fighting for things, especially for women and kids, and this is a very important issue. I have seen this kind of thing have devastating consequences, even deadly consequences, when we are talking about nonconsensual pornography.

I want to piggyback on what Dr. Walden just talked about, civil damages not being enough. You are right. Any victim who is a victim of a nonconsensual image or video, real or deepfake, should know, should be able to take possession of that and know that it is never going to be seen anywhere ever again for the rest of their life, if that is what they want. But that is not really a thing today, I mean, because these things can be found online and everywhere. Once that is out, it is forever. And these victims should be allowed to get their content back, real or fake, if their image and their likeness is part of it, and know that it has been destroyed forever, from every device, any cloud, anywhere online.

And we are not there yet, and it is deeply troubling. So, civil damages are not enough, and in some cases, I mean, there is not even criminal action here. I mean, I look at the Violence Against Women Act, and it is just a civil right of action, not even criminal. I think if you are doing voyeurism at the Federal level, you got to be, like, over international water for it to be against Federal law under Title 18. Like, it is insane to me. And so, I am deeply passionate about trying to correct some of this, correct course, find the gaps, like, as you said, Mr. Szabo, on definitions. While we were sitting here today, I went into the South Carolina's Code of Laws, and I just looked up the word "porn." It does not exist in South Carolina's Code of Law. So, when we are talking about definitions, I agree with you, there is room for improvement, there are gaps here, and I really want to figure out how we move forward in a bipartisan manner at the Federal level, but also with states.

Especially in my home state of South Carolina, there is a lot of work to do. Five hundred fine for voyeurism, the first time is a misdemeanor is wrong, and it is offensive, and it should be much more expensive. We want to make sure that a man who does that to over a dozen women in South Carolina does not ever do it again, and a $500 fine and 3 years in jail just does not cut it. And the law is not clear on whether or not, if it is the first offense or if, let us say, for example, an example that I shared, if it is over a dozen women, images and videos this individual took, if it would be a felony because it is multiple victims. The law is not clear. So, there certainly is, you know, definitely room for improvement in our state as well. And I looked up impersonations, forgery. Forgery in South Carolina law is only related to financial transactions, mostly.

So, there is just so much room to improve here, both at the Federal and the state level. I want you all to know that my office is very much keen on adding to our portfolio of legislation, constitutionally, as it makes sense, not overdoing it, but just the right amount so that victims are no longer victimized, or when they are, that it is quickly corrected.

So, with that and without objection, all Members will have 5 legislative 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, and thank you.

[Whereupon, at 3:53 p.m., the Subcommittee was adjourned.]