S. HRG. 119–171

THE GOOD, THE BAD, AND THE UGLY: AI-GENERATED DEEPFAKES IN 2025

HEARING

BEFORE THE

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

MAY 21, 2025

Serial No. J–119–20

Printed for the use of the Committee on the Judiciary

www.judiciary.senate.gov
www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
61–677 WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

CHARLES E. GRASSLEY, Iowa, *Chairman*

LINDSEY O. GRAHAM, South Carolina	RICHARD J. DURBIN, Illinois, *Ranking Member*
JOHN CORNYN, Texas	SHELDON WHITEHOUSE, Rhode Island
MICHAEL S. LEE, Utah	AMY KLOBUCHAR, Minnesota
TED CRUZ, Texas	CHRISTOPHER A. COONS, Delaware
JOSH HAWLEY, Missouri	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	MAZIE K. HIRONO, Hawaii
JOHN KENNEDY, Louisiana	CORY A. BOOKER, New Jersey
MARSHA BLACKBURN, Tennessee	ALEX PADILLA, California
ERIC SCHMITT, Missouri	PETER WELCH, Vermont
KATIE BOYD BRITT, Alabama	ADAM B. SCHIFF, California
ASHLEY MOODY, Florida	

KOLAN DAVIS, *Chief Counsel and Staff Director*
JOE ZOGBY, *Democratic Chief Counsel and Staff Director*

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

MARSHA BLACKBURN, Tennessee, *Chair*

LINDSEY O. GRAHAM, South Carolina	AMY KLOBUCHAR, Minnesota, *Ranking Member*
JOHN CORNYN, Texas	CHRISTOPHER A. COONS, Delaware
JOSH HAWLEY, Missouri	RICHARD BLUMENTHAL, Connecticut
JOHN KENNEDY, Louisiana	ALEX PADILLA, California
ASHLEY MOODY, Florida	ADAM B. SCHIFF, California

BEN BLACKMON, *Republican Chief Counsel*
DAN GOLDBERG, *Democratic Chief Counsel*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

THE GOOD, THE BAD, AND THE UGLY: AI–GENERATED DEEPFAKES IN 2025

WEDNESDAY, MAY 21, 2025

UNITED STATES SENATE,
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY,
AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:34 p.m., in Room 226, Dirksen Senate Office Building, Hon. Marsha Blackburn, Chairman of the Subcommittee, presiding.

Present: Senators Blackburn [presiding], Hawley, Tillis, Moody, Klobuchar, and Coons.

OPENING STATEMENT OF HON. MARSHA BLACKBURN, A U.S. SENATOR FROM THE STATE OF TENNESSEE

Chair BLACKBURN. The Senate Judiciary Committee on Privacy, Technology, and the Law will come to order.

And I want to thank all of you for being here with us this afternoon. As you can see, everyone is curious about AI. And today, we are going to talk about AI and how this affects our content creators, our creative community, our children, and how it affects all Americans when it comes to the digital space and what happens with AI-generated deepfakes.

This hearing is titled "The Good, the Bad, and the Ugly," and it is titled in that regard for a specific reason. Now in Tennessee, we talk about there is a lot of good that has come from AI when you are talking about logistics, advanced manufacturing, healthcare, cutting-edge research, and we've even seen the amazing role that AI has played in giving voice to some, Randy Travis to be specific, who joined us here on the Hill recently in introducing the NO FAKES bill. It gave Randy Travis the ability to share his talent with the world once again.

And despite some of these benefits, there are really some bad and unpleasant sides to AI, and specifically when it comes to AI-generated deepfakes. These deepfakes cause tremendous harm, and today, we are going to examine those harms and the legislative solutions, including the NO FAKES Act that Senators Coons, Klobuchar, Tillis, and I have introduced. We have introduced them specifically to address these harms.

First, these deepfakes pose significant harm to our content creators, from Music Row to Beale Street, back over to the Smoky Mountains in Upper East Tennessee. Tennesseans have made their mark in the music world, and we've got one of those artists with

us today. But the proliferation of these digital replicas created without the artist's consent pose a real threat to their livelihoods and the livelihoods of all American artists and creators.

The NO FAKES Act is a monumental step forward in protecting our creative community. It provides landmark protection of the voice and visual likenesses of all individuals and creators from the spread of these digital replicas that are created without their consent. And I am looking forward to speaking with our witnesses about this critical bill and how impactful it will be for the creative community.

And I have got to be clear, our efforts must protect all Americans from the harms of deepfakes, and that includes our precious children. In recent years, we have seen a deeply troubling spike in the use of generative AI to create sexually explicit deepfake content. Just as concerning, NCMEC saw a—get this number—1,325 percent increase from 2023 to 2024 in reports involving generative AI. We have got to do something about that, and both the NO FAKES Act and the TAKE IT DOWN Act, which President Trump just signed into law this week, go a long way to providing greater protections for our children from these deepfakes.

These deepfakes have also served as a powerful tool for fraud. In one example, scammers used AI-generated images and voices of a multinational firm CEO to steal millions of dollars. We've also seen celebrities' likenesses misappropriated in false product endorsements.

It is clear that Congress has to act, and that's why the three of us sitting right here on this dais have joined forces, plus Senator Tillis, who is going to get here in a little bit, to work on the NO FAKES Act and get it to President Trump's desk this year. We know that the creative community, all these content creators, our children, and all Americans deserve nothing less than our best efforts on this issue.

And I turn to Senator Klobuchar for her opening statement.

OPENING STATEMENT OF HON. AMY KLOBUCHAR, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Senator KLOBUCHAR. Thank you very much, Senator Blackburn. I am very excited about this Subcommittee and the work we have already done together for years on this issue and similar issues when it comes to tech.

I share your hopes for AI and see that we are on this cusp of amazing advancements if this is harnessed in the right way. But I am also concerned if things go the wrong way. I think it was Jim Brooks, a columnist, that said he has trouble writing about it because he doesn't know if it will take us to heaven or hell. So it is our job to head to heaven, and it is our job to put some rules in place. And this is certainly one of them. We want this to work for children, for consumers, for artists, and not against them.

And you brought up the example, Chair, of Randy Travis, who was at the event that we recently had with you and Senator Coons and myself about the bill and how he used AI in such a positive way. But then we know there are these risks.

And one of the things that I think is really exciting about this week is that, in fact, on Monday, the President signed my bill with

Senator Cruz, the TAKE IT DOWN Act, into law. This was a bill I discussed with him and the First Lady at the inaugural lunch. It is an example of use every moment you have to advance a cause. And then she supported the bill and hoped to get it passed in the House. Senator Cruz and I had already passed it in the Senate, and we were having some trouble getting it done over in the House. So we are really pleased because it actually does set some track moving forward, even though that bill is about nonconsensual porn, both AI-created and non-AI-created.

It has had huge harmful effects, about 20-some suicides a year of young kids who think they are sending a picture innocently to a girlfriend or a potential boyfriend, and then it gets sent out on their school internet. It gets sent out to people they know, and basically they believe their life is in ruins and don't have any other context and take their own lives. And that is just the most obvious and frightful part of this, but there are others as well. So I am hoping this is going to be a first step to some of the work that we can do, including with the bill that we are going to be discussing today.

So AI-enabled scams have become far too common. We know that. It takes only a few seconds of audio to clone a voice. Criminals can pull the audio sample and personal backstory from public sources. Just last week, the FBI was forced to put out an alert about scams using AI-cloned voices of FBI agents and officials asking people for sensitive payment information.

Jamie Lee Curtis was forced to make a public appeal to Mark Zuckerberg to take down an unauthorized deepfake ad that included her digital replica endorsing a dental product. While Meta removed the ad after her direct outreach, most people don't have that kind of influence.

We also need rules of the road to ensure that AI technologies empower artists and creators and not undermine them. Art just doesn't entertain us. It is something that uplifts us and brings us together. When I recently met with Cory Wong, a Grammy-nominated artist from Minnesota, he talked about how unauthorized digital replicas threaten artists' livelihoods and undermine their ability to create art.

So this is not just a personal issue; it is also an economic issue. One of the reasons our country, one of our best exports to the world is music and movies. When you look at the numbers and how we have been able to captivate people around the world, that is going to go away if people can just copy everything that we do. And one of the keys to our success as a Nation in innovation has been the fact—and Senator Coons does a lot of work in this area. We have been able to respect copyrights and patents and people own the rights to their own products.

So that is why this NO FAKES Act is so important. It protects people from having their voice and likeness replicated using AI without their permission, all within the framework of the Constitution. And it protects everybody because everyone should have a right to privacy.

I also am working in the space on AI to put some base rules in place in my role on the Commerce Committee. Senator Thune and I have a bill that we are reintroducing on this to set some rules for NIST to be able to put out there for companies that are using

AI. And then I am always concerned about its effect on democracy. But that is for a different day and in a different Committee.

But I do want to thank Senator Blackburn for her willingness to come out on doing something about tech, including the work she does with Senator Blumenthal, the work that we have done together on Commerce. And if Monday is any sign with the first bill getting through, and they are in that Rose Garden signing ceremony, there is more to come. And so thank you, and I look forward to hearing from the witnesses.

Chair BLACKBURN. Thank you, Senator Klobuchar.

Senator Coons, you are recognized.

OPENING STATEMENT OF HON. CHRISTOPHER A. COONS, A U.S. SENATOR FROM THE STATE OF DELAWARE

Senator COONS. Thank you so much, Chair Blackburn, Ranking Member Klobuchar. It is a delight to work with you. And thank you for inviting me to give some brief opening remarks about the NO FAKES bill.

Because of you and Senator Tillis working on this together since 2023, we have made real progress. There is momentum with this bill. We have been adding co-sponsors. My thanks to Senators Durbin and Hagerty, Schiff and Cassidy. We are adding organizations that are endorsing it like YouTube and RAINN. And as we saw at the White House on Monday, if there is bipartisan agreement in Congress and support from the White House that action is needed, we can make progress in complex, challenging technical areas.

This hearing is a chance to look critically at the current State of the NO FAKES bill so we can both build on that momentum and answer the questions, what did we get right? What do we need to tweak? How can we get more co-sponsors and push to a Full Committee markup?

So I am excited to hear from our witnesses today. There are two other Committee hearings going on right now, which is why you will see Senators come in and out, not a lack of interest.

Senator KLOBUCHAR. Or be late.

[Laughter.]

Senator COONS. Yes. When we were drafting this bill, its applicability to pillars of the creative community like Ms. McBride, Martina McBride, or to a movie star like Tom Hanks, its applicability to people who make a living off of their voice or likeness was clear. But Senator Blackburn and I agreed at the outset, the rules we were drafting should apply to everyone. Everyone should have the power to control their digital replica online, not just those who are superstars.

So I appreciate, Chair Blackburn, the witnesses you brought together today speak to the full scope of what this bill can do to keep the public safe from scams, just like the bill Senator Klobuchar just got signed into law, and help wipe nonconsensual deepfake pornography off the internet.

Second, the revised draft we introduced last month was the product of stakeholders negotiating in good faith. Ms. Carlos, you and YouTube came to the table with the intention of getting to yes, and we got there. And if Google can get behind this bill, can handle the

obligations that NO FAKES impose, so can the other tech platforms.

Thank you. I look forward to hearing from you and returning to questions.

Chair BLACKBURN. Thank you, Senator Coons.

I would like to introduce our witnesses. Martina McBride is a Nashville-based singer-songwriter who has sold more than 23 million albums worldwide with six singles hitting number one on the country music chart.

In addition to her 14 Grammy Award nominations, Ms. McBride is a four-time Country Music Association Female Vocalist of the Year, a three-time Academy of Country Music Top Female Vocalist, and a member of the Grand Ole Opry. She first signed to RCA Records in 1991 and has since been awarded 14 gold records, 12 platinum honors, 3 double platinum records, and 2 triple platinum awards.

Mitch Glazier is the CEO and chairman of the Recording Industry Association of America. We use the acronym RIAA. He helps to represent the rights and interests of over 1,600 member labels. Prior to joining RIAA, Mr. Glazier served as Chief Counsel for Intellectual Property to the U.S. House of Representatives Judiciary Committee, as well as numerous other roles in and around government, including as a commercial litigation associate. He earned his bachelor's degree from Northwestern University and his JD from Vanderbilt School of Law.

Our next witness is Christen Price. Ms. Price serves as Senior Legal Counsel for the National Center for Sexual Exploitation NCOSE. Correct? And she works to combat all forms of sexual exploitation and advocate for justice for survivors of sex trafficking, child sexual abuse, pornography, and prostitution.

Before her work at NCOSE, Ms. Price served as legal counsel at the Alliance Defending Freedom, where she specialized in First Amendment law and conscious protections. Ms. Price earned her bachelor's degree from Cedarville University and her JD from Georgetown University Law Center.

And Mr. Justin Brookman, Mr. Brookman is the Director of Technology Policy for Consumer Reports, where he specializes in data privacy and security issues. Before joining Consumer Reports, he was Policy Director of the Federal Trade Commission Office of Technology, Research, and Investigation. Earlier in his career, he served as Chief of the Internet Bureau of the New York Attorney General's Office. He earned his bachelor's degree from University of Virginia and his JD from New York University School of Law.

And Ms. Suzana Carlos, who serves as Head of Music Policy at YouTube. Until 2022, she served as Senior Counsel for YouTube's Music Publishing and in senior positions at the American Society of Composers, Authors, and Publishers—we like to call it ASCAP–Universal Music Group and EMI Publishing. She is also on the board of Digital Media Association, which represents the leading global audio streaming companies and promotes legal access and engagement of music content between creators and users. Ms. Carlos earned her bachelor's at the University of California, Los Angeles, and her JD from Fordham University School of Law. Welcome to each of you.

At this time, I want to ask you all to rise and raise your right hands.

[Witnesses are sworn in.]

Chair BLACKBURN. And let the record reflect that everyone is in the affirmative.

We will begin with our testimony. Ms. McBride, you are recognized for 5 minutes and welcome.

STATEMENT OF MARTINA MCBRIDE, MULTIPLATINUM COUNTRY MUSIC SINGER-SONGWRITER, NASHVILLE, TENNESSEE

Ms. MCBRIDE. Chairman Blackburn, Ranking Member Klobuchar, Senator Coons, and Members of the Subcommittee, thank you for inviting me to speak about S. 1367, the NO FAKES Act of 2025, a landmark effort to protect human voices and likenesses from being cloned by artificial intelligence without consent. I am so grateful for the care that went into this effort, and I want to thank you and your colleagues for making this issue a priority.

I started singing when I was 4 years old, and my voice is at the center of my art form. Each of my recordings includes a piece of me that is individual and unique. Songs reflect the human experience, and I am honored that they are a part of people's lives, from wedding vows to breakups to celebrating milestones and even the special relationship between a mother and daughter.

But today, my voice and likeness, along with so many others, are at risk. AI technology is amazing and can be used for so many wonderful purposes. But like all great technologies, it can also be abused. In this case, by stealing people's voices and likenesses to scare and defraud families, manipulate the images of young girls in ways that are unconscionable, impersonate government officials, or make phony recordings posing as artists like me. It is frightening, and it is wrong.

Congress just took a very important step forward to deal with sexually explicit deepfake images by passing the TAKE IT DOWN Act. I want to thank all the leaders, including Senators Cruz, Klobuchar, Blackburn, and many on this Committee who worked hard with others to push that bill into law.

The NO FAKES Act is a perfect complement to that effort by preventing AI deepfakes that steal someone's voice or likeness and use them to harass, bully, and defraud others or to damage their career, reputation, or values. The NO FAKES Act would give each of us the ability to say when and how AI deepfakes of our voices and likenesses can be used. If someone doesn't ask before posting a harmful deepfake, we can have it removed without jumping through unnecessary hoops or going to court.

It gives every person the power to say yes or no about how their most personal human attributes are used. It supports AI technology by providing a roadmap for how these powerful tools can be developed in the right way. And it doesn't stand in the way of protected uses like news, parodies, or criticism.

I want to thank the technology companies like OpenAI and Google who support this bill, as well as the legions of creators who have worked so hard to advocate for it and the Child Protection and Anti-Sex Trafficking and Exploitation groups who support it and continue to fight for those who are most vulnerable.

In my career, it has been a special honor to record songs that shine a light on the battles that many women fight, especially the terrible battle of domestic violence. Many fans have told me that the song "Independence Day" has given them strength. And in some cases, the song has been the catalyst that has made them realize that they need to leave an abusive situation. Imagine the harm that an AI deepfake could do, breaching that trust using my voice in songs that belittle or justify abuse.

One of the things I am most proud of in my career is I have tried to conduct myself with integrity and authenticity. And the thought that my voice could be deepfaked or my likeness could be deepfaked to go against everything that I have built, to go against my character, is just terrifying. And I am pleading with you to give me the tools to stop that kind of betrayal.

Setting America on the right course to develop the world's best AI while preserving the sacred qualities that make our country so special—authenticity, integrity, humanity, and our endlessly inspiring spirit—that is what the NO FAKES Act will help to accomplish. I urge you to pass the bill now.

Thank you.

[The prepared statement of Ms. McBride appears as a submission for the record.]

Chair BLACKBURN. We thank you.

Mr. Glazier, you are recognized for 5 minutes.

STATEMENT OF MITCH GLAZIER, CEO, RECORDING INDUSTRY ASSOCIATION OF AMERICA, WASHINGTON, D.C.

Mr. GLAZIER. Thank you so much. Thank you for having me. I am honored to testify today alongside the groundbreaking artist, Martina McBride, who just spoke so eloquently about the value of someone's voice, the value of their image, and the threats posed by abuses of deepfake technology.

I would also like to recognize the almost 400 artists and performers and actors who have just signed a statement in support of the NO FAKES Act with some very simple words. It is your voice, your face, your image, your identity. Protect your individuality. That is why we are here. That is what this is all about.

Artists' voices and likenesses are fundamental to their work, credibility, expression, careers. In many ways, these deeply personal, highly valuable attributes are the foundations of the entire music ecosystem. And unauthorized exploitation of them using deepfakes does cause devastating harm. We have to prevent that harm.

So my deepest thanks and the thanks of a very grateful music community go out to all of you, to Chairman Blackburn, to Ranking Member Klobuchar, to Senator Coons, and to all of the Senators, Senators Tillis, Hagerty, Durbin, Cassidy, Schiff, and I hope many more on this Committee and throughout the Senate for introducing and supporting the NO FAKES Act.

You did it. After months, actually years, of work with each other, stakeholders, your counterparts in the House, you have been able to build bipartisan, bicameral, broad-based consensus around legislation that will protect not just artists but all victims of deepfake

abuses, including child exploitation and voice clone scams, which we will hear about from the other witnesses today.

You have shaped a commonsense bill that has won the support of AI companies like Google, who is here today, OpenAI, IBM, as well as broadcasters, motion picture studios, child protection groups, free market groups, labor unions, and virtually the entire creative community. That is hard to do.

The NO FAKES Act provides balanced yet effective protections for all Americans while supporting free speech, reducing litigation, and promoting the development of AI technology. It empowers individuals to have unlawful deepfakes removed from UGC platforms as soon as it can be done without requiring anyone to hire lawyers or go to court in those situations. It contains clear exemptions for uses typically protected by the First Amendment, such as parody, news reporting, and critical commentary. And it encourages AI development and innovation, targeting only malicious applications and setting the stage for the legitimate licensing of rights with real and meaningful consent.

NO FAKES is the perfect next step to build on after the TAKE IT DOWN Act. It provides a civil remedy to victims of invasive harm that go beyond the criminal posting of intimate images addressed by that legislation and protects artists like Martina from nonconsensual deepfakes and voice clones that breach the trust she has built with millions of fans.

American music is the most valuable music in the world. We lead in investment, exports, and market power. Music drives the success of other important American industries, including the technology industry, through thriving partnerships. If we signal to the rest of the world that it is acceptable to steal Americans' voices and likenesses, we have the most to lose. Our voices and our music are the most popular and will be taken the most, destabilizing the music economy, our intellectual property system, our national identity, and the very humanity of the individuals who bless us with their genius.

The NO FAKES Act is a critical step in setting America up as an example and to continue and extend its global leadership in innovation and creativity. It shows that we can boost AI development while preserving every individual's autonomy, all individual liberties, and protect our constitutional property rights at the same time.

We are really proud to support this legislation, and we vow to help you pass it into law this year. Thank you again.

[The prepared statement of Mr. Glazier appears as a submission for the record.]

Chair BLACKBURN. We thank you.

And Ms. Price, you are recognized for 5 minutes.

STATEMENT OF CHRISTEN PRICE, SENIOR LEGAL COUNSEL, NATIONAL CENTER ON SEXUAL EXPLOITATION (NCOSE), WASHINGTON, D.C.

Ms. PRICE. Chair Blackburn, Ranking Member Klobuchar, thank you for holding this hearing and addressing this truly urgent matter. My name is Christen Price, Senior Legal Counsel at the National Center on Sexual Exploitation, NCOSE, a nonpartisan non-

profit dedicated to eradicating all forms of sexual exploitation by exposing the links between them. Our law center represents survivors in lawsuits against those who perpetrate, enable, and profit from sex trafficking, including pornography companies.

Contemporary pornography depicts and normalizes violence, including asphyxiation, electrocution, and rape. This is pervasive. The top four sites—Pornhub, XVideos, xHamster, and XNXX—had nearly 60 billion total visits in 2024. One woman's husband sexually assaulted her while she was sleeping and put the video on XVideos, which was tagged "Sleeping Pills." Pornhub hosts child sexual abuse material and sex trafficking content with their employees admitting that traffickers use their sites with impunity.

Forged or deepfake pornography uses AI that is trained on this kind of abusive content, merging it with the faces of other women and girls. A 2023 report found that deepfake pornography increased by 464 percent between 2022 and 2023. The top 10 deepfake pornography sites had 300 million video views in 2023. Ninety-eight percent of all deepfake videos are pornography related, and 99 percent of those who are targeted are women.

The perpetrators are disproportionately male. One survey found that 74 percent of deepfake pornography users don't feel guilty about it. A high schooler discovered a boy she had never met took a photo off of her Instagram, created an AI deepfake, and circulated it through Snapchat. Two years later, she still hasn't been able to remove all the images.

A woman whose close family friend made deepfake pornography of her said, "My only crime was existing online and sharing photos on platforms like Instagram. The person who did this was not a stranger. I was not hacked, and my social media has never been public."

These are serious human rights abuses, violating the person whose face is depicted and the person whose body is shown. Survivors report fear; isolation; shame; powerlessness; suicidal thoughts; doxxing; harassment from sex buyers; and difficulty attending school, maintaining jobs, and participating in public life. This is a form of sexual exploitation from which it is impossible to fully exit.

There is a very old idea that to protect more privileged women from male violence, society needs an underclass of women that men can violate with impunity. This was always a morally inexcusable premise, and the rise of forged pornography shows that it is also a lie. Deepfake technology allows any man to turn any woman into his pornography. These are impossible conditions for equality. As Andrew Dworkin stated in his book, "The civil impact of pornography on women is staggering. It keeps us socially silent, socially compliant. It keeps us afraid in neighborhoods and it creates a vast hopelessness for women, a vast despair. One lives inside a nightmare of sexual abuse that is both actual and potential, and you have the great joy of knowing that your nightmare is someone else's freedom and someone else's fun."

The harms are severe and irreversible, so deterrence is essential. This is why NCOSE supported the bipartisan effort to pass the TAKE IT DOWN Act, which the President signed into law on Mon-

day, and requires online platforms to remove nonconsensual content within 48 hours of being notified.

NCOSE strongly supports three additional bills that complement TAKE IT DOWN, the NO FAKES Act, the Kids Online Safety Act and the DEFIANCE Act. These bills help protect individuals from the harmful effects of image-based sexual abuse and increase pressure on tech companies to manage websites more responsibly.

Finally, NCOSE is concerned about the recent AI State moratorium language included in the House Budget Reconciliation bill, as it creates a disincentive for AI companies to put safety first.

Technological progress should not come at the expense of human dignity. It is our collective responsibility to protect the voice, face, and likeness of every person from unauthorized use.

Thank you.

[The prepared statement of Ms. Price appears as a submission for the record.]

Chair BLACKBURN. We thank you.

And I will note for the record that we are submitting your full testimony into the record with all of your footnotes. I really appreciate that. Thank you so much.

Mr. Brookman, you are recognized for 5 minutes.

STATEMENT OF JUSTIN BROOKMAN, DIRECTOR OF TECHNOLOGY POLICY, CONSUMER REPORTS, WASHINGTON, D.C.

Mr. BROOKMAN. Thank you, Chairwoman Blackburn, Ranking Member Klobuchar. Thank you very much for the opportunity to get to testify here today.

I am here on behalf of Consumer Reports, where I head up our work on tech policy advocacy. We are the world's largest independent testing organization. We use our ratings, our journalism, our surveys, our advocacy to try to create a more fair, healthier, and safer world.

I am gratified the Committee is focusing on the problems created by audio and video deepfakes, which, for better or worse, are getting more realistic and convincing every day. They are used in romance scams and grandparent scams where a relative gets a frantic call from a distressed family member who is in immediate need of cash. As the Chairwoman noted, they are used in fake testimonial videos from celebrities hawking everything from meme coins to cookware. I believe Elon Musk is one of the most frequently impersonated celebrities online.

As Ms. Price testified eloquently, obviously, one of the most prevalent uses is for the creation of nonconsensual intimate images and videos. And they are increasingly used to propagate misinformation, certainly in the political realm, but also in the more petty personal realm. There is a story in Maryland recently about an aggrieved teacher who created deepfake audio of his boss saying racist and antisemitic slurs. As this last example shows, realistic cloning tools are easily available to the public and very cheap and easy to use.

Earlier this year, Consumer Reports conducted a study of six voice-cloning tools that are easy to find online to see how easy it would be to create fake audio based on a public recording like a YouTube clip. Our study found that four of the six companies we

looked at didn't employ any reasonable technical mechanisms to reasonably ensure they had the consent of the person whose voice was being cloned. Instead, the customer just had to click, like, yes, I have the person's consent. Two require the person to read a script to help indicate the person was onboard with having their voice cloned. Four of the companies also did not collect much identifying information from customers, just a name or an email address to start creating deepfake voice clones.

Given how likely abuse of these services are, I don't think they were doing enough. And a lot of our members agree. We recently got 55,000 signatures on a recent petition asking the Federal Trade Commission and State Attorneys General to investigate whether these services were in violation of existing consumer protection laws.

And that brings me to solutions. So one thing, we need strong consumer protection agencies who have the resources to crack down on abusive emerging technologies. Last year, the FTC brought a handful of AI cases as part of Operation AIs' Comply, but they don't have the capacity right now to confront the massive wave of scams and abuses online.

Tools and responsibilities, I think some of these AI-powered tools are designed such that they are almost always going to be used for illegitimate purposes, whether it is deepfake pornographic image generators or voice impersonation. Developers of these tools need to have heightened obligations to try to forestall harmful uses. If they can't do that, then maybe they should not be freely available to the public.

Platforms too need to be doing more to proactively get harmful material off their platforms. It is a very difficult job. It takes resources, but it absolutely needs to be done.

Transparency: People deserve to know whether the content they are seeing online is real or fake. I know there have been a number of bills introduced in this Congress to try to address that. Also, there is a law recently passed in California to start to put transparency obligations on entities that make deepfake content.

Stronger privacy and security laws: As this Committee knows very well, the United States generally has fairly weak legal protections. As the Ranking Member noted, the ready availability of information about us online makes it easier for scammers to target us with scams. We have seen a ton of progress at the State level on privacy and security laws, but they are not strong enough.

Whistleblower protections and incentives: In many cases, we only find out about abuses inside these tech companies when someone comes forward with their story. I was glad to see bipartisan legislation introduced on this issue protecting AI whistleblowers in the last week.

Education: I don't want to put all the burden on consumers, but the reality is this is the world we live in. We need to teach people to look out for these sorts of scams. We are part of a campaign called Pause Take9, which tries to train people that if they get an urgent call to action, they should pause, take 9 seconds, think about if this is real or not.

And finally, I want to echo the words of Ms. Price about a lot of discussion about a moratorium on State laws policing bad uses of

AI. I want to stress this is the wrong idea. AI has tremendous, amazing potential, but as this hearing shows, it has some real potential harms as well. The States have been leaders in trying to address these harms, whether it is privacy, co-opting performers' identities, regulating self-driving cars, rooting out hidden biases, other deepfakes. AI is an incredibly powerful technology, but that does not mean it should be completely unregulated.

Thank you very much, and I look forward to answering your questions.

[The prepared statement of Mr. Brookman appears as a submission for the record.]

Chair BLACKBURN. And Ms. Carlos, you are recognized for 5 minutes.

STATEMENT OF SUZANA CARLOS, HEAD OF MUSIC POLICY, YOUTUBE, BROOKLYN, NEW YORK

Ms. CARLOS. Chairwoman Blackburn, Ranking Member Klobuchar, and Members of the Subcommittee, thank you for the opportunity to speak with you today on the important topic of the NO FAKES Act and AI-generated digital replicas. My name is Suzana Carlos, and I serve as the Head of Music Policy for YouTube.

Just last month, YouTube marked the 20th anniversary of the first video ever uploaded to our platform. It is difficult to fathom how much the world and YouTube have changed in those 2 short decades. Today, we have over 2 billion active monthly members on our platform across more than 100 countries, with 500 hours of content uploaded every minute. We are proud that YouTube has transformed culture through video and built a thriving creator economy here in the United States and around the world.

Our unique and industry-leading revenue-sharing model empowers our creators to take 55 percent of the revenue earned against ads on their content. And as a result, YouTube's creative economy has contributed more than $55 billion to the United States' gross domestic product and supported more than 490,000 full-time American jobs in the last year alone. In the 3 years prior to January 2024, YouTube paid more than $70 billion to creators, artists, and media companies.

At YouTube Music, we built one of the world's deepest catalogs, over 100 million official tracks, plus remixes, live performances, covers, and hard-to-find music you simply can't find anywhere else. We have now reached over 125 million paid YouTube music and premium subscribers. And YouTube continues to be at the forefront of handling rights management at scale, protecting the intellectual property of creators and our content partners, ensuring that they can monetize their content and keeping YouTube free for viewers around the world.

In 2007, YouTube launched Content ID, a first-of-its-kind copyright management system that helps rightsholders effectively manage their works. Rightsholders or their agents provide YouTube with reference files for their works they own, along with metadata, such as title and detailed ownership rights. And based on these references, YouTube creates digital fingerprints for those works in question and scans the platform to determine when content in an uploaded video matches the reference content. Rightsholders can

instruct the system to block, monetize, or track the reference content. And over 99 percent of the copyright issues on YouTube are handled through Content ID. It has also proven to be an effective revenue generation tool for rightsholders, as over 90 percent of Content ID claims are monetized.

And as we navigate the evolving world of AI, we understand the importance of collaborating with partners to tackle emerging challenges proactively. We firmly believe that AI can and will supercharge human creativity, not replace it.

Indeed, AI has the potential to amplify and augment human creativity, unlocking new opportunities for artists, creators, journalists, musicians, and consumers to engage creatively with new tools and play an active role in innovation. We are already seeing creators exploring new areas, including the creation of new types of music, books, photography, clothing, pottery, games, and other art inspired in collaboration with AI models. And as this technology evolves, we must collectively ensure that it is used responsibly, including when it comes to protecting our creators and viewers.

Platforms have a responsibility to address the challenges posed by AI-generated content, and Google and YouTube stand ready to apply our expertise to help tackle them on our services and across the digital ecosystem.

We know that a practical regulatory framework addressing digital replicas is critical, and that is why we are especially grateful to Chairwoman Blackburn, Senator Coons, Ranking Member Klobuchar, and all the bill sponsors for the smart and thoughtful approach adopted in developing the NO FAKES Act of 2025. We deeply appreciate their willingness to bring a variety of stakeholders together to forge a consensus on this important topic.

YouTube and Google are proud to support this legislation, which tackles the problems of harm associated with unauthorized digital replicas and provides a clear legal framework to address these challenges and protect individuals' rights. The NO FAKES Act appropriately balances innovation, creative expression, and individuals' rights while offering a broadly workable, tech-neutral, and comprehensive legal solution. By supplanting the need for a patchwork of inconsistent legal frameworks, the NO FAKES Act would streamline global operations for platforms like ours and empower artists and rightsholders to better manage their likeness online. We look forward to seeing the legislation passed by Congress and enacted into law.

We have similarly proudly supported the TAKE IT DOWN Act because it is critical to prevent bad actors from producing and disseminating nonconsensual explicit images. We would like to thank Ranking Member Klobuchar, along with Senator Cruz, for their leadership on the legislation. This is an area we continue to invest in at Google, building our longstanding policies and protections to ultimately keep people safe online.

Thank you again for inviting me to participate in today's hearing. I look forward to your questions.

[The prepared statement of Ms. Carlos appears as a submission for the record.]

Chair BLACKBURN. And we thank you all for sticking to the 5-minute clock. I didn't have to gavel down a person.

[Laughter.]

Chair BLACKBURN. These are great content creators, I mean, so there we go.

I am going to recognize myself for 5 minutes for questions.

And as Senator Coons said earlier, there are going to be Members coming and going because we do have a variety of hearings that are going on.

Ms. McBride, I want to come to you first. I think that your perspective is such an important perspective as we talk about this and talk on the direct impact to someone who is creating content. And I appreciated so much that in your testimony, you talked about how your voice and likeness, along with so many other creators, that that is at risk. And therefore, your livelihood is at risk.

So talk a little bit about how harmful deepfakes are in the long term and why it is important to get legislation like this to the President's desk. And then talk about fellow artists that you have spoken with and their concerns on the issue.

Ms. MCBRIDE. Well, as you said, it does affect livelihood for musicians, backup singers, voiceover actors, authors, like so many people in the arts. For me, being established and having done this for over 30 years, that's not necessarily my first concern. I have the luxury of that not being my first concern, but it is a concern for younger artists that are coming up.

So as I said in my testimony, the thing that I am most concerned with personally is how we work so hard to present ourselves with integrity and a certain character. And the fact that, you know, long term, that could be distorted or manipulated to be the opposite of what I stand for and what I believe or to be used to cause harm to someone through endorsing a harmful product or, you know, far into the future, after I am gone, somebody creating a piece of music or me saying something that I never did. And it just kind of like disintegrating what I have worked so hard to establish, which is trust with my fans, with people who, you know, when I say something, they believe it.

I think for younger artists, to your point of livelihood, to be new and having to set up what you stand for and who you are as a person, as an artist, what you endorse, what you believe in, and establishing a trust with your fans, and then on top of it, having to navigate these waters of someone coming in and distorting all of that is devastating. Like, I don't know how—I can't stress enough how it can impact the careers of up-and-coming artists and even just in their ability to, you know, speak their truth or just to live in fear of being a victim of these deepfakes.

Chair BLACKBURN. Yes. Mr. Glazier, I want to come to you on something you mentioned about the critical balance of protecting the artists' voices and likenesses and then also reducing litigation. And that is why we need to have this framework. And I think helping artists stay out of court, I mean, they're at a point where they may have to spend much of what they have earned in order to protect themselves and to protect their brand, if you will, if you will elaborate on that.

Mr. GLAZIER. Sure, I am happy to. The bill has to be effective and practical at the same time, both for the victim and for the platform who is going to limit the damage to the victim. It has to work

on both ends. And that is why I think the approach that was taken both in the TAKE IT DOWN Act and in this act are so important, especially in areas where the platform has less knowledge and less control because end users are posting on the platform. And those can go viral very, very quickly.

The ability for the platform to take it down as soon as, you know, technically and practically feasible so that they stop the damage and to keep it down so that the artist or any other victim doesn't have to spend their lives monitoring a platform and continually sending more notices and more notices as end users keep putting up the same material over and over and over again. We now have tools that will allow the removal off of the platform. And once the removal is done, the damage can be limited. There is no liability for the platform, and the artist doesn't have to spend their time just litigating.

Where there is more knowledge and control, right, where the platform has an employee upload it, for example, then there should be responsibility on the platform. And those are cases where you might need to go to court because the platform could have prevented it, and they didn't prevent it.

So I think the bill is incredibly balanced and really innovative in its approach to protecting free speech, reducing litigation, but also effectively protecting the right that is necessary.

Chair BLACKBURN. Senator Klobuchar, you are recognized.

Senator KLOBUCHAR. All right. Thank you very much. I guess I will start with Mr. Brookman, the non-Grammy winner.

[Laughter.]

Senator KLOBUCHAR. And I want to talk to you just a little bit about this consumer angle here, which I think is interesting to people. And I think at its core, all of us involved in this legislation have made it really clear that it is not just people who are well known that will be hurt by this eventually and that getting this bill passed as soon as possible is just as important for everyone.

But I do so appreciate Ms. McBride's being willing to come forward because those stories and the stories that we have heard from, like I mentioned, Jamie Lee Curtis or the stories that we have heard from many celebrities are very important to getting this done.

So you just did a report, AI-generated voice cloning scams, including that AI voice cloning applications, in the words of the report, "presents a clear opportunity for scammers." And we need to make sure our consumer protection enforcers are prepared to respond to the growing threat of these scams. I had this happen to my State Director's husband, who their kid is in the Marines and they got a call. They figured out that it wasn't really him asking for stuff and money. They knew he couldn't call from where he was deployed to. But this is just going to be happening all over the place. And the next call will be to a grandma who thinks it is real and she sends her life savings in.

So I have called on the FTC and the FCC to step up their efforts to prevent these voice cloning scams. And what are some of the tools that agencies need to crack down on these scams, even outside of this bill?

Mr. BROOKMAN. Yes, absolutely. So I think the first thing that the Federal Trade Commission probably needs is more resources. They only have like 1,200 people right now for the entire economy. That is down from 100 just in the past couple of months.

Senator KLOBUCHAR. Way down from even during like the Nixon era.

Mr. BROOKMAN. Yes, like 1,700 it used to be and the economy has grown like three or four times. Chairman Ferguson has said more cuts are coming, which I think is the wrong direction. I worked at the Federal Trade Commission for a couple of years. We could not do like a fraction of all the things that we wanted to do to protect consumers. So people, more capacity, more technologists, like there is just not enough technology capacity in government.

I was in the Office of Technology, Research, and Investigation there. That was like five people. That is just not enough. Obviously, with all these very sophisticated—I mean, just, just deepfakes alone, let alone the rest of the tech economy. The ability to get penalties and even injunctive relief, right? If someone gets caught stealing something, the FTC often doesn't have the ability to make them give the money back.

Senator KLOBUCHAR. Yes.

Mr. BROOKMAN. I know this Committee has tried to restore that authority, but that would be important.

And also like, you know, again, maybe it is clear, FTC could have rulemaking authority, but also I would like to see Congress consider legislative authority to address tools. Like, again, if you are offering a tool that can be used only for harm, voice impersonation, deepfake pornographic images, maybe there should be responsibilities to make sure it is not being used for harm.

Senator KLOBUCHAR. Okay. Thank you.

Ms. Carlos, can you talk about what YouTube is doing to ensure it is not facilitating these scams?

Ms. CARLOS. Sure. And thank you for the question, Senator.

Senator KLOBUCHAR. And thanks for your support for the bill.

Ms. CARLOS. Of course. So just to primarily consider, we obviously see great and tremendous opportunity coming from AI, but we also acknowledge that there are risks, and it is our utmost responsibility to ensure that it is deployed responsibly. So we have taken a number of efforts to protect against unharmful contact on our platform. Primarily, we have updated our privacy policies last year to ensure that all individuals can now submit a notice to YouTube when their unauthorized voice or likeness has been used on our platform. And once reviewed, it is applicable and we have confirmed that that content should be removed, we will take it down.

We have additionally implemented watermarks on our AI products. We originally began with both image and watermarks using our SynthID technology. And we have recently expanded it to also be applied to text generated from our Gemini app and web experience and most recently, as part of our VO video tool.

Senator KLOBUCHAR. Okay.

Ms. CARLOS. We have also taken the additional step to become a member of C2PA, the Coalition for Content Provenance and Authenticity. And there, we are serving as a steering member to work

with the organization to create indicators and markings that will allow the content provenance that was created off platforms to additionally be recognized, and we are deploying those technologies across our platform.

Senator KLOBUCHAR. Okay. Thank you. We have mentioned the TAKE IT DOWN Act, and thank you for the support for that.

Mr. Glazier, you talked about how this is the first Federal law related to generative AI and that it is a good first step. And could you talk about how if we don't move on from there and we just stop and don't do anything for years, which seems to be what has been going on, what is going to happen here and why it is so important to do this?

Mr. GLAZIER. I think there is a very small window and an unusual window for Congress to get ahead of what is happening before it becomes irreparable. The TAKE IT DOWN Act was an incredible model. It was done for criminal activity, you know——

Senator KLOBUCHAR. I know.

[Laughter.]

Mr. GLAZIER. Yes, right, you know. You wrote it.

[Laughter.]

Mr. GLAZIER. It was a great model, but it only goes so far. But we need to use that model now, and we need to expand it carefully in a balanced way to lots of other situations, which is exactly what the NO FAKES Act does.

Senator KLOBUCHAR. Right.

Mr. GLAZIER. And I think, you know, we have a very limited amount of time in order to allow people and platforms to act before this gets to a point where it is so far out of the barn that instead of encouraging responsible AI development, instead, we allow investment and capital to go into——

Senator KLOBUCHAR. Into——

Mr. GLAZIER [continuing]. AI development that hurts us.

Senator KLOBUCHAR [continuing]. Stealing things, yes.

Mr. GLAZIER. So let's encourage investment the right way to boost great AI——

Senator KLOBUCHAR. Right.

Mr. GLAZIER [continuing]. Development and be first. Let's not be the folks that encourage investment in AI technologies that really harm us.

Senator KLOBUCHAR. And Ms. Price, you have expressed concerns about this 10-year moratorium on State rules. I am very concerned, having spent years trying to pass some of these things, and I think that one of the ways we pass things quickly, like Mr. Glazier was talking about, is if people actually see a reason that they don't want to patchwork, they want to get it done. But if you just put a moratorium and you look at like the ELVIS law coming out of Tennessee, Ms. McBride, and some of the other things that would stop all of that. My last question here before we go to another round, could you talk about why you are concerned about what is right in front of us now, which is this 10-year moratorium?

Ms. PRICE. Yes. Thank you for the question, Senator. We are concerned about the moratorium because it is basically signaling to the AI companies that they can kind of do whatever they want in the meantime, and it inhibits States' ability to adapt their laws to

this form of technology that is changing very quickly and then has this potential to cause great harm.

Senator KLOBUCHAR. Thank you.

Chair BLACKBURN. And I know Senator Coons is on his way and Senator Hawley is coming back, but Ms. Price, staying with you, you talked about the TAKE IT DOWN Act and the importance there, but touch on the gap that NO FAKES fills for a child who may have something posted, but yet it doesn't fit under TAKE IT DOWN and how this would open up an avenue of recourse for them.

Ms. PRICE. Yes, thank you, Senator. So under the NO FAKES Act, because there is a private right of action, there would be another way essentially for a victim to seek accountability from a perpetrator or platform, which is really important because the layers of accountability are what really deter bad actors from engaging in harm. So having the criminal, but then also having the ability to do the private right of action, the civil action is important.

Chair BLACKBURN. And speaking to the States and their actions, I do want to mention that Tennessee passed the ELVIS Act, which is like our first generation of the NO FAKES Act. And we certainly know that in Tennessee, we need those protections. And until we pass something that is federally preemptive, we can't call for a moratorium on those things, so——

Senator KLOBUCHAR. Excellent statement.

Chair BLACKBURN. Of course.

[Laughter.]

Chair BLACKBURN. Of course. Ms. Carlos, I want to talk with you for just a minute. And we are grateful for the support that you all have talked about. And there is a provision in the bill that I know is important to your platform and many others, and that's the notification piece and giving individuals harm. You have talked about artists being able to contact you, but for you all to be able to notify and letting people know about this and then asking for that content to come down and then taking that action.

As we have worked on the Kids Online Safety Act, one of the complaints that had come to Senator Blumenthal and I from individuals that tried to get things off was they could not get a response. So this is something that that notification is an imperative. So talk a little bit about how you are approaching notification.

Ms. CARLOS. Thank you. Thank you for the question. Yes, so in looking at the framework of NO FAKES, again, we began with a voluntary framework on YouTube, which allows individuals to notify us when digital replica content of them is online. And this is smartly mirrored in the NO FAKES Act. It empowers a user to identify content and flag it to us when they believe it should be removed for an unauthorized use of their voice or likeness.

And as you mentioned, that notification is critical because it signals to us the difference between content that is authorized and harmful fakes. And it is with that notice that we are able to review content and make an informed decision as to whether or not it should be removed.

Chair BLACKBURN. And then what is your length of time for getting it down upon receiving notification? What is your process going to be on implementation?

Ms. CARLOS. Sure. So as a similar framework, we envision as under the DMCA where a web form would be easily available for any user quickly filled out and then submitted to our trust and safety team. We make every effort to review every notice on a case-by-case basis and remove it as soon as possible.

Chair BLACKBURN. So are you talking hours, days? What is your framework?

Ms. CARLOS. I don't have the exact number on the top of my head, but I do know that we try to process every notification as quickly as possible.

Chair BLACKBURN. Thank you. If you will check on that——

Ms. CARLOS. Sure.

Chair BLACKBURN [continuing]. And then get that information back to us, I think we would like to know that because the fact that this has taken such lengths of time for people to have any kind of response has been very difficult for consumers, and they feel like they are talking to the outer space and nobody is listening and nobody is responding.

Ms. CARLOS. Thank you for flagging the concern. I would be happy to followup with you and the Committee.

Chair BLACKBURN. I appreciate that.

Senator Coons, you are recognized for 5 minutes.

Senator COONS. Thank you so much, Madam Chair.

I would like to first thank Ms. McBride for being here to testify in support of NO FAKES. Could you speak to why this bill is so important, both to protect artists like you and to protect your fans?

Ms. MCBRIDE. Thank you. I think that it is important because, as artists, we hopefully want to speak the truth. We want to build a relationship with our fans in which they trust us so they believe what we say. So when you have something like a deepfake that either sells a product or says a statement, it can be so harmful to that trust. You know, I mean, I just realized sitting here that I bought a product, a collagen supplement off of Instagram the other day because it had LeAnn Rimes and a couple of other people, and I am sitting here thinking, oh my goodness, I don't even know if that was really them, right? So it is damaging to the artist and to the fan.

You know, we had a situation personally where one of my fans believed they were talking to me, ended up selling their house and funneling the money to someone who they thought was me. That is so devastating to me to realize that somebody who trusts me could be duped like that, you know?

And then also I think that eventually, somebody who is duped by a deepfake is going be angry enough to have retribution, which we are on stages in front of thousands of people. We are in public places. So it is a danger to the artist as well.

Senator COONS. Mr. Glazier, to followup on Ms. McBride's testimony, what do you think are the consequences for the music industry if we don't get NO FAKES over the finish line? What will the consequences be for music fans and for the industry?

Mr. GLAZIER. The entire music ecosystem is dependent on the authentic voice and the authentic image of the artist, right? That is what the music industry is. If you allow deepfakes to perpetuate,

you are taking the soul out of the art. And when you do that, you are taking the humanity out of the art. And that is what art is.

So I think it is fairly existential that the voice of music be the voice of music. I think that is what everything is built on. And the idea, it is almost bizarre that we have to sit here today talking about allowing someone to protect the use of themselves. If there is anything that we have a right in and should be able to control, it's the gifts that God gave us, the voices that we have, the image that we have. And for that to be taken from you is devastating both for the individual and obviously for the industry itself, which is built on these very voices.

Senator COONS. Ms. Carlos, if I might, I just want to thank you for YouTube's partnership in getting to the place where you support NO FAKES. Other tech companies haven't come forward. I would be interested in what you might say or encourage me to say to the Metas or TikToks of the world about why they should support this bill, even though it imposes new obligations on them.

And some have argued that NO FAKES might show legitimate speech by incentivizing platforms to over-remove content out of fear of being sued. How does YouTube think about balancing its obligations under this bill with its First Amendment obligations to users?

Ms. CARLOS. Thank you for the question, Senator. As we mentioned, YouTube largely supports this bill because we see the incredible opportunity of AI, but we also recognize those harms, and we believe that AI needs to be deployed responsibly.

I believe Mr. Glazier mentioned during his opening statement that the NO FAKES Act does carry First Amendment exemptions: parody, satire, newsworthiness. And that is one of the reasons that we felt comfortable endorsing this bill. We are, at the end of the day, an open platform, and we believe that a variety of viewpoints can succeed on YouTube. So those would be some of the things that I would share with you to share with those other companies, but I cannot speak directly on behalf of why they may or may not choose to endorse the bill.

Senator COONS. Understood. Thank you. And thank you all for your testimony today. Thank you.

Chair BLACKBURN. Senator Hawley, you are recognized for 5 minutes.

Senator HAWLEY. Thank you very much, Madam Chair. Thanks to all of the witnesses for being here.

Ms. Carlos, if I could just start with you. You are here on behalf of YouTube, is that right?

Ms. CARLOS. That is correct.

Senator HAWLEY. Can you tell me, why is it that YouTube has monetized videos that teach people how to generate pornographic deepfakes of women? Why does that happen on your platform?

Ms. CARLOS. Thank you for the question. Protecting our users is one of our top priorities. My general expertise is in music policy, so I am not in the best position to answer that question, but I am happy to followup with you.

Senator HAWLEY. Do you know how many such videos there are out there that are—these are monetized videos now on YouTube.

Ms. CARLOS. I am not aware of that number. I can say that our community policies do not allow that type of content on our platform.

Senator HAWLEY. Well, Forbes magazine just reported that YouTube has in fact promoted over 100 YouTube videos with millions of views that showcase AI deepfake porn and include tutorials on how to make deepfake porn, particularly porn that targets young women. Do you have any idea how much money YouTube has made off of this monetization?

Ms. CARLOS. Thank you for bringing this to my attention. I do not have detail on this specific news article. I am happy to followup with you and the Committee.

Senator HAWLEY. So you don't have any idea of how many ad dollars YouTube has made off of this?

Ms. CARLOS. I do not.

Senator HAWLEY. Are you aware that one of these websites that was promoted by YouTube in these videos was later cited in a criminal prosecution for AI sexual abuse material—let me be more specific—generating AI sexual abuse material involving children?

Ms. CARLOS. Thank you again for the question, Senator. As we mentioned earlier, YouTube has endorsed the TAKE IT DOWN Act, and we take these issues very seriously. Again, I will notify that I represent music policy and do not have the information to give you a fulsome response during today's hearing.

Senator HAWLEY. Well, so let me ask you this then. If a teenage girl's face ends up in an AI porn video on your platform, what does YouTube do about it? What is her recourse right now? What can she do to get some recompense, get some restitution?

Ms. CARLOS. After over a year ago, we updated our privacy policy so that anybody who believes that their voice or likeness is being used without their authorization on our platform can submit a request for removal.

Senator HAWLEY. A request for removal. Is there some policy in getting reimbursement for any profits the company may have made, again, if these videos are monetized? I mean, does the victim get a share of anything?

Ms. CARLOS. I am not aware of those policies. I would have to followup with you, Senator.

Senator HAWLEY. Why is it that the enforcement of YouTube's own policy here seems to only happen after videos go viral? Is there a reason for that?

Ms. CARLOS. I do not have the answer to that question to you.

Senator HAWLEY. Do you know how many AI-generated deepfake videos or deepfake content is removed before a victim complains? Does the victim have to complain before YouTube does anything?

Ms. CARLOS. Again, my specialty is in music policy. I do understand that we use technology such as AI to search for that content. And when it is in violation of our policies, we will remove it.

Senator HAWLEY. Let me ask you about this. YouTube training data, has YouTube provided data for use in Google's Gemini or other AI training programs?

Ms. CARLOS. YouTube does provide data in Google training data in accordance with our agreements.

Senator HAWLEY. So if an artist uploads music to YouTube, does the company use that music to train AI models?

Ms. CARLOS. As I mentioned, we do share data in accordance with our agreements. I can't speak to the specifics of any individual agreement.

Senator HAWLEY. Well, so how are people like Ms. McBride protected? I mean, so if you are an artist and you put any content on YouTube, does that mean that it is just free range? I mean, they can do whatever you want with it?

Ms. CARLOS. Again, it goes down to the terms of our agreement. I will say that we have forged deep partnerships with the music industry. We came out of the gate with forming AI music principles with the music industry and are continuing to experiment with them to see how AI can best benefit their creative process.

Senator HAWLEY. So are there privacy protections? You are telling me YouTube has in place privacy protections for artists?

Ms. CARLOS. They apply to all individuals on our platform.

Senator HAWLEY. Oh, so this is the click wrap scenario. This is in order to watch cute dog videos or whatever, you have got to click the "I consent" and that wraps in—you basically give consent for your stuff to be used?

Ms. CARLOS. There are all different types of various agreements, but our terms of service are included in that batch of agreements.

Senator HAWLEY. I guess my question is, where are users told about their privacy protections if they have any, and where do they explicitly consent?

Ms. CARLOS. They agree to our terms of service, and we also have our privacy policy available on the web.

Senator HAWLEY. Okay. So that is the click wrap. So in other words, if you come onto YouTube, you want to use it, you click, you got to click through. So you click it, and there, you basically agreed to allow YouTube to give your content to AI and allow them to train it without any further consent. Is that basically it?

Ms. CARLOS. Again, we implement our policies in terms of our agreement are what govern what goes into our training.

Senator HAWLEY. Well, and I am asking you the content of that agreement. So in other words, if I am an artist and I upload something to YouTube and yes, sure, I have clicked the button that says, yes, I want to be able to use YouTube, are you telling me that I don't have any further recourse? If YouTube then goes and gives the information to AI models and systems, there is nothing further I can do, or am I missing something?

Ms. CARLOS. If it is in accordance with our agreements, we will share that data.

Senator HAWLEY. Yes, that seems like a big problem to me. That seems like a huge, huge problem to me. And the fact that YouTube is monetizing these kinds of videos seems like a huge, huge problem to me.

I am glad you are here today. I wish there were more tech companies here today, but we have got to do more. I mean, YouTube, I am sure, is making billions of dollars off of this. The people who are losing are the artists and the creators and the teenagers whose lives are upended. We got to give individuals powerful enforceable

rights in their images, in their property, in their lives back again, or this is just never going to stop.

Thank you, Madam Chair.

Chair BLACKBURN. Thank you. And that is the reason we have the NO FAKES bill, and we are trying to push it across the finish line.

I would like to offer a second round. Senator Klobuchar, do you have additional questions?

Senator KLOBUCHAR. Very, very short. I know that Senator Coons has asked some of my questions about just people's personal experience with this. I guess I would ask you, Mr. Glazier, I am not sure you were asked about this. Do you agree that using copyrighted materials to create copycat content undermines the value of the music created by artists and could chill creation of new art?

Mr. GLAZIER. Absolutely. You know, if you are able to copy copyrighted material for any purpose without consent, you are basically allowing the person who is copying to make the money and to do with it what they want, but not the creator who is supposed to actually control it and who made it to be compensated for it and to control its exploitation. It is the very opposite of what the Constitution calls for in creating intellectual property.

Senator KLOBUCHAR. Very good. One last question.

Chair BLACKBURN. Sure, go ahead.

Senator KLOBUCHAR. This is the last one on the consumer education issue that was raised. Thank you. I am sure you all care about it, but Mr. Brookman, so while we should not place the burden solely on consumers to protect themselves from AI scams, I don't think that is going to work very well. What steps should Congress take to help educate consumers when it comes to AI literacy and the like? I think it is something we could have some agreement on.

Mr. BROOKMAN. Yes, I think spending the money for a public awareness campaign is, I think, a really good idea. I think people, you know, hear stories of friends of friends who it has happened to, but a lot of people just have no idea that the things they see online, the things they see on Facebook are just not real. So in addition to laws——

Senator KLOBUCHAR. You know one that says I am the fourth richest woman in the world now?

Mr. BROOKMAN. Oh, congratulations.

[Laughter.]

Senator KLOBUCHAR. Yes, that is just this week. I am sorry. I don't want to exaggerate. America.

[Laughter.]

Senator KLOBUCHAR. And then people try to defend me by sending out the list of the top 10 richest with like Oprah, and I always think it is kind of sad that I am nowhere near it. But yes, that is the latest thing that is out there.

[Laughter.]

Senator KLOBUCHAR. Go on, Mr. Brookman.

Mr. BROOKMAN. Yes, training people to be aware of it, to think about it, just to, you know, watch out for social engineering attacks, false, you know, calls for urgency. You know, the deepfake voice right now is usually good for a little while, but it is getting

better, right, and it is going to continue to get better. So one idea is, you know, having a family safe word, right, a word that only you and your family know that the scammer can't get. But like they have access to a lot of personal data about us, so we are all vulnerable. The numbers are going up dramatically, so just like teaching people. Like I said, it is a shame we have to teach people to do this, but it is the world we live in.

Senator KLOBUCHAR. Okay. Thank you.

Thank you, Senator Blackburn.

Chair BLACKBURN. Senator Coons.

Senator COONS. Ms. Price, I was glad to see President Trump sign the TAKE IT DOWN Act earlier this week. Why is NO FAKES still necessary if TAKE IT DOWN is on the books?

Ms. PRICE. Thank you, Senator. No fakes is still necessary because it provides a way for victims to bring a civil lawsuit on their own behalf, and so there is an importance to having, yes, on the one hand, the criminal piece, the criminal law accountability and the required take down under the FTC, but then, of course, the victims being able to bring their own lawsuit if they wish to do that. It is more effective for deterrence to have multiple things.

Senator COONS. Ms. Carlos, why did YouTube come to the table? You could have just made it a whole lot harder for the bill to move forward if you didn't make concessions and agree to be a part of advocating for the bill.

Ms. CARLOS. Thank you for the question and thank you for including us in that round of stakeholders. So YouTube sits in a very unique kind of universe. You know, we not only have our users and music partners and media partners, but we also have creators. And that is one area where this idea of digital replicas can cause real world harm. So in addition to supporting NO FAKES, which gives them the individual right to remove content, not just from YouTube, but from other platforms, we are continuing to invest in new technology, which we refer to as likeness ID, which will allow our participating members and our pilot to have their face and voice scanned and will be able to match across our platform. So we are continuing to invest in this technology as we see it is a top issue.

Senator COONS. Thank you. Thank you very much, Senator Blackburn, Ranking Member Klobuchar.

Chair BLACKBURN. Thank you, Senator Coons.

Mr. Glazier, I want you to touch on contracts. We have had quite a discussion this week on copyright.

And as artists negotiate these contracts for their name, their image, their likeness, recently SAG–AFTRA made a move in some of their negotiations on this. But talk a little bit about the importance of having a federal standard as it relates to standard contract law.

Mr. GLAZIER. Yes, this goes to the very essence of consent for the artist. And so not only does the NO FAKES Act give control and consent to the individual about the use of their voice and the use of their likeness, it also imposes some guardrails around the length of those contracts, what those contracts mean when the person is alive, what that means after the person passes. And it also has special provisions that protect minors who might enter into con-

tracts that includes parents and guardians and also court authority.

So it does a very good job of preventing abuse while giving the power to the individual whose voice is at stake and whose image is at stake in being able to license it.

Chair BLACKBURN. Thank you so much.

Ms. Price, I want you to submit to us—you can do this in writing. When we look at the physical world and the statutes that exist for protecting individuals from some of the harms that you have listed today and the importance of TAKE IT DOWN and the importance of NO FAKES, but we don't have all of those criminal statutes that transfer to the virtual space. And I would like for you to give me a summary of your thoughts on that. Your testimony is expansive and helpful. And as I said, we have submitted that whole testimony.

Mr. Brookman, we have submitted your entire testimony also, and we thank you for that.

But I would like to have just a little bit more from you on that issue of those protections. We have talked about NO FAKES and the COPIED Act and KOSA. We talk often about this difference, and you touched on it, and I would like to have something more expansive.

With that, we have no further Members present and no further questions. I will remind you all that Members have 5 days to submit questions for the record, and then you are going to have 10 days to return those answers to us.

I thank you all. Our witnesses have been wonderful today. We appreciate your testimony for the record.

And with that, the hearing is adjourned.

[Whereupon, at 3:52 p.m., the hearing was adjourned.]

[Additional material submitted for the record follows.]

Prepared Opening Remarks
Senator Thom Tillis (R-N.C.)
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law
Hearing
"The Good, the Bad, and the Ugly: AI-Generated Deepfakes in 2025"
May 21, 2025

Thank you Senator Blackburn for inviting me to provide remarks today.

I am proud to be a co-sponsor of the NO FAKES Act and I am glad that we are looking at this bill not just in the IP Subcommittee, but also in this Subcommittee.

Deepfakes, especially those used for scams, explicit content, or in the entertainment industry, need to be stopped. And as we will hear from witnesses today, generative AI, when misused, is a real threat to creators and everyday people.

But I'm interested in how this bill affects innocent, non-commercial uses of AI. For example, if friends make harmless images of each other, would they be in trouble? What about realistic but clearly satirical images of public figures? Are those covered? I don't have all the answers yet, but I'm excited to hear the discussion.

When we make laws about AI, we need to focus on real problems and create solutions that aren't too broad or stop new ideas. We should use a "scalpel, not a chainsaw" when making AI laws.

The NO FAKES Act has big implications for everyone, not just celebrities. It will greatly affect the entertainment industry financially and, more importantly, protect personal privacy.

I look forward to working with my colleagues to pass this important bill into law.

It will be a strong defense against deepfakes for all Americans.

Thank you.

Statement of **Justin Brookman**
Director, Technology Policy
Consumer Reports

Before the Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law

The Good, the Bad, and the Ugly: AI-Generated Deepfakes in 2025

May 21, 2025

On behalf of Consumer Reports, I want to sincerely thank you for the opportunity to testify here today. We appreciate the leadership of Chairwoman Blackburn and Ranking Member Klobuchar not only for holding this important hearing, but also for working in a constructive, bipartisan fashion to develop smart and effective policy solutions to protect American consumers from increasingly sophisticated deepfake technology powered by artificial intelligence.

Founded in 1936, Consumer Reports (CR) is an independent, nonprofit, and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to our six million members across the United States.

I have been head of Technology Policy for Consumer Reports for seven years, and during all that time we have been active on AI policy.[1] We have called for stronger privacy protections for consumers' data even before the widespread advent of AI, back when the

[1] Katie McInnis, *Pre-Hearing Comments on Consumer Privacy for the Federal Trade Commission's Hearings on Competition and Consumer Protection in the 21st Century on February 12-13, 2019, FTC-2018-0098*, Consumer Reports Advocacy, (Dec. 21, 2018), https://advocacy.consumerreports.org/wp-content/uploads/2018/12/Consumer-Reports-comments-FTC-2018-0098-2.pdf.

buzzword was "Big Data" instead.[2] We have supported federal[3] and state[4] legislation and rulemaking[5] to require developers of automated decisionmaking systems to provide consumers information about how those systems work and to account for potential bias.[6] We have written about the importance of independent testing of AI systems, calling on policymakers to make changes to existing laws that often impede good faith research.[7] And of course, Consumer Reports has long been active on consumer protection as well, offering tools to educate consumers on how to protect themselves,[8] and petitioning Congress to give the Federal Trade Commission the tools it needs to more aggressively pursue wrongdoers.[9]

---

[2] Press Release, *Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace*, Consumer Reports, (Mar. 6, 2017), https://www.consumerreports.org/media-room/press-releases/2017/03/consumer_reports_launches_digital_standard_to_safeguard_consumers_security_and_privacy_in_complex_marketplace/.

[3] Press Release, *Senator Markey Introduces AI Civil Rights Act to Eliminate AI Bias, Enact Guardrails on Use of Algorithms in Decisions Impacting People's Rights, Civil Liberties, Livelihoods*, Ed Markey United States Senator for Massachusetts, (Sep. 24, 2024), https://www.markey.senate.gov/news/press-releases/senator-markey-introduces-ai-civil-rights-act-to-eliminate-ai-bias-enact-guardrails-on-use-of-algorithms-in-decisions-impacting-peoples-rights-civil-liberties-livelihoods.

[4] Grace Gedye, *Consumer Reports backs signing of high-risk AI bill, calls on Colorado General Assembly to strengthen it before it goes into effect*, Consumer Reports, (May 18, 2024), https://advocacy.consumerreports.org/press_release/consumer-reports-backs-signing-of-high-risk-ai-bill-calls-on-colorado-general-assembly-to-strengthen-it-before-it-goes-into-effect/. Gedye currently serves on the Colorado Artificial Intelligence Impact Task Force set up to make recommendations to the Colorado legislature to revise the law before it goes into effect in 2026. *See* Artificial Intelligence Impact Task Force, Colorado General Assembly, https://leg.colorado.gov/committees/artificial-intelligence-impact-task-force/2024-regular-session.

[5] Matt Schwartz and Justin Brookman, *Consumer Reports Submits Comments on the California Privacy Protection Agency's Preliminary Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking, Consumer Reports Advocacy*, (Mar. 27, 2023), https://advocacy.consumerreports.org/research/consumer-reports-submits-comments-on-the-california-privacy-protection-agencys-preliminary-rulemaking-on-cybersecurity-audits-risk-assessments-and-automated-decisionmaking; Justin Brookman *et al.*, *Consumer Reports submits comments on FTC privacy and security rulemaking*, Consumer Reports Advocacy, (Nov. 21, 2022), https://advocacy.consumerreports.org/research/consumer-reports-submits-comments-on-ftc-privacy-and-security-rulemaking/.

[6] Grace Gedye and Matt Scherer, *Opinion | Are These States About to Make a Big Mistake on AI?*, Politico, (Apr. 30, 2024), https://www.politico.com/news/magazine/2024/04/30/ai-legislation-states-mistake-00155006.

[7] Nandita Sampath, *New Paper: Opening Black Boxes: Addressing Legal Barriers to Public Interest Algorithmic Auditing*, Consumer Reports Innovation Blog, (Oct. 13, 2022), https://innovation.consumerreports.org/new-paper-opening-black-boxes-addressing-legal-barriers-to-public-interest-algorithmic-auditing/.

[8] Security Planner, Consumer Reports, https://securityplanner.consumerreports.org/.

[9] Letter from Consumer Reports to Chairwoman Rosa L. DeLauro *et al.*, (May 25, 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/05/CR-letter-on-FTC-appropriations-052521.pdf (petitioning for an increase in funding for the FTC); Testimony of Anna Laitin, Director, Financial Fairness and Legislative Strategy, Consumer Reports Before the House of Representatives Committee on Energy & Commerce Subcommittee on Consumer Protection and Commerce on "The Consumer Protection and Recovery Act: Returning Money to Defrauded Consumers," (Apr. 27, 2021), https://www.congress.gov/117/meeting/house/112501/witnesses/HHRG-117-IF17-Wstate-LaitinA-20210427.pdf (petitioning for the restoration of the FTC's 13(b) injunctive authority).

In my testimony today, I will discuss the benefits and risks to consumers from the widespread use of artificial intelligence, including detailing how deepfake technology is fuelling scams, fraud, non-consensual intimate images, and misinformation. I will focus specifically on a study that Consumer Reports released earlier this year detailing how many commercially available AI voice cloning tools let consumers generate realistic sounding audio from publicly available media, with few protections in place to protect against misuse. I will then discuss existing legal protections and consumer education efforts that have advanced significantly in recent years but which have still proved insufficient to the scope of the problem. Finally, I will discuss potential solutions including:

- Stronger enforcement bodies,
- Clearer tool and platform accountability rules,
- Transparency obligations,
- Stronger privacy and security laws,
- Whistleblower protections and incentives,
- Citizen education and better tools, and
- No moratorium on state laws.

I. The substantial benefits of artificial intelligence

As an initial matter, we must recognize the massive societal benefits from the advent of artificial intelligence, which can accomplish a broad variety of important tasks far more efficiently than traditional methods. AI is already delivering impressive public benefits, ranging from real-time translation,[10] autonomous vehicles,[11] and improved medical diagnoses.[12] Even when it comes to scams, AI does and will continue to play an important defensive role, improving spam filters and search engine ranking, identifying bad actors, and alerting consumers to potentially fraudulent solicitations.[13]

We use artificial intelligence at Consumer Reports in a variety of ways to make us more effective in our mission to deliver a fairer, safer marketplace for consumers. In our testing on privacy and security, we use AI to automate document collection and policy review to speed up product evaluations. We have used machine learning to analyze large data sets to find evidence

---

[10] Rhiannon Williams, *A new AI translation system for headphones clones multiple voices simultaneously*, MIT Technology Review, (May 9, 2025), https://www.technologyreview.com/2025/05/09/1116215/a-new-ai-translation-system-for-headphones-clones-multiple-voices-simultaneously/.

[11] Rachel Weiner and Ian Duncan, *Waymo wants to put self-driving taxis in the District next year*, Washington Post, (Mar. 25, 2025), https://www.washingtonpost.com/dc-md-va/2025/03/25/waymo-self-driving-cars-dc/.

[12] D'Adderio, L., Bates, D.W., *Transforming diagnosis through artificial intelligence*., npj Digit. Med. 8, 54 (2025). https://doi.org/10.1038/s41746-025-01460-1,

[13] Fredrik Heiding *et al.*, *Devising and Detecting Phishing Emails Using Large Language Models*, IEEE Explore, (Mar. 11, 2024), https://ieeexplore.ieee.org/document/10466545.

of racial discrimination in auto insurance prices.[14] We are looking to use AI semantic tools to expand our early warning system to monitor publicly available product reviews to detect potentially dangerous or defective products. And last year we rolled out "AskCR" — a generative-AI system designed to more effectively draw upon CR's extensive data troves to provide answers to our members' questions about various products.[15]

II. The use of AI deepfakes to power fraud and scams

However, artificial intelligence, like any tool, can be used for harm as well. And artificial intelligence is a very powerful tool. It can scrape and steal content from publicly available sources, depriving content creators of the value of their work and substituting it with AI-generated slop of dubious provenance.[16] AI can exacerbate privacy invasions, giving companies more data and power over us and the ability to personalize prices to extract greater proportions of consumer surplus from any transaction.[17] AI makes it easy to generate nonconsensual sexual images just by uploading a picture of an acquaintance or celebrity.[18] Humans can overly rely on AI and outsource critical decisions to systems that are not in fact well designed for those particular tasks — including highly consequential decisions such as hiring and benefits eligibility.[19] AI could also lead to increased corporate consolidation and perversely less innovation if only the companies with the most existing resources can take advantage of technological advances.[20] These are very real harms not solved by the existing marketplace and they need serious policy solutions.

---

[14] Jeff Larson *et al.*, *How We Examined Racial Discrimination in Auto Insurance Prices*, ProPublica and Consumer Reports, (Apr. 5, 2017), https://www.propublica.org/article/minority-neighborhoods-higher-car-insurance-premiums-methodology.
[15] AskCR, Consumer Reports, https://innovation.consumerreports.org/initiatives/askcr/.
[16] Benjamin Hoffman, *First Came 'Spam.' Now, With A.I., We've Got 'Slop'*, New York Times, (Jun. 11, 2024), https://www.nytimes.com/2024/06/11/style/ai-search-slop.html.
[17] Brian Pearson, Personalizing Price With AI: How Walmart, Kroger Do It, Forbes, (Sep. 7, 2021), https://www.forbes.com/sites/bryanpearson/2021/09/07/personalizing-price-with-ai-how-walmart-kroger-do-it/. Another way AI can lead to higher consumer prices is when multiple sellers use the same algorithm to help set prices. Using the nonpublic data from all its customers together, the AI vendor can recommend to all its customers universally higher prices, especially in markets where a greater number of market participants use its systems. *See* Hannah Garden-Monheit and Ken Merber, Price fixing by algorithm is still price fixing, Federal Trade Commission Business Blog, (Mar. 1, 2024), https://www.ftc.gov/business-guidance/blog/2024/03/price-fixing-algorithm-still-price-fixing. Indeed, some academics have suggested that even different algorithms based on different data may implicitly collude if both are independently setting prices, leading to higher costs from consumers. *See* Ariel Ezrachi and Maurice Strucke, Sustainable and Unchallenged Algorithmic Tacit Collusion, 17 Northwestern Journal of Technology and Intellectual Property 217 (2020).
[18] Matteo Wong, *High School Is Becoming a Cesspool of Sexually Explicit Deepfakes*, The Atlantic, (Sep. 26, 2024), https://www.theatlantic.com/technology/archive/2024/09/ai-generated-csam-crisis/680034/.
[19] *Objective or Biased: On the questionable use of Artificial Intelligence for job applications*, BR24, https://interaktiv.br.de/ki-bewerbung/en/,
[20] Jai Vipra and Anton Korinek, *Market concentration implications of foundation models: The Invisible Hand of ChatGPT*, Brookings, (Sep. 7, 2023), https://www.brookings.edu/articles/market-concentration-implications-of-foundation-models-the-invisible-hand-of-chatgpt/.

Beyond deepfakes which I will discuss below, AI is empowering scammers in a number of other ways. Artificial intelligence allows bad actors to automate previously laborious tasks and sometimes opens up new capabilities entirely. Recent research suggests that generative AI can be used to scale "spear phishing" — the personalization of phishing messages based on personal data to make them more convincing. By using freely available generative AI services, researchers found the cost of creating individualized spear phishing solicitations fell from $4.60 to just 12 cents per message.[21] AI allows fraudsters to spin up fake websites with just a few clicks that look like legitimate services.[22] AI could also help bad actors supercharge search engine optimization efforts to fool search engines into displaying fake customer service numbers for popular companies. (The *Washington Post* recently reported that scammers were easily able to get Google to provide fake phone numbers for companies such as Delta and Coinbase).[23]

Deepfake voice cloning

One area where Consumer Reports has focused its research is on the use of AI for voice cloning. AI voice cloning products enable consumers to clone—that is, create an artificial copy of—an individual's voice using only a short audio clip of the individual speaking. These products have many legitimate uses, including speeding up audio editing, enhancing movie dubbing, and automating narration. But without proper safeguards, they also present a clear opportunity for scammers.

AI voice cloning tools have the potential to supercharge impersonation scams, including a phone scam sometimes known as the 'Grandparent scam', in which a consumer is contacted and is told that a loved one is in trouble: they wrecked their car or they landed in jail and need money fast.[24] In the past, scammers might try to achieve a rough approximation of a young relative's voice. Now, if scammers have access to audio of a family member speaking, from, say, social media videos, they can create a potentially compelling AI clone of their voice.

This is already happening. The *Washington Post* has covered consumers who sent thousands of dollars to scammers after thinking they've heard their family member on the phone in need of help.[25] The *New Yorker* highlighted the stories of several parents sent into a state of

---

[21] Fredrik Heiding *et al.*, *Devising and Detecting Phishing Emails Using Large Language Models*, IEEE Explore, (Mar. 11, 2024), https://ieeexplore.ieee.org/document/10466545.
[22] Chris Smith, *Mind-blowing AI instantly makes artificial web pages from anything you type*, Boy Genius Report, (Jun. 26, 2024), https://bgr.com/tech/mind-blowing-ai-instantly-makes-artificial-web-pages-from-anything-you-type/.
[23] Shira Ovide, *Don't trust Google for customer service numbers. It might be a scam.*, Washington Post, (Aug. 20, 2024, https://www.washingtonpost.com/technology/2024/08/20/google-search-scams-customer-service-phone-numbers/.
[24] Consumer Alert, *Scammers use AI to enhance their family emergency schemes*, Federal Trade Commission, (Mar. 20, 2023), https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes.
[25] Pranshu Verma, *They thought loved ones were calling for help. It was an AI scam.*, Washington Post, (Mar. 5, 2023), https://www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/.

terror after thinking they heard their panicked child's voice, followed by dark threats.[26] Scammers have targeted companies as well, using AI voice tools to convince employees they are getting a call from a superior who needs them to transfer funds. In one case, the managing director of a British energy company wired $240,000 to Hungary, thinking he was speaking to his boss.[27]

This technology is also improving rapidly. The latest models now make it possible to face- and voice-swap in real time, letting scammers react and respond to their victims, while software repeats what they say in someone else's voice (and sometimes video likeness).[28] Overseas criminal enterprises are already using these tools to defraud Americans through romance and other scams.[29]

In February of last year, CR reached out to consumers across the country, asking if they had received a phone call from a scammer mimicking the voice of someone they knew, or someone well-known. We heard from consumers who said the experience left them feeling "vulnerable," "shaken by the experience," and "really weirded out":[30]

- "My Grandpa got a call from someone claiming to be me. Supposably, I was traveling, and my car broke down and I needed to have him send money so I could complete my travels. Grandpa said there was no doubt in his mind that I was the caller and was preparing to do as asked. Luckily, before he went through with the transaction, he reasoned that if I was in trouble and honestly needed money, he would have heard from my mom….Scary that the tools they use could imitate my voice that closely as to fool a close relative…" – member from Minnesota

- "The initial caller's voice sounded very much like my nephew's. He knew family details, pleaded with me not to call his father and promised to pay me back as soon as he got home - all very convincing. I should add that I spent more than 60 years in law-enforcement and intelligence work. This scam was so carefully arranged and executed that I fell for it nevertheless." – member from Massachusetts

---

[26] Charles Bethea, *The Terrifying A.I. Scam That Uses Your Loved One's Voice*, New Yorker, (Mar. 7, 2024), https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice.
[27] Drew Harwell, *An artificial-intelligence first: Voice-mimicking software reportedly used in a major theft*, Washington Post, (Sep. 4, 2019), https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/.
[28] Joseph Cox, *The Age of Realtime Deepfake Fraud Is Here*, 404 Media, (Apr. 28, 2025), https://www.404media.co/the-age-of-realtime-deepfake-fraud-is-here/.
[29] Matt Burgess, *The Real-Time Deepfake Romance Scams Have Arrived*, Wired, (Apr. 18, 2025), https://www.wired.com/story/yahoo-boys-real-time-deepfake-scams/.
[30] Member Stories, *Have you received a phone call that impersonated someone?*, Consumer Reports, https://www.consumerreports.org/stories?questionnaireId=307.

- "I received a phone call from my grandson explaining that he was in a car accident at college and needed $5,000. He sounded scared and upset and asked that I not tell his parents. So, I went to my bank to get the money and the bank teller told me it was a scam. I did not believe her as I was sure it was my grandson's voice." – member New York

- "The voice on the other end sounded just like my grandson and it said 'Gramie, I've been in an accident.'" – member from Florida

- "I was skeptical, and told him I had heard of scams such as this. So he said, 'I'll let Nate say a few words to you.' It sounded exactly like my Nate!! He has a rather unusual voice, so I was then almost convinced." – member in Indiana

- "The phone rang and a voice said, 'Hi Gramma, this is Mac. I'm in New Jersey with my friend Chris. We had an accident. I broke my nose.' I immediately knew it wasn't my grandson. He calls me Gramma Beth…and he'd have no reason to be in New Jersey. He's New York, born and bred…The voice did sound exactly like him, however, and I could easily have been duped." – member from New York

- "I received a call and heard my daughter crying hysterically! She wasn't making sense so an 'officer' took over the call. He stated I needed to come right away but would not answer my questions. Thankfully I have Life360 and looked to see where my daughter was at and it showed her at home. …To hear my daughter's crying voice shook me for a long time!" – member from Minnesota

Consumer Reports voice cloning study

In March of this year CR published a report about voice cloning tools, assessing six widely available products, recommending best practices for companies to reduce the likelihood their tools are misused for fraud, and analysing whether voice cloning tools with limited protections run afoul of existing consumer protection laws.[31]

We chose six companies that offer tools for free or at low cost and that represent a range of practices when it comes to safeguarding against the misuse of their products. For each company selected, we attempted to create a voice clone using publicly available audio of a CR employee—something that anyone could do. CR researchers were able to easily create a voice clone based on publicly available audio in four of the six products in the test set.

ElevenLabs, Speechify, PlayHT, and Lovo, did not employ any technical mechanisms to ensure researchers had the speaker's consent to generate a clone or to limit the cloning to the

[31] Grace Gedye, *New Report: Do These 6 AI Voice Cloning Companies Do Enough to Prevent Misuse?*, Consumer Reports Innovation Lab, (Mar. 10, 2025), https://innovation.consumerreports.org/new-report-do-these-6-ai-voice-cloning-companies-do-enough-to-prevent-misuse/.

user's own voice. Instead, they required only that researchers check a box confirming that they had the legal right to clone the voice or make a similar self-attestation. Descript and Resemble AI, on the other hand, took steps to make it more difficult for customers to misuse their products by requiring customers to speak a specific phrase before a clone could be created. Four of the six companies—Speechify, Lovo, PlayHT, and Descript—required only a customer's name or email address, or both, to make an account and create deepfake voice clones.

Based on our findings, and in consultation with computer scientists and experts in digital media forensics, CR made recommendations to companies, including:

- Companies should have mechanisms and protocols in place to confirm the consent of the speaker whose voice is being cloned, such as by requiring users to upload audio of a unique script.
- Companies should collect customers' credit card information, along with their names and emails, as a basic know-your-customer practice so that fraudulent audio can be traced back to specific users.
- Companies should watermark AI-generated audio for future detection and update their marking technique as research on best practices progresses.
- Companies should provide a tool that detects whether audio was generated by their own products.
- Companies should detect and prevent the unauthorized creation of clones based on the voices of influential figures, including celebrities and political figures.
- Companies should build so-called semantic guardrails into their cloning tools. These should automatically flag and prohibit the creation of audio containing phrases commonly used in scams and fraud and other forms of content likely to cause harm, such as sexual content.
- Companies should consider supervising AI voice cloning, rather than offering do-it-yourself voice products. Companies might also ensure that access to the voice model is limited to necessary actors and enter into a contractual agreement about which entity is liable if the voice model is misused.

Deepfake endorsements and reviews

AI voice and likeness cloning tools have unlocked scammers' abilities to generate deepfake videos falsely depicting celebrities and political figures endorsing products, suggesting investments, and urging citizens to take action. Recent research suggests that consumers struggle to recognize deepfake videos as false, and also overestimate their own ability to detect deepfakes.[32]

[32] Nils C Köbis *et al.*, *Fooled twice: People cannot detect deepfakes but think they can*, National Library of Medicine National Center for Biotechnology Information, (2021), https://pubmed.ncbi.nlm.nih.gov/34820608/.

AI-powered celeb-bait has proliferated on social media. An investigation by *ProPublica* identified videos on Meta seemingly depicting President-elect Trump and President Biden — each with their distinctive tone and cadence — offering cash handouts if people filled out an online form.[33] *404 Media* has reported on the spread of low-rent AI clones of Joe Rogan, Taylor Swift, Ice Cube, Andrew Tate, Oprah, and The Rock pushing Medicare and Medicaid-related scams on YouTube.[34] Scammers have used an AI clone of Taylor Swift's to hawk Le Creuset dishware.[35] Elon Musk's likeness and voice has been frequently repurposed by scammers using AI video and voice tools to push fraudulent "investment" schemes. One consumer was reportedly scammed out of $690,000 after seeing a deepfaked Elon Musk endorse an investment opportunity.[36]

AI can also make it easier to illegally promote products through the creation of mass fake reviews. Biased and downright fraudulent reviews are rampant online. Popular sites are riddled with thousands of dubious reviews, polluting the information available to consumers to make an informed choice.[37] One study finds that nearly half of reviews for clothes and apparel are faked — and, on average across all product lines, 39% of the reviews are false.[38] Another study put the number at closer to 30%.[39] And another found that online reviews are, overall, untrustworthy through a variety of metrics, including convergence with Consumer Reports ratings and resale value.[40]

---

[33] Craig Silverman and Priyanjana Bengani, *Exploiting Meta's Weaknesses, Deceptive Political Ads Thrived on Facebook and Instagram in Run-Up to Election*, ProPublica, (Oct. 31, 2024), https://www.propublica.org/article/facebook-instagram-meta-deceptive-political-ads-election.
[34] Jason Koelber, *Deepfaked Celebrity Ads Promoting Medicare Scams Run Rampant on YouTube*, 404 Media, (Jan. 9, 2024), https://www.404media.co/joe-rogan-taylor-swift-andrew-tate-ai-deepfake-youtube-medicare-ads/.
[35] Tiffany Hsu and Yiwen Lu, *No, That's Not Taylor Swift Peddling Le Creuset Cookware*, New York Times, (Jan. 9, 2024), https://www.nytimes.com/2024/01/09/technology/taylor-swift-le-creuset-ai-deepfake.html.
[36] Stuart Thompson, *How 'Deepfake Elon Musk' Became the Internet's Biggest Scammer*, New York Times, (Aug. 14, 2024), https://www.nytimes.com/interactive/2024/08/14/technology/elon-musk-ai-deepfake-scam.html.
[37] Simon Hill, *Inside the Market for Fake Amazon Reviews*, Wired, (Nov. 2, 2022), https://www.wired.com/story/fake-amazon-reviews-underground-market/; Joe Enoch, *Can You Trust Online Reviews? Here's How to Find the Fakes*, NBC News (Feb. 27, 2019), www.nbcnews.com/business/consumer/can-you-trust-online-reviews-here-s-how-find-fakes-n976756.
[38] Eric Griffith, *39 Percent of Online Reviews Are Totally Unreliable*, PCMag.com (Nov. 7, 2019), https://www.pcmag.com/news/371796/39-percent-of-online-reviews-are-totally-unreliable.
[39] Bettie Cross, *Up to 30% of online reviews are fake and most consumers can't tell the difference*, CBS Austin, (Nov. 1, 2022), https://cbsaustin.com/news/local/up-to-30-of-online-reviews-are-fake-and-most-consumers-cant-tell-the-difference.
[40] Bart de Langhe *et al*, *Navigating by the Stars: Investigating the Actual and Perceived Validity of Online User Ratings*, Journal of Consumer Research, Volume 42, Issue 6 at 818-19 (April 2016) https://www.colorado.edu/business/sites/default/files/attached-files/jcr_2016_de_langhe_fernbach_lichtenstein_0.pdf; *see also* Jake Swearingen, Hijacked Reviews on Amazon Can Trick Shoppers, Consumer Reports (Aug. 26, 2019), https://www.consumerreports.org/customer-reviews-ratings/hijacked-reviews-on-amazon-can-trick-shoppers/.

Using generative AI, a fraudster can generate dozens of realistic sounding fake reviews in seconds. Inputting into ChatGPT for example the prompt "generate ten fake five star reviews of varying length and tone for the Ukrainian DC restaurant Ruta" results in ChatGPT's response: "Here are ten fake five-star reviews for the Ukrainian restaurant Ruta, showcasing a variety of tones and lengths:" followed by ten detailed reviews praising particular dishes, the decor, and the service. Earlier this year, the FTC brought a case against the generative AI service Rytr for offering a product that would generate unlimited reviews for a product or service with limited user input — Rytr would then create detailed reviews with invented details and anecdotes.[41]

Misinformation, reputational harm, and non-consensual intimate images

AI tools can also be used to generate misinformation, spread falsehoods to damage someone's reputation, and to create non-consensual intimate images. Ahead of New Hampshire's primary election, for example, a political consultant and a magician used ElevenLabs to create an AI clone of Joe Biden's voice discouraging citizens from voting in the primary and then sent the message out as a robocall to New Hampshire voters.[42] In August of 2024, AI generated audio that sounded like former president Obama saying, about the assasination attempt against President Trump, "It was their only opportunity and these idiots missed it.[43]" In February of 2024, a fake recording created with AI of a top candidate in a Slovakian election went viral; the recordings sounded like the candidate was bragging about rigging the election and talking about raising the price of beer.[44]

AI has also been used to undermine the reputations of everyday Americans. A Maryland high school athletic director reportedly used AI voice cloning tools to mimic the voice of a school

---

[41] In the Matter of Rytr, LLC, Fed. Trade Comm'n, File No. 232-3052, Complaint, (Sep. 25, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2022/09/CR-Endorsement-Guides-comments-September-2022-3.pdf; Consumer Reports filed a comment on the Rytr proceeding in support of the settlement, arguing it was in the public interest and that Rytr's product could only be reasonably used for fraudulent purposes. *See* Justin Brookman *et al.*, Consumer Reports files comment in support of FTC's settlement with Rytr, (Nov. 4, 2024), https://advocacy.consumerreports.org/research/consumer-reports-files-comment-in-support-of-ftcs-settlement-with-rytr/.

[42] Holly Ramer and Ali Swenson, Political consultant behind fake Biden robocalls faces $6 million fine and criminal charges, Associated Press, (May 23, 2024), https://apnews.com/article/biden-robocalls-ai-new-hampshire-charges-fines-9e9cc63a71eb9c78b9bb0d1ec2aa6e9c; Maggie Astor, Behind the A.I. Robocall That Impersonated Biden: A Democratic Consultant and a Magician, New York Times, (Feb. 27, 2024), https://www.nytimes.com/2024/02/27/us/politics/ai-robocall-biden-new-hampshire.html; Vijay Balasubramaniyan, *Pindrop Reveals TTS Engine Behind Biden AI Robocall*, Pindrop, (Jan. 25, 2024), https://www.pindrop.com/article/pindrop-reveals-tts-engine-behind-biden-ai-robocall.

[43] France24, *Pro-Russia 'news' sites spew incendiary US election falsehoods*, (Aug. 19, 2024), https://www.france24.com/en/live-news/20240819-pro-russia-news-sites-spew-incendiary-us-election-falsehoods.

[44] Curt Devine *et al.*, *A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning*, CNN, (Feb. 1, 2024), https://www.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html.

principal.[45] The recording came after the athletic director and the principal had discussed the athletic director's poor work performance. The manufactured audio clip reportedly contained racist remarks about Black students' test taking abilities, as well as antisemitic comments.

Finally, by far the most common use of generative AI deepfake technology is to create non-consensual intimate images and pornography. A 2019 review of deepfakes online found that 96% were pornographic.[46] A 2023 analysis of non-consensual deepfakes covered by *Wired* found that at least 244,625 videos had been added to top websites set up to host deepfake porn videos in the preceding seven years, 113,000 of which were added in 2023, marking a 54% increase over the prior year.[47] Non-consensual intimate images, including of children, were readily found on Google image search and on Microsoft's Bing by NBC News.[48] Apps that promise to create an AI nude image based on an image of a real person are readily found online. Schools across the country, from New Jersey to Washington, have been grappling with students using AI to create non-consensual deepfakes of their fellow classmates.[49] Elected officials have also been targeted, and bad actors have attempted to use such images for blackmail.[50]

III. The Role of Tools and Platforms

In the vast majority of cases described above, scammers and fraudsters do not create AI tools themselves — instead they take advantage of commercially available resources (many of which are free or at least very low cost). Sometimes these are general purpose tools, such as ChatGPT. In other cases, they are specialized products, including products like Rytr that are overwhelmingly likely to be used predominantly for illegitimate purposes — such as pornographic deepfake generation and voice impersonation. Many of the purveyors of these high-risk applications fail to take basic precautions to try to deter bad actors from using their products for illegitimate purposes.[51]

---

[45] Ben Finley, *Athletic director used AI to frame principal with racist remarks in fake audio clip, police say*, AP News, (Apr. 25, 2024), https://apnews.com/article/ai-artificial-intelligence-principal-audio-maryland-baltimore-county-pikesville-853ed171369bcbb888eb54f55195cb9c.

[46] Tom Simonite, *Most Deepfakes Are Porn, and They're Multiplying Fast*, Wired, (Oct. 7, 2019), https://www.wired.com/story/most-deepfakes-porn-multiplying-fast/.

[47] Matt Burgess, *Deepfake Porn Is Out of Control*, Wired, (Oct. 16, 2023), https://www.wired.com/story/deepfake-porn-is-out-of-control/.

[48] Kat Tenbarge, *Fake nude photos with faces of underage celebrities top some search engine results*, NBC News, (Mar. 1, 2024), https://www.nbcnews.com/tech/internet/fake-nude-photos-faces-underage-celebrities-top-search-engine-results-rcna136828.

[49] Natasha Singer, *Teen Girls Confront an Epidemic of Deepfake Nudes in School*, New York Times, (Apr. 8, 2024), https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html. I

[50] Coralie Kraft, *Trolls Used Her Face to Make Fake Porn. There Was Nothing She Could Do.*, New York Times, (Jul. 31, 2024), https://www.nytimes.com/2024/07/31/magazine/sabrina-javellana-florida-politics-ai-porn.html.

[51] Janus Rose, *AI Tools Make It Easy to Clone Someone's Voice Without Consent*, Proof, (Jun. 25, 2024), https://www.proofnews.org/ai-tools-make-it-easy-to-clone-someones-voice-without-consent/.

Once created, scammers use other general purpose platforms to host their solicitations. Amazon is rife with fake reviews, and social media sites like YouTube and Facebook host the deepfake endorsement scams described in the previous section. Using Google to search for "voice impersonation tools" yields several different options for people to impersonate others' voices, including several sponsored results.

Nearly all online tools and platforms engage in some degree of content moderation to root out illegal activity, but in general they are underincentivized to expend sufficient resources to protect consumers.[52] Platforms that host illegal content are often explicitly immunized from responsibility by Section 230 of the Communications Decency Act.[53] In many cases, they benefit directly from the fraud, whether because they are paid by fraudsters who use their tools, they derive advertising revenue from hosting fraudulent content, they derive commissions from fraudulently endorsed products, or they benefit indirectly through artificially augmented engagement metrics which drive investors.[54]

IV. Existing Legal Protections

Scams and fraud are already illegal under a variety of federal and state civil and criminal laws. The Federal Trade Commission along with other regulators and prosecutors around the country bring numerous enforcement actions every year.[55] In September of this year, the FTC announced a law enforcement sweep entitled "Operation AI Comply" to take action against companies that have used AI to perpetrate fraud.[56] The Rytr enforcement action discussed earlier was part of that sweep, as well as a case against a company that overstated the capabilities of their AI tool, and cases against companies that promoted fraudulent AI-powered business opportunities.

---

[52] Testimony of Laurel Lehman, Policy Analyst, Consumer Reports Before the United States House of Representatives Committee on Energy & Commerce Subcommittee on Consumer Protection and Commerce on "Holding Big Tech Accountable: Legislation To Protect Online Users," (Mar. 1, 2022), https://www.congress.gov/117/meeting/house/114439/witnesses/HHRG-117-IF17-Wstate-LehmanL-20220301.pdf.

[53] 47 U.S. Code § 230, https://www.law.cornell.edu/uscode/text/47/230.

[54] Mark Scott, *Report: Social Media Networks Fail to Root Out Fake Accounts*, Politico (Dec. 6, 2019), https://www.politico.com/news/2019/12/06/social-media-networks-fake-accounts-report-076939; Nicholas Confessore *et al.*, *The Follower Factory*, N.Y. Times (Jan. 27, 2018), https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.

[55] *E.g.*, Press Release, *FTC Takes Action to Stop Online Business Opportunity Scam That Has Cost Consumers Millions*, Federal Trade Commission, (Oct. 28, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-stop-online-business-opportunity-scam-has-cost-consumers-millions.

[56] Press Release, *FTC Announces Crackdown on Deceptive AI Claims and Schemes*, Federal Trade Commission, (Sep. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes.

We are also seeing policymakers around the country enacting new laws to try to address potential abuses of AI. More than half the states have enacted laws prohibiting the use of AI to generate nonconsensual pornographic images.[57] Some states have expanded existing right-of-publicity laws to forbid the creation of digital replicas of real persons without their permission (or in the case of the deceased, their estates).[58] Twenty states have enacted comprehensive privacy laws since 2018,[59] and California passed the DELETE Act last year to make it easier for consumers to erase data broker records which could be used for targeted scams.[60] Colorado passed the first comprehensive bill designed to address potential bias in AI systems used in high-stakes decisions; the bill also requires consumer-facing AI systems to be labeled.[61] The state of California has initiated rulemaking proceedings under its privacy statute to enact similar protections for decision-making AI.[62] California also enacted an AI transparency law designed to address deceptive deepfakes: it requires generative AI products to offer deepfake detection tools and to embed invisible latent identifiers in artificial content to reflect the provenance of the image.[63] In general, after decades of failure to update the law to address the threats posed by new technologies such as the internet and social media, state legislatures have been quicker to respond to some of the threats posed by artificial intelligence.

Finally, regulators and others are ramping up user education efforts to warn consumers about the potential of AI scams and other AI-enabled fraud. Consumer Reports offers a free product called "Security Planner" to give people custom advice on the threats they are most concerned about;[64] Security Planner includes resources, for example, on how to spot phishing attempts and malicious websites posing as legitimate businesses.[65] We also publish and regularly update "The Consumer Reports Scam Protection Guide" that contains the latest

---

[57] Vittoria Elliott, *The US Needs Deepfake Porn Laws. These States Are Leading the Way*, Wired, (Sep. 5, 2024), https://www.wired.com/story/deepfake-ai-porn-laws/; *Most States Have Enacted Sexual Deepfake Laws*, multistate.ai, (Jun. 28, 2024), https://www.multistate.ai/updates/vol-32.
[58] CA AB-2602 Contracts against public policy: personal or professional services: digital replicas (2024),https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB2602 ; CA AB-1836 Use of likeness: digital replica (2024), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240AB1836; TN HB2091 "Ensuring Likeness, Voice, and Image Security (ELVIS) Act of 2024," https://legiscan.com/TN/text/HB2091/id/2900923.
[59] *Which States Have Consumer Data Privacy Laws?*, Bloomberg Law, (Sep. 10, 2024), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/.
[60] SB-362 Data broker registration: accessible deletion mechanism (2023), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202320240SB362.
[61] CO Senate Bill 24-205, The Colorado AI Act (2024), https://leg.colorado.gov/sites/default/files/2024a_205_signed.pdf.
[62] Press Release, *CPPA Adopts New Regulations for Data Brokers and Advances ADMT Rulemaking Package*, California Privacy Protection Agency, (Nov. 8, 2024), https://cppa.ca.gov/announcements/2024/20241108_2.html.
[63] CA SB-942 California AI Transparency Act (2024), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942.
[64] Security Planner, Consumer Reports, https://securityplanner.consumerreports.org/.
[65] *Spot Malicious Sites and Phishing Attempts*, Consumer Reports Security Planner, https://securityplanner.consumerreports.org/tool/protect-yourself-from-phishing.

information about evolving tactics.[66] Others like the FTC,[67] New York City,[68] and the Electronic Frontier Foundation[69] offer similar materials. The Public Interest Research Group offers helpful advice on how consumers can spot potential fake reviews.[70]

Consumer Reports is also part of a broad consumer awareness campaign called "Pause Take 9," an ambitious, nationwide public awareness initiative designed to help consumers recognize, avoid, and respond to these ever-evolving threats. At the core of this initiative is a simple but powerful message: Pause. Take nine seconds. By slowing down and taking a moment to think before acting, we can help prevent falling victim to these increasingly sophisticated scams.[71] This campaign launched last year in an effort to prepare consumers to identify potential scams — including deepfake audio and video scams — by taking a critical view of online media and to resist the false sense of urgency typically employed in social engineering attacks. Pause Take9 has already reached more than 42 million consumers nationwide—through large-scale media placements, online content and video explainers, a dedicated website, and support from over 57 partner organizations.

Finally, developers are working on new tools — often themselves powered by AI — to identify artificial content. Mozilla offers a browser extension called "Fakespot" designed to identify potential fraudulent reviews when consumers are shopping online.[72] Polyguard offers a voice communication app for wealth managers (likely targets for voice impersonation schemes) to identify potential calls from AI generated voice clones.[73] TrueMedia.org is a nonprofit organization dedicated to helping identify synthetic deepfake content.[74] As discussed above, recently enacted California legislation will also mandate that generative AI platforms create and offer AI deepfake detection tools which will hopefully increase the sophistication and adoption of such tools.[75]

---

[66] Janet Siroti, *The Consumer Reports Scam Protection Guide*, Consumer Reports, (Jul. 6, 2023), https://www.consumerreports.org/money/scams-fraud/how-to-protect-yourself-from-scams-and-fraud-a6839928990/.
[67] *Scams*, Federal Trade Commission, https://consumer.ftc.gov/scams.
[68] Tips on AI-Related Scams, NYC.gov, https://www.nyc.gov/site/dca/consumers/artificial-intelligence-scam-tips.page.
[69] *How to: Avoid Phishing Attacks*, Electronic Frontier Foundation Surveillance Self-Defense, (Jun. 24, 2024), https://ssd.eff.org/module/how-avoid-phishing-attacks.
[70] *How to recognize fake online reviews of products and services*, U.S. PIRG Education Fund, (Mar. 10, 2022), https://pirg.org/edfund/resources/how-to-recognize-fake-online-reviews-of-products-and-services/.
[71] *Nine Seconds for a Safer World*, Take9, https://pausetake9.org/.
[72] *Use AI to detect fake reviews and scams*, Fakespot, https://www.fakespot.com/.
[73] *Trusted relationships demand trusted communications.*, Polyguard, https://www.polyguard.ai/.
[74] *Identifying Political Deepfakes in Social Media using AI*, TrueMedia.org, https://www.truemedia.org/; *see also* Cade Metz and Tiffany Hsu, *An A.I. Researcher Takes On Election Deepfakes*, New York Times, (Apr. 2, 2024), https://www.nytimes.com/2024/04/02/technology/an-ai-researcher-takes-on-election-deepfakes.html.
[75] CA SB-942 California AI Transparency Act (2024), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942.

V. Solutions

Responding to the new waves of deepfakes powered by increasingly sophisticated AI is going to take a combination of legislation, enforcement, education, and cooperation from industry.

Stronger enforcement bodies

Fraud and scams are already illegal. However, because of insufficient enforcement — or consequences when caught — there is not enough deterrence against potential scammers. The FTC recently brought a handful of AI enforcement cases but those five actions are unlikely to meaningfully stem the already powerful wave of AI-power fraud.[76]

Currently, the FTC only has 1,221 FTEs total to pursue both its competition and consumer protection missions.[77] This number has decreased by nearly 100 over the last several months, and represents a decrease from 1,746 FTEs in 1979.[78] Put another way, since that time, the economy has grown nearly three times while the FTC's capacity has decreased by more than a quarter. The FTC is expected to hold giant sophisticated tech giants accountable for their transgressions, but they are severely hamstrung by unjustifiable resource constraints. Unfortunately, Chairman Ferguson recently testified that he expects the FTC to downsize even further by using "the Voluntary Early Retirement Act (VERA), the Voluntary Separation Incentive Program (VSIP), and the Deferred Resignation Program, as well as potentially through a targeted Reduction in Force (RIF), if necessary."[79] Congress cannot reasonably expect the FTC to function effectively as the primary consumer protection agency in this country if the agency's resources continue to be slashed.[80]

---

[76] Press Release, *FTC Announces Crackdown on Deceptive AI Claims and Schemes*, Federal Trade Commission, (Sep. 25, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes.

[77] Testimony of the Federal Trade Commission Before the House of Representatives Committee on Appropriations Subcommittee on Financial Services and General Government, (May 15, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-Chairman-Andrew-N-Ferguson-FSGG-Testimony-05-15-2025.pdf.

[78] *FTC Appropriation and Full-TIme Equivalent (FTE) History*, Federal Trade Commission, https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation.

[79] Testimony of the Federal Trade Commission Before the House of Representatives Committee on Appropriations Subcommittee on Financial Services and General Government, (May 15, 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-Chairman-Andrew-N-Ferguson-FSGG-Testimony-05-15-2025.pdf.

[80] The FTC's capacity is further stretched due to even more dramatic cuts at the Consumer Financial Protection Bureau, forcing the FTC to cover more of the agencies' shared responsibilities. *See* Derek Kravitz, *The Dismantling of a Financial Watchdog Is Already Harming Consumers—and Worse May Be to Come*, Consumer Reports, (Feb. 20, 2025), https://www.consumerreports.org/consumer-protection/cfpb-dismantling-is-harming-consumers-worse-may-be-to-come-a1107755089/.

Even when the FTC does manage to bring a case, they often cannot get meaningful relief from the wrongdoer. For most violations of Section 5 of the FTC Act, the FTC cannot get statutory penalties from offenders. Historically, the FTC was at least able to obtain restitution — to get back the money that consumers lost to fraudsters. However, in 2021, the Supreme Court held that the FTC's enabling statute doesn't even give them that limited authority in many instances.[81] Despite bipartisan agreement that the FTC should be empowered to, at the very least, obtain the disgorgement of fraudulent gains from wrongdoers, Congress has failed to enact legislation to restore that power.[82]

Congress should grant the FTC additional resources to hire attorneys and technologists, and expand legal powers in order to allow the agency to keep pace with the threats that plague the modern economy.

Clearer tool and platform accountability rules

Companies that offer AI tools and online platforms need clearer responsibility about how they respond to bad actors' use of those services. This could potentially be done using existing law. Section 5 of the Federal Trade Commission Act prohibits business practices that lead to significant consumer injury when that injury is not avoidable by consumers and the injury is not offset by countervailing benefits to consumers or competition.[83]

The FTC has long held that companies' failure to take action to identify and remediate harmful uses by bad actors of their products will in many cases be an unfair business practice. One analogous line of cases is the FTC's enforcement actions on data security. In nearly a hundred cases since 2005, the FTC has said that companies have a legal obligation to anticipate and respond to ways that attackers could misuse their systems to gain access to consumers' personal information.[84] In these cases, the FTC has said that companies' failure to take steps to remediate likely abuses by third parties caused a substantial likelihood of injury

---

[81] *AMG Capital Management, LLC v. Federal Trade Commission*,141 S. Ct. 1341 (2021), https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf.

[82] Testimony of Anna Laitin, Director, Financial Fairness and Legislative Strategy, Consumer Reports Before the House of Representatives Committee on Energy & Commerce Subcommittee on Consumer Protection and Commerce on "The Consumer Protection and Recovery Act: Returning Money to Defrauded Consumers," (Apr. 27, 2021), https://www.congress.gov/117/meeting/house/112501/witnesses/HHRG-117-IF17-Wstate-LaitinA-20210427.pdf.

[83] 15 U.S. Code § 45, https://www.law.cornell.edu/uscode/text/15/45.

[84] See Press Release, *BJ's Wholesale Club Settles FTC Charges*, Federal Trade Commission, (Jun. 16, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges; Press Release, *DSW Inc. Settles FTC Charges*, Federal Trade Commission, (Dec. 1, 2005), https://www.ftc.gov/news-events/news/press-releases/2005/12/dsw-inc-settles-ftc-charges; Press Release, *FTC Releases 2023 Privacy and Data Security Update*, Federal Trade Commission, (Mar. 28, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update; Staff Report, *Start with Security: A Guide for Business*, Federal Trade Commission (Jul. 2017), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

that was unavoidable by consumers and not offset by countervailing benefits to consumers or competition. As just one example, earlier this year, the FTC brought an action against the security camera company Verkada for failure to take steps to prevent attackers from accessing video feeds from consumers' cameras.[85]

Beyond data security, the FTC has held companies responsible for how others use their products to cause harm to consumers.[86] For example, the FTC successfully sued QChex for violating Section 5 for allowing any customer to create checks for any bank account number without implementing reasonable safeguards to ensure that fraudsters were not creating checks for accounts they did not control. In that case, QChex's failure to take steps to prevent foreseeable harmful and illegal uses constituted an unfair business practice.

It is important to note that an obligation to identify and remediate likely harmful behaviors does not amount to strict liability for any harm caused by another bad actor using a company's product. Section 5's requirement that any harm not be offset by countervailing benefits to consumers or competition means that companies are not expected to spend unlimited resources to try to chase down potential offenders. Instead, the FTC only intervenes when companies fail to take cost-effective measures whose implementation would have prevented an even greater risk of injury.

Product design is also an important consideration in assessing the extent to which a company must take steps to remediate potential harm from bad faith actors. If the potential harms from a platform are especially significant, or the platform's design makes it likely that it will be used for harmful purposes, then companies should have a greater obligation to expend resources to remediate those uses. QChex, for example, allowed attackers to generate checks on consumers' bank accounts; given the high risk of substantial financial harm, the company had an obligation to ensure that the check writers in fact controlled those accounts and to monitor and respond to complaints of fraud. If a company creates a product that has a high likelihood of being used for illegitimate purposes, it should have a greater obligation to take

---

[85] See Press Release, *FTC Takes Action Against Security Camera Firm Verkada over Charges it Failed to Secure Videos, Other Personal Data and Violated CAN-SPAM Act*, Federal Trade Commission, (Aug. 30, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-takes-action-against-security-camera-firm-verkada-over-charges-it-failed-secure-videos-other.

[86] See, e.g., Press Release, *FTC Sues Walmart for Facilitating Money Transfer Fraud That Fleeced Customers Out of Hundreds of Millions*, Federal Trade Commission, (Jun. 28, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-sues-walmart-facilitating-money-transfer-fraud-fleeced-customers-out-hundreds-millions; Press Release, *U.S. Circuit Court Finds Operator of Affiliate Marketing Network Responsible for Deceptive Third-Party Claims Made for LeanSpa Weight-loss Supplement*, Federal Trade Commission, (Oct. 4, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/10/us-circuit-court-finds-operator-affiliate-marketing-network-responsible-deceptive-third-party-claims; Press Release, *Court Orders Permanent Halt to Illegal Qchex Check Processing Operation Court Finds Qchex Unfair Practices Created a Dinner Bell for FraudstersOperators to Give Up All Their Ill-Gotten Gains*, Federal Trade Commission, (Feb. 9, 2009), https://www.ftc.gov/news-events/news/press-releases/2009/02/court-orders-permanent-halt-illegal-qchex-check-processing-operation-court-finds-qchex-unfair.

steps to account for those harms to ensure the harms do not outweigh any potential benefits to consumers from the product.[87]

As such, generative AI products that are likely to be predominantly used for harm — such as Rytr's review generation service or the voice impersonation companies we assessed — should have heightened obligations to address uses for illegal purposes (if they should be made commercially available at all). Those products are very likely to lead to significant consumer injury and consumers are unable to reasonably avoid them — to the contrary, the services are designed to create content that is indistinguishable from authentic content. There are limited positive use cases for these tools, so the harms caused by making these platforms generally available without reasonable safeguards in place is unlikely to be outweighed by countervailing benefits.

For more general purpose tools, the calculus is significantly more complicated. ChatGPT, for example, is a multipurpose system designed to respond to any number of constantly changing prompts — the cost of anticipating and responding to every potential abuse of the system is substantially higher. In fact, the developers of ChatGPT do consider potential misuse by bad actors and do put some limits on how the platform can be used. For example, ChatGPT regularly updates and publishes a system card identifying "Key Areas of Risk Evaluation & Mitigation," including "unauthorized voice generation" and "generating erotic and violent speech."[88] Further, making changes to account for harmful uses could also potentially constrain known or unknown positive uses of ChatGPT — another potential countervailing benefit that is less likely for narrower tools designed for specific tasks.

Nevertheless, there is a strong case that the developers of general purpose generative AI products should take more aggressive measures to prevent or deter obvious abuses (as discussed above, general purpose services comply with requests to generate multiple "fake reviews"). The extent to which such a multipurpose platform should take steps to respond to different threats is a complex question, balancing the costs of potential harm with the costs of remediation and potential limitations of beneficial uses. The same goes for platforms that host fraudulent content; if their services are causing significant harm and there are cost-effective measures they could employ to remediate that harm, they should do so.

Clarifying tool and platform responsibility for customer abuse could be done through enforcement under Section 5 and comparable state consumer protection laws. Or new legal protections could be enacted to specify what steps these companies should take and under what circumstances when their products are used to defraud consumers. For example, members of this Committee have introduced the Nurture Originals, Foster Art, and Keep Entertainment Safe (NO FAKES) Act to prohibit the creation of deepfake digital replicas without

---

[87] Press Release, *U.S. Circuit Court Finds Operator of Affiliate Marketing Network Responsible for Deceptive Third-Party Claims Made for LeanSpa Weight-loss Supplement*, Federal Trade Commission, (Oct. 4, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/10/us-circuit-court-finds-operator-affiliate-marketing-network-responsible-deceptive-third-party-claims.

[88] GPT-4o System Card, OpenAI, (Aug. 8, 2024), https://openai.com/index/gpt-4o-system-card/.

the subject's permission, and requiring platforms to remove unauthorized replicas upon notice.[89] The bill would give individuals greater rights over their personal identity and give platforms stronger incentives to remove unauthorized synthetic content. However, we are concerned that the current bill does not sufficiently deter bad faith takedown requests of legitimate, authentic media, as there is no counternotice procedure for affected speakers as exists under the Digital Millennium Copyright Act and the penalty for dishonest takedown requests is as low as $5,000 — a small price to pay for the rich and powerful to remove unwanted content for the internet. The bill's safe harbor for digital replica tools is also unduly broad, largely exempting tool developers from legal responsibilities except in the most narrow of circumstances — especially given the bill's broad preemption of state laws. And the bill could include stronger guardrails to ensure that people are not coerced or tricked into signing over the right to make digital replicas of them. Nevertheless, we are heartened to see Congress considering novel approaches to the very real problem of unauthorized digital replicas and we believe the NO FAKES bill could be an effective solution with additional targeted amendments.

Transparency obligations

As a general matter, consumers deserve to know whether the content they're interacting with is real or AI-generated. Content creators and companies should be labeling AI-generated content and chatbots as such. The fact that content is AI-generated should be communicated prominently and contextually in such a way that an ordinary consumers is likely to notice, through visual labeling (or in the case of AI-generated phone calls, through an introductory statement, as the FCC recently proposed in a rulemaking on AI-generated robocalls).[90] It should also be communicated latently through standardized metadata, watermarks, or other technology to allow platforms and agents to automatically identify content as synthetic — this approach was recently mandated in California in legislation enacted in September of last year.[91]

However, mandated transparency has limitations too, as bad actors will simply fail to provide prominent disclosures, and will endeavor to strip our latent identifiers imposed by generative platforms — or they will turn to smaller, malicious, or open-source platforms that are not covered by or otherwise do not comply with transparency obligations. For this reason, some advocates have argued against transparency obligations, noting that adversarial transparency

---

[89] Press Release, *Blackburn, Coons, Salazar, Dean, Colleagues Introduce "NO FAKES Act" to Protect Individuals and Creators from Digital Replicas*, Senator Marsha Blackburn, (Apr. 9, 2025), https://www.blackburn.senate.gov/2025/4/technology/blackburn-coons-salazar-dean-colleagues-introduce-no-fakes-act-to-protect-individuals-and-creators-from-digital-replicas.

[90] Comments of Consumer Reports on Implications on Artificial Intelligence Technologies on Protecting Consumers From Unwanted Robocalls and Robotexts, CG Docket No. 23-362, (Oct. 10, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/10/CR-Comment-on-FCC-AI-Robocall-Rulemaking-.pdf. 50,000 consumers signed onto our petition in support of our comments calling for transparency in AI-generated robocalls. *See* Grace Gedye, 50,000 consumers support FCC AI robocall rulemaking, Consumer Reports Advocacy, (Oct. 10, 2024), https://advocacy.consumerreports.org/research/50000-consumers-support-fcc-ai-robocall-rulemaking/.

[91] CA SB-942 California AI Transparency Act (2024), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240SB942.

obligations have historically been ineffective.[92] Nevertheless, we think there is a benefit in requiring transparency from actors who may be deterred from breaking the law, and over time content identification (including reliably authenticating when content is organic and legitimate) may improve.[93]

Stronger privacy and security laws

Scams are much more effective when attackers have access to personal information in order to customize a solicitation. However, the United States's privacy laws are weak, and hundreds of unregulated data brokers are able to amass detailed dossiers about all of us which are then sold to anyone willing to pay for them.[94]

The federal government has no comprehensive privacy law, and instead only has a handful of laws of varying strength covering sensitive categories of personal information such as medical, financial, and kids' data. Over the past six years, twenty states have passed their own general privacy laws, though most of those laws are too weak to meaningfully stem the flow of personal information to data brokers and advertisers.[95]

Policymakers should enact stronger privacy rules based on the principle of *data minimization* — meaning companies should only be collecting, processing, sharing, and retaining data as is reasonably necessary to deliver the goods or services requested by consumers.[96] Such a model would protect personal data *by default* rather than subject consumers to relentless requests for "opt-in" consent for superfluous data usage or forcing consumers to navigate innumerable "opt-out" mechanisms.[97]

---

[92] Jacob Hoffman-Andrews, *AI Watermarking Won't Curb Disinformation*, Electronic Frontier Foundation, (Jan. 5, 2024), https://www.eff.org/deeplinks/2024/01/ai-watermarking-wont-curb-disinformation.

[93] Grace Gedye, *CR submits testimony AI and consumer protection to New York Assembly*, Consumer Reports Advocacy, (Sep. 25, 2024), https://advocacy.consumerreports.org/research/cr-submits-testimony-ai-and-consumer-protection-to-new-york-assembly/.

[94] This Committee has published a detailed investigation into data brokers, though at this point the report is over ten years old. *See* Office of Oversight and Investigations Majority Staff, A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes, Committee on Commerce, Science, and Transportation, (Dec. 18, 2013), https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577. The situation has not materially improved in the meantime.

[95] *The State of Privacy: How state "privacy" laws fail to protect privacy and what they can do better*, Electronic Privacy Information Center and U.S. PIRG Education Fund, (Feb. 2024), https://publicinterestnetwork.org/wp-content/uploads/2024/01/State-of-Privacy-Feb.-2024.pdf.

[96] *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, Consumer Reports and the Electronic Privacy Information Center, (Jan. 26, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

[97] In 2021, Consumer Reports published model privacy legislation based on the concept of data minimization. *See Model State Privacy Act*, Consumer Reports Advocacy, (Feb. 2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf. Last year, Consumer Reports and the Electonic Privacy Information Center published a compromise approach based on the Connecticut privacy legislation that has served as a model for several other states. *See* Press Release, *Consumer Reports and the Electronic Privacy Information*

Whistleblower protections and incentives

Whistleblowers are often the only way the American public learns about the inner workings of our biggest companies — especially tech companies. Just last month, another Subcommittee of this Committee held a hearing highlighting Sarah Wynn-Williams — a former Facebook executive who recently published a book alleging sexual harassment and other misbehavior by senior management.[98] However, companies often do everything they can to stop such whistleblowers, both prophylactically through employee monitoring and non-disclosure and non-disparagement agreements and arbitration clauses in employment contracts, as well as after the fact through retaliation and legal threats. In the case of Ms. Wynn-Williams, Meta even went to court to try to block the sale and promotion of her book.[99]

Congress should enact whistleblower protections to protect insiders who publicly reveal corporate wrongdoing. Whistleblowers are especially needed in the AI space, as AI systems are notoriously inscrutable and difficult for outsiders to test and hold to account. Last year, whistleblowers from OpenAI and Google's DeepMind issued a public letter warning about the lack of safety and security protocols at those companies and criticizing the lack of legal protections for whistleblowers.[100] In 2020, Google effectively forced out a top AI ethics researcher for trying to publish a paper critiquing the kinds of algorithms (large language models) that Google uses; the paper pointed out some of the harms that can come from these models, as well as other ethical considerations concerning these algorithms.[101]

Whistleblower protections should include prohibitions on overbroad non-disclosure and non-disparagement provisions and dictate procedures for whistleblowers to escalate complaints within companies to be free from retaliation.[102] Legislation could also include incentives for

---

Center unveil new model legislation to protect the privacy of American consumers, Consumer Reports Advocacy, (Sep. 24, 2024), https://advocacy.consumerreports.org/press_release/consumer-reports-and-the-electronic-privacy-information-center-unveil-new-model-legislation-to-protect-the-privacy-of-american-consumers/.

[98] United States Committee on the Judiciary Subcommittee on Crime and Counterterrorism, *A Time for Truth: Oversight of Meta's Foreign Relations and Representations to the United States Congress*, Committee Activity and Hearings, (Apr. 9, 2025), https://www.judiciary.senate.gov/committee-activity/hearings/a-time-for-truth-oversight-of-metas-foreign-relations-and-representations-to-the-united-states-congress.

[99] Mike Isaac, Meta Seeks to Block Further Sales of Ex-Employee's Scathing Memoir, New York Times, (Mar. 12, 2025), https://www.nytimes.com/2025/03/12/technology/meta-book-sales-blocked.html.

[100] Pranshu Verma and Nitasha Tiku, *AI employees warn of technology's dangers, call for sweeping company changes,* Washington Post, (Jun. 4, 2024), https://www.washingtonpost.com/technology/2024/06/04/openai-employees-ai-whistleblowers/.

[101] Khari Johnson, *AI ethics pioneer's exit from Google involved research into risks and inequality in large language models*, VentureBeat, (Dec. 3, 2020), https://venturebeat.com/2020/12/03/ai-ethics-pioneers-exit-from-google-involved-research-into-risks-and-inequality-in-large-language-models.

[102] Nandita Sampath, *New Paper: Opening Black Boxes: Addressing Legal Barriers to Public Interest Algorithmic Auditing*, Consumer Reports Innovation Blog, (Oct. 13, 2022), at 23-24 (detailing whistleblower legislation recommendations)

insiders to report wrongdoing, such as *qui tam* provisions in False Claims Act cases and Internal Revenue System awards for people who report tax fraud. Last week, several members of this Committee introduced the bipartisan AI Whistleblower Protection Act which includes several of the protections just mentioned.[103]

Citizen education and better tools

Finally, consumers have a role to play too, and digital citizens will have to become more savvy and discriminating in a world where even very realistic looking and sounding content may be entirely AI-generated. For the last three years, Consumer Reports has published a "Cyber Readiness Report" which draws on nationally representative surveys to track the adoption of cybersecurity best practices over time.[104] While a majority of respondents did exhibit awareness of the importance of unique passwords, software updates, and multifactor authentication, adoption of more sophisticated techniques (such as use of password managers and tracker blockers) is lagging; moreover, adoption of cybersecurity best practices in general has remained fairly flat over the past three years. Institutions will need to adapt to find ways to encourage consumers to adopt more sophisticated protections over time, including protections designed to protect consumers from AI-generated deepfake scams. At the same time, researchers in industry, academia, civil society, and government will have to continue to develop new tools to help consumers identify inauthentic content. Over time, these tools need to become seamlessly embedded into browsers, mobile phone operating systems, and other platforms that consumers use to access online content.

No moratorium on state laws

The recent House budget reconciliation package included a provision that would prohibit states from enacting laws governing artificial intelligence for the next ten years.[105] Consumer Reports strongly opposes such a provision.[106] The states have been leaders on tech policy issues such as privacy for the past several years while Congress has failed to act. Despite stated concerns about a contradictory patchwork of state AI laws, in fact, relatively few laws have been passed that specifically regulate AI or automated decisionmaking. These laws have generally targeted real harms derived from the use of AI, such as the creation of deepfake

---

https://innovation.consumerreports.org/new-paper-opening-black-boxes-addressing-legal-barriers-to-public-interest-algorithmic-auditing/.

[103] Geoff Schweller, *Congress Introduces "Urgently Needed" AI Whistleblower Bill*, Whistleblower Network News, (May 15, 2025), https://whistleblowersblog.org/corporate-whistleblowers/congress-introduces-urgently-needed-ai-whistleblower-bill/

[104] Yael Grauer, *New Report: 2024 Consumer Cyber Readiness*, Consumer Reports Innovation Blog, (Oct. 1, 2024), at 4 https://innovation.consumerreports.org/new-report-2024-consumer-cyber-readiness/.

[105] Khari Johnson, Congress moves to cut off states' AI regulations, The Markup, (May 16, 2025), https://themarkup.org/artificial-intelligence/2025/05/16/congress-moves-to-cut-off-states-ai-regulations.

[106] Press Release, *Consumer Reports opposes AI state preemption language in House budget reconciliation bill*, Consumer Reports Advocacy, (May 12, 2025), https://advocacy.consumerreports.org/press_release/consumer-reports-opposes-ai-state-preemption-language-in-house-budget-reconciliation-bill/.

digital replicas and the use of blackbox decision-making systems to unfairly deprive individuals of opportunities. The language in the House budget resolution would reverse many of these protections, offer no federal protections to replace them, and prohibit the states from taking additional steps to protect their citizens. While artificial intelligence is a very promising field that can and will continue to deliver meaningful benefits for companies and consumers, simply invoking the term "AI" should not be *carte blanche* to avoid any regulation.

Thank you very much for the opportunity to testify today, and I look forward to answering your questions.

Senate Judiciary Committee
Subcommittee on Privacy, Technology & the Law
May 21, 2025

The Good, the Bad, and the Ugly: AI-Generated Deepfakes in 2025
Written Testimony
of Suzana Carlos
Head of Music Policy, YouTube

Chairwoman Blackburn, Ranking Member Klobuchar, and Members of the Subcommittee: thank you for the opportunity to speak with you today on the important topic of the NO FAKES Act and digital replicas generated by artificial intelligence. My name is Suzana Carlos, and I serve as Head of Music Policy at YouTube.

YouTube Music: Cultivating A Thriving Creative Economy

Just last month, YouTube marked the 20th anniversary of the first video ever uploaded to the platform. It is difficult to fathom how much the world and YouTube have changed in those two short decades. Today, we have over two billion active monthly users on our platform across more than 100 countries, with 500 hours of content uploaded every minute. We are proud that YouTube has transformed culture through video and built a thriving creative economy here in the United States and around the world. Thanks to our unique and industry-leading revenue-sharing model – where our creators take 55 percent of the revenue of ads running against their content – in 2024, YouTube's creative ecosystem contributed over $55 billion to US GDP and supported more than 490,000 full time jobs in the US alone.

At YouTube Music, we have built the world's deepest catalogue – over 100 million official tracks plus remixes, live performances, covers, and hard to find music you simply can't find anywhere else. We have now reached over 125 million paid YouTube Music and Premium subscribers.

AI should empower human creativity, not replace it, and that is why we are building it together with our partners - artists, songwriters, producers, executives, creatives - as we iterate for the future. Over the past two years YouTube has been laying the foundation for the future of music and AI. We started by publishing our AI Music Principles in 2023, written in collaboration with many music partners, and launched our Music AI Incubator, which now includes over 50 global participants across the ecosystem. In 2024, we accelerated this work with new 'Dream Track' experiments in YouTube Shorts, unlocked new avenues for professional creativity with the Music AI Sandbox, and introduced Google's most sophisticated video generation model, VEO, hinting at future capabilities for AI and music video production.

This year we will continue to focus on building, testing and learning for the future so that AI can assist us in ushering in a new creative era, one that enhances creative opportunities, enables innovation, and drives prosperity.

We will continue to identify the challenges and risks of AI and build solutions that benefit the entire ecosystem. If done right, we can build safe, reliable and profitable avenues for music acceleration with AI that exceeds our most ambitious goals and imaginative ideas.

Helping People Navigate AI-Generated Content

As this technology evolves, we must collectively ensure that it is used responsibly, including when it comes to protecting creators and viewers. Platforms have a responsibility to address the challenges posed by AI-generated content, and Google and YouTube stand ready to apply our expertise to help tackle them not just on our services, but across the digital ecosystem. With more people using artificial intelligence to create content, we are building on the ways in which we help our audiences identify AI-generated content through several new tools and policies.

- **Providing users with additional context:** The About this Image feature in Search helps people assess the credibility and context of images found online. The double-check feature in Gemini evaluates whether there is content across the web to substantiate the responses it provides to user queries.
- **Digital watermarking:** Google continues to bring SynthID — embedded watermarking—to additional Google Gen AI tools for content creation and more forms of media including text, audio, visual and video. For instance, images generated by Gemini, including with its most recent Imagen 3 model, are embedded with SynthID watermarks.
- **Content labels on YouTube:** The Company requires creators to disclose content that is meaningfully altered or synthetically generated when it seems realistic. It applies transparency labels to signal to users that they are watching this type of content. For most videos, a label will appear in the expanded description, but for videos that touch on more sensitive topics, YouTube also shows a more prominent label on the video itself.
- **YouTube Disclosures:** YouTube also recently introduced the "Captured with a camera" disclosure in the “How this content was made” section in the expanded description of some videos. It signifies that the creator used specific technology to verify their video's origin and confirm its audio and visuals haven’t been altered. This, along with the policy on altered and synthetic content, is part of YouTube’s efforts to increase transparency.

Beyond safeguarding its own products and platforms, we are actively collaborating across the tech industry to identify emerging challenges and counter abuse. As a 2024 steering member of the Coalition for Content Provenance and Authenticity (C2PA), we meaningfully contributed

to the development and advancement of C2PA's open standard. Google Search, Google Ads, and YouTube already detect C2PA information attached to imagery and/or videos. We will continue to expand its application to more products and use cases over time and encourage more services and hardware providers to adopt the C2PA's Content Credentials standard.

Additional Protections to Safeguard Against Unauthorized Digital Replicas

In addition to the efforts detailed above, we also have longstanding, robust policies in place that create important safeguards against misleading and deceptive content.

On YouTube, our Privacy Guidelines provide a detailed explanation of our privacy complaint process, including an outline of the factors we consider when evaluating privacy claims. We will consider content for removal if a uniquely identifiable individual or their legal representative submit the privacy complaint. When assessing if an individual is uniquely identifiable, we consider the following factors:

- Image or voice
- Full name
- Financial information
- Contact information
- Other personally identifiable information

When evaluating a privacy complaint, we consider public interest, newsworthiness, and consent as factors in our final decision with respect to removing the specific piece of content at issue.

On Google, we do not allow sites or accounts that impersonate any person or organization, or that misrepresent or conceal their ownership or primary purpose. Additionally, we do not allow sites or accounts that engage in inauthentic or coordinated behavior that misleads users. This prohibition covers, but is not limited to, sites or accounts that misrepresent or conceal their country of origin or that direct content at users in another country under false premises. It also applies to sites or accounts working together in ways that conceal or misrepresent information about their relationships or editorial independence.

We also prohibit users on Google from impersonating a person or organization or misrepresenting themselves, including by impersonating any person or organizations they do not represent or providing misleading information about a user/site's identity, qualifications, ownership, purpose, products, services, or business. We do not allow content or accounts that misrepresent or conceal their ownership or primary purpose, including by misrepresenting or intentionally concealing their country of origin or other material details about themselves when

directing content about politics, social issues, or matters of public concern to users in a country other than their own. We do allow parody, satire, and the use of pseudonyms or pen names.

Developing Practical Regulatory Frameworks

We know that a practical regulatory framework addressing digital replicas is critical. For nearly two decades, YouTube has been at the forefront of handling rights management at scale, and as we navigate the evolving world of AI, we understand the importance of collaborating with partners to tackle emerging challenges proactively.

NO FAKES Act

We know that a practical regulatory framework addressing digital replicas is critical, and we are grateful to Chairwoman Blackburn, Senator Coons, Ranking Member Klobuchar and all the bill sponsors for the smart and thoughtful approach adopted in developing the NO FAKES Act of 2025. We deeply appreciate the Members' willingness to bring a variety of stakeholders together to forge a consensus on this important topic.

Unauthorized synthetic digital imitations can be used to spread misinformation, manipulate users, and damage reputations–eroding trust in online platforms in the process. The NO FAKES Act provides a tool to combat this threat and protect the credibility of online content. Google's support for the legislation is consistent with our commitment to provide a safe and reliable online environment, as well as our own efforts to promote responsible AI development and deployment.

AI regulation should not penalize companies merely for providing tools that can be used for both permissive and non-permissive uses. The NO FAKES Act not only appropriately balances innovation, creative expression and individuals' rights, but also offers a broadly workable, tech-neutral, and comprehensive legal solution. By supplanting the need for a patchwork of inconsistent legal frameworks, the NO FAKES Act would streamline global operations for platforms like ours and empower musicians and rights holders to better manage their IP. We look forward to seeing the legislation passed by Congress and enacted into law.

YouTube and Google are proud to support the NO FAKES Act, which tackles the problem of harm associated with unauthorized digital replicas and provides a clear legal framework to address these challenges and protect individuals' rights.

TAKE IT DOWN Act

We have similarly supported the TAKE IT DOWN Act, which will be critical to preventing bad actors from producing and disseminating nonconsensual explicit images. We would like to

thank Ranking Member Klobuchar, along with Senator Cruz, for their leadership on the legislation. This is an area in which we continue to invest at Google, building on our longstanding policies and protections to ultimately help keep people safe online.

* * *

Thank you, again, for inviting me to participate in today's hearing.

Statement of Mitch Glazier
Chairman and Chief Executive Officer
Recording Industry Association of America
Before the
Subcommittee on Privacy, Technology, and the Law
Committee on the Judiciary
United States Senate
on
"The Good, the Bad, and the Ugly: AI-Generated Deepfakes in 2025"
May 21, 2025

Chairman Blackburn, Ranking Member Klobuchar, and members of the Subcommittee,

I am Mitch Glazier, Chairman and CEO of the Recording Industry Association of America, and I am honored to testify today alongside Martina McBride, a ground-breaking artist who can speak firsthand to the value of one's voice – personally and professionally – and the threats posed by abuses of deepfake technology.

RIAA is the trade organization that supports and promotes the creative and commercial vitality of music labels in the United States, the most vibrant recorded music community in the world. Our membership – which includes several hundred companies, ranging from small-to-medium-sized enterprises to global businesses – creates, manufactures and/or distributes sound recordings.

Artists' voices and likenesses are fundamental to their work, their credibility and expression, and their careers. In many ways, these deeply personal, highly valuable attributes are the foundation of the entire music ecosystem, and unauthorized exploitation of them using deepfakes can cause devastating harm. We must prevent that harm.

My deepest thanks and those of a grateful music community go out to Chairman Blackburn, Senator Coons, and Ranking Member Klobuchar for introducing the NO FAKES Act. You did it! After months of work with each other, stakeholders, and your counterparts in the House, you have been able to do something very rare these days – build bipartisan bicameral broad-based consensus around legislation that will protect not just artists, but all victims of deepfake abuses including child exploitation and voice clone scams. You have shaped a common-sense bill that has won the support of AI companies like Google, OpenAI, and IBM, as well as broadcasters, motion picture studios, child protection groups, free market groups, labor unions, and virtually the entire creative community.

The NO FAKES Act provides balanced yet effective protections for all Americans while also supporting free speech, reducing litigation, and promoting the development of AI technology.

It empowers individuals to have unlawful deepfakes removed as soon as a platform is able without requiring anyone to hire lawyers or go to court. It contains clear exemptions for uses typically protected by the First Amendment – such as parody, news reporting, and critical

commentary – so free expression and public dialogue will continue to flourish. And it paves the way for genuine AI development and innovation, targeting only malicious applications and setting the stage for legitimate licensing of these rights – but only with real and meaningful consent.

NO FAKES is the perfect next step to build on the recent and important TAKE IT DOWN Act. It provides a remedy to victims of invasive harms that go beyond the intimate images addressed by that legislation, protecting artists like Martina from non-consensual deepfakes and voice clones that breach the trust she has built with millions of fans.

American music is the most valuable in the world. We lead in investment, exports, and market power. Music drives the success of other important American industries, including the tech industry, through thriving partnerships.

If we signal to the rest of the world that it's acceptable to steal American voices and likenesses, the US has the most to lose. Our voices and our music are the most popular in the world, and will be taken the most, destabilizing the music economy, our intellectual property system, our national identity, and the very humanity of the individuals who bless us with their genius.

The NO FAKES Act is a critical step in setting America up to continue and extend its global leadership in innovation and creativity. It shows that we can protect AI innovation while preserving every individual's autonomy and protecting our property rights. We are proud to support this legislation and vow to help you pass it into law this year.

STATEMENT OF MARTINA MCBRIDE

ON S. 1367, THE "NO FAKES ACT OF 2025"

BEFORE THE SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

SENATE JUDICIARY COMMITTEE

May 21, 2025

Chairman Blackburn, Ranking Senator Klobuchar, and Members of the Subcommittee, thank you for inviting me to speak about S. 1367, the "NO FAKES Act of 2025," a landmark effort to protect human voices and likenesses from being cloned by artificial intelligence without consent. I am so grateful for the care that went into this effort, and I want to thank you both, and your colleagues, for making this issue a priority.

I started singing when I was four years old and my voice is my art form. Each of my recordings includes a piece of me that is individual and unique.

My songs reflect the human experience, and I am honored that they are a part of people's lives - from wedding vows to break-ups, to celebrating milestones and even the special relationship between a mother and daughter.

But today – my voice and likeness, along with so many others, are at risk. AI technology is amazing and can be used for so many wonderful purposes. But like all great technologies, it can also be abused, in this case by stealing people's voices and likenesses to scare and defraud families, manipulate the images of young girls in ways that are shocking to say the least, impersonate government officials, or make phony recordings posing as artists like me.

It's frightening. And it's wrong.

Congress just took a very important step forward to deal with sexually explicit deepfake images by passing the "Take It Down Act." And I want to thank all the leaders, including Senators Cruz, Klobuchar, Blackburn, and many on this Committee who worked hard with others to push that bill into law.

The NO FAKES Act is a perfect complement to that effort, by preventing AI deepfakes that steal someone's voice or likeness and use them to harass, bully, and defraud others, or to damage their career, reputation, or values.

The NO FAKES Act would give each of us the ability to say when and how AI deepfakes of our voices and likenesses can be used. If someone doesn't ask before posting a harmful deepfake, we can have it removed without jumping through unnecessary hoops or going to court.

It gives every person the power to say "yes" or "no" about how their most personal human attributes are used.

It supports AI technology by providing a roadmap for how these powerful tools can be developed the right way. And it doesn't stand in the way of protected uses like news, parodies, or criticism. I want to thank the technology companies like OpenAI and Google who support this bill, as well as the legions of creators who have worked so hard to advocate for it, and the child protection and anti sex trafficking and exploitation groups who support it and continue to fight for those who are most vulnerable.

In my career, it's been a special honor to record songs that shine a light on the battles many women fight, especially the terrible cost of domestic violence. Many fans have told me that the song "Independence Day" has given them strength, and in some cases the song has been the catalyst that has made them realize they need to leave an abusive situation.

Imagine the harm an AI deepfake could do breaching that trust, using my voice in songs that belittle or justify abuse. As an artist, a mother, a human being who cares about others – I am pleading with you to give me the tools to stop that kind of betrayal.

Setting America on the right course to develop the world's best AI while preserving the sacred qualities that make our country so special – authenticity, integrity, humanity, and our endlessly inspiring spirit – that what the NO FAKES Act will help to accomplish. I urge you to pass the bill *now*.

Thank you.

Senate Judiciary Subcommittee on Privacy, Technology, and the Law
"The Good, the Bad, and the Ugly: AI-Generated Deepfakes in 2025"

Written Testimony Submitted by:
Christen Price, Senior Legal Counsel, National Center of Sexual Exploitation
May 21, 2025

I. Introduction

Chairwoman Blackburn, Ranking Member Klobuchar, and Members of the Subcommittee: Thank you for holding this hearing and addressing a truly urgent matter that strikes at the heart of human dignity and safety.

My name is Christen Price, and I am Senior Legal Counsel at the National Center on Sexual Exploitation (NCOSE). We are a nonpartisan nonprofit, dedicated to eradicating all forms of sexual abuse and exploitation by exposing the links between them.

NCOSE's philosophy of change recognizes that while crimes have perpetrators, systemic crimes have perpetrators *and* enablers. Systemic sexual abuse often implicates mainstream, institutional facilitators, who profit from the exploitation. Our goal is to make it costly for them instead, so that they stop. To that end, the NCOSE Law Center represents sex trafficking survivors in civil lawsuits against both perpetrators and enablers, which include pornography companies.

My testimony will focus on the nature of contemporary pornography, which provides the context for sexually explicit deepfakes, discuss the rise of deepfake pornography, with its gendered and severe harms, and review legislation necessary to address the growing problem of AI deepfakes.

II. The context: contemporary pornography's pervasiveness and violence

Contemporary pornography is characterized by its pervasiveness and violence. Profits are concentrated in a few major companies, which have operated, until recently, largely with impunity.

Survey data collected between 1973 and 2010 shows pornography use among US men increased gradually over the years—from 26% in the 1970s, 30% in the 1980s, 32% in the 1990s, to 34% in the 2000s. Studies of pornography use in the US, Korea, and Australia over the last decade, by contrast, estimate that between 84% and 94% of men are regular pornography consumers.[1]

Even back in 2010, an analysis of the most popular pornography videos found physical violence in 88%.[2] This violence includes slapping, biting, hair pulling, gagging, electrocution, and

---

[1] Chyng Sun et al., "Korean Men's Pornography Use, Their Interest in Extreme Pornography, and Dyadic Sexual Relationships," *International Journal of Sexual Health* (2014): 1–20, doi:10.1080/19317611.2014.927048. Megan S. C. Lim et al., "Young Australians Use of Pornography and Associations with Sexual Risk Behaviours," *Australian and New Zealand Journal of Public Health* 41, no. 4 (2017): 438–443, https://doi.org/10.1111/1753-6405.12678, John D. Foubert, Matthew W. Brosi, and R. Sean Bannon, "Effects of Fraternity Men's Pornography Use on Bystander Intervention, Rape Myth Acceptance and Behavioral Intent to Commit Sexual Assault," *Sexual Addiction & Compulsivity: The Journal of Treatment & Prevention* 18, no. 4 (2011): 212–231, https://doi.org/10.1080/10720162.2011.625552.

[2] NCOSE, *The Public Health Harms of Pornography: Research Summaries of Key Peer-Reviewed Studies and Collection of Papers Presented at the U.S. Capitol* (Washington, DC: National Center on Sexual Exploitation, 2018), https://endsexualexploitation.org/wp-content/uploads/2021/04/NCOSE_SymposiumBriefingBooklet_1-28-2.pdf.

penetration of a woman by three or more men at the same time,[3] as well as pornography clearly depicting rape—such as when the woman is obviously unconscious or extremely impaired by alcohol or drugs.[4]

As a result, pornography is providing scripts for sexual activity in which mutuality, emotional intimacy, and affection are absent, while aggression and physically risky practices are prevalent.[5]

In addition to providing propaganda for sexual assault, pornography also normalizes sexual violence in consensual relationships. A recent BBC study surveyed over 2,000 UK men ages 18-39.[6] 71% of them admitted to using some form of violence against a partner, including slapping, spitting, and choking, much of it—by their admission—pornography inspired. 33% of those men said they did not even seek consent for these violent acts beforehand.[7]

A recent report by NCOSE's research department noted that the top four pornography websites: Pornhub, XVideos, xHamster, and XNXX, had a collective total of nearly 60 billion visits in 2024.[8] All of these websites have engaged in mass scale distribution of and profiting from non-consensual content.

For example, XVideos distributes content depicting rape. One woman, who spoke to the *New York Times*, said her husband sexually assaulted her while she was sleeping and put the video on XVideos.[9] She does not remember the attack, but the video was tagged "sleeping pills." Another woman, based in Illinois, was sex trafficked and her pimp/trafficker had posted videos of her on XVideos, four of which remained on the site despite her attempts to have them taken down. These videos were consumed by over 100,000 viewers.[10]

Legal Porno, a hardcore pornography studio owned by XVideos' parent company, has been accused of scenes so violent that women ended up in the hospital.[11] Women reported being pressured to engage in acts different from what they originally agreed to, sometimes with producers changing the scene in the middle of shooting.[12] One woman was unable to complete a

---

[3] Ibid. See also Gail Dines, "Introduction," in *Pornland: How Porn has Hijacked our Sexuality* (Boston, MA: Beacon Press, 2010), xx-xix. Dines searched for "porn" in Google, and these were the most popular acts she found.
[4] Megha Mohan, "'I was Raped at 14, and the Video Ended Up on a Porn Site'," *BBC,* February 9, 2020, https://www.bbc.com/news/stories-51391981.
[5] NCOSE, *The Public Health Harms of Pornography: Research Summaries of Key Peer-Reviewed Studies and Collection of Papers Presented at the U.S. Capitol* (Washington, DC: National Center on Sexual Exploitation, 2018), https://endsexualexploitation.org/wp-content/uploads/2021/04/NCOSE_SymposiumBriefingBooklet_1-28-2.pdf.
[6] Myles Bonnar, "'I Thought He was Going to Tear Chunks Out of my Skin'," *BBC,* March 22, 2020, https://www.bbc.com/news/uk-scotland-51967295.
[7] Ibid.
[8] NCOSE, *The Public Health Harms of Pornography: Research Summaries of Key Peer-Reviewed Studies and Collection of Papers Presented at the U.S. Capitol* (Washington, DC: National Center on Sexual Exploitation, 2018), 4, 7-9, https://endsexualexploitation.org/wp-content/uploads/2021/04/NCOSE_SymposiumBriefingBooklet_1-28-2.pdf.
[9] Nicholas Kristof, "Why Do We Let Corporations Profit From Rape Videos?" *The New York Times*, April 16, 2021, https://www.nytimes.com/2021/04/16/opinion/sunday/companies-online-rape-videos.html.
[10] Ibid.
[11] Jakub Zelenka & Lukas Prchal, "'I was Bleeding and Ended Up in Hospital.' Women Accuse Producers of XVideos of Violent Porn Shooting," *Deník N*, February 2021, https://denikn.cz/552186/i-was-bleeding-and-ended-up-in-hospital-women-accuse-producers-of-xvideos-of-violent-porn-shooting/?ref=list.
[12] Ibid.

scene due to bleeding and extreme pain, and was forced to leave without being paid anything.[13] Another woman wrote on Twitter that she had a serious prolapse injury after a shoot with Legal Porno.[14]

Czech Casting, an XVideos content partner, was investigated in 2020 for sex trafficking and rape due to manipulating people into creating pornography, in part by telling women it would be a professional modeling shoot.[15] The Czech police arrested 10 people and charged 9 of them.[16] As of May, 18, 2025, a Google search indicates that Czech Casting continues to have a channel page on XVideos.[17]

The inclusion on Pornhub of child sexual abuse material (CSAM), sex trafficking content, recorded sexual assault, and other abusive content is similarly well documented.[18] Nicholas Kristof's 2020 investigation for the *New York Times* uncovered scenes of women being "asphyxiated in plastic bags" and scenes where the women were clearly unconscious.[19] Pornhub employees have admitted that sex traffickers and other criminal actors use its site with impunity.[20]

III. The problem: deepfake pornography

This content forms the backdrop for a more recent phenomenon: sexually explicit deepfakes or deepfake pornography, a sub-category of image-based sexual abuse (IBSA). This violent, abusive content merges forged pornography with other women and girls' faces; It's also what AI-generated pornography has been trained on.[21]

IBSA, broadly, is the "sexual violation of a person committed through the abuse, exploitation, or weaponization of any image depicting the person,"[22] and includes nonconsensual distribution of

---

[13] Ibid.
[14] Ibid.
[15] Prague Morning, "Czech Casting: Women Lured By Modeling Gigs, Manipulated Into Shooting Porn," *Prague Morning,* July 18, 2020, https://www.praguemorning.cz/czech-casting-women-lured-by-modeling-gigs-manipulated-into-porn.
[16] Policie Ceske Republiky, "Czech Casting – 9 People Accused," news release, July 17, 2020, https://www.policie.cz/clanek/czech-casting-obvineni-9-osob.aspx.
[17] See XVIDEOS.COM, *CZECH CASTING CHANNEL*, https://www.xvideos.com/channels/czech-casting-1.
[18] See, e.g., Doe v. MG Freesites, LTD, No. 7:21-CV-00220-LSC, 2024 WL 5339485, at *1 (N.D. Ala. Dec. 19, 2024) (denying motion for summary judgment from Pornhub's parent company on CSAM and sex trafficking claims).
[19] Kristof writes: "Yet there's another side of the company: Its site is infested with rape videos. It monetizes child rapes, revenge pornography, spy cam videos of women showering, racist and misogynist content, and footage of women being asphyxiated in plastic bags." Nicholas Kristof, "The Children of Pornhub," *The New York Times,* December 4, 2020, https://www.nytimes.com/2020/12/04/opinion/sunday/pornhub-rape-trafficking.html.
[20] Sound Investigations, "Pornhub Exec: Rapists, Traffickers Using Pornhub 'Loophole' to 'Make a Lot of Money'," Rumble, September 13, 2023, 12 min., https://rumble.com/v3ha3zc-pornhub-exec-rapists-traffickers-using-pornhub-loophole-to-make-a-lot-of-mo.html?e9s=src_v1_upp; Sound Investigations, "Undercover Vid: Fmr Aylo Compliance Employee Reveals 'So Much Room for Error' in Unverified P*rn Ads," Rumble, August 10, 2023, 13 min., 40 sec., https://rumble.com/v3t0u7a-undercover-vid-fmr-aylo-compliance-employee-reveals-so-much-room-for-error-.html?e9s=src_v1_upp.
[21] Lisa Thompson et al., *Not a Fantasy: How the Pornography Industry Exploits Image-based Sexual Abuse in Real Life* (Washington, DC: National Center on Sexual Exploitation, 2025), 50, https://endsexualexploitation.org/wp-content/uploads/Not-a-Fantasy-Report_NCOSE.pdf.
[22] Lisa Thompson et al., *Identifying Image-based Sexual Abuse: Classifications and Definitions* (Washington, DC: National Center on Sexual Exploitation, August 2024), https://endsexualexploitation.org/wp-content/uploads/NCOSE_IBSA-Chart_Identifying-Image-based-Sexual-Abuse_FINAL.pdf.

sexually explicit content, recording sexual violence, sexual extortion (such as using sexually explicit images to blackmail a person into sending money to the perpetrator), video voyeurism (including upskirting and spycam pornography), and AI-generated forged (deepfake) pornography.[23]

Forged pornography is rapidly escalating, deeply gendered, and devastating for its victims. Examples abound:

- As a junior in high school, Brooke Currey discovered that a boy she had never met had taken a photo off her Instagram to generate an AI "deepfake" and circulated it via Snapchat. Two years later, she still has not been able to get all of the images removed and has no idea who has seen them.[24]
- At least 30 Illinois students had images of themselves altered into sexually explicit images and shared with their classmates. The list of victims included three teachers. Victims described the discovery as disturbing, alarming, and upsetting. One student was suspected of causing the harm.[25]
- Molly Kelley, a woman from Minnesota, is one of 85 women who had deepfake pornography created of her by a close family friend. She said, "My only crime was existing online and sharing photos on platforms like Instagram. The person who did this was not a stranger. I was not hacked. And my social media has never been public." She worries about the impact to her career, her reputation, and her family.[26]
- A psychiatrist in Charlotte, South Carolina was found guilty of using AI to digitally alter clothed images of minors into child sexual abuse images. Some of the victims included his former classmates, now in their 40s, who are victims of CSAM as a result of images taken two decades prior. Many of his victims were unknown to him.[27]
- Bree Smith, a Nashville meteorologist, was forced to quit her job after months of fighting against AI deepfakes of her that circulated online. The images multiplied, and scammers circulated them with offers for private dinners and sexual acts in exchange for hundreds of dollars. She's terrified that her children will encounter these videos online. She has been unable to get the images removed and is tracking accounts that repost them.[28]

A. Forged pornography is growing and profitable

---

[23] Ibid.
[24] A.G. Gancarski, "How a Deepfake Changed Brooke Curry's Life, and What She's Doing About It," *Florida Politics,* April 7, 2025, https://floridapolitics.com/archives/730515-how-a-deepfake-changed-brooke-currys-life-and-what-shes-doing-about-it.
[25] Charlie De Mar, "Students at Illinois High School Say Photos were Altered by AI to be Explicit," *CBS News,* March 14, 2024, https://www.cbsnews.com/chicago/news/illinois-high-school-photos-altered-ai-explicit.
[26] William Lien, "Protecting Victims of Non-Consensual Deepfake Pornography," *WDIO ABC,* December 17, 2024, https://www.wdio.com/front-page/top-stories/protecting-victims-of-non-consensual-deepfake-pornography.
[27] FBI News, "'Horribly Twisted' Charlotte Pornography Case Shows the 'Unsettling' Reach of AI-generated Imagery," *FBI News,* April 29, 2024, https://www.fbi.gov/news/stories/charlotte-child-sexual-abuse-material-case-shows-unsettling-reach-of-ai-generated-imagery.
[28] Nicole Valdes and Emily Mae Czachor, "Former TV Meteorologist Fights Deepfakes after her Image was Doctored in Sextortion Scams," *CBS News,* May 1, 2025, https://www.cbsnews.com/news/deepfakes-meteorologist-bree-smith-image-doctored-sextortion-scams.

In 2018, the year the first site dedicated to deepfake pornography was launched, "the top four dedicated sexual deepfake websites harness[ed] over 134 million views."[29]

Deepfakes are nonconsensual by definition, yet one company found that in a two-year period, between 2018 and 2020, the total number of deepfake videos "doubled every sixth months [.]".[30] Malicious and pornography deepfakes made up 93% of the videos.[31]

A 2023 report found the availability of AI-generated forged pornography online increased by 464% between 2022 and 2023.[32] There were 303,640,207 total video views across the top 10 dedicated deepfake pornography websites in 2023, with total traffic of 34,836,914 across these sites.[33]

Xvids and XNXX returned more than 170,000 results for "deep fake" in February 2025.[34] (Both owned by the same company). Searches for "AI" on Pornhub returned over 48,000 results in 2023, and "AI porn" returned more than 400,000 results on XVideos and XNXX in February 2025. [35] Mr. Deepfakes, the most prominent of the pornographic deepfake sites, had 13 million monthly visitors and 250,000 members in 2023.[36] The site recently closed down after Congress passed the Take It Down Act.[37]

Deepfake pornography includes CSAM. The National Center on Missing and Exploited Children (NCMEC) reported that its CyberTipline received 67,000 AI-related reports in 2024, up from 4,700 in 2023, representing a "1,325% increase in reports involving Generative AI[.]"[38]

Underground CSAM trading networks are disseminating AI-generated CSAM as well. The Internet Watch Foundation (IWF) reported in 2023 that one forum posted more than 20,000 images of AI-CSAM in a one-month period and that "there's jubilation that fantasies can be made to order" among perpetrators.[39] In a July 2024 report, the IWF found that 90% of AI-

---

[29] Victoria Rousay, "Sexual Deepfakes and Image-based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms" (Master's thesis, Harvard University, Division of Continuing Education, 2023), 21, https://dash.harvard.edu/handle/1/37374909.
[30] Ibid, citing footnote 55.
[31] Ibid.
[32] Home Security Heroes, "2023 State of Deepfakes," Infographic, accessed March 5, 2024, https://www.homesecurityheroes.com/state-of-deepfakes/assets/pdf/state-of-deepfake-infographic-2023.pdf.
[33] Ibid.
[34] XVideos and XNXX are owned by the same parent company, WebGroup Czech Republic (WGCZ) Holdings. See: Lisa Thompson et al., *Not a Fantasy: How the Pornography Industry Exploits Image-based Sexual Abuse in Real Life* (Washington, DC: National Center on Sexual Exploitation, 2025), https://endsexualexploitation.org/wp-content/uploads/Not-a-Fantasy-Report_NCOSE.pdf; See also: Complaint, Doe v. WebGroup Czech Republic, No. 221CV02428VAPSKX (C.D. Cal. Mar. 18, 2021), https://endsexualexploitation.org/wp-content/uploads/Xvideos-complaint-as-filed_Jane-Doe-v.-WebGroup-Czech-Republic-et-al_03-18-2021.pdf.
[35] Lisa Thompson et al., *Not a Fantasy: How the Pornography Industry Exploits Image-based Sexual Abuse in Real Life* (Washington, DC: National Center on Sexual Exploitation, 2025), 23, https://endsexualexploitation.org/wp-content/uploads/Not-a-Fantasy-Report_NCOSE.pdf.
[36] Victoria Rousay, "Sexual Deepfakes and Image-based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms" (Master's thesis, Harvard University, Division of Continuing Education, 2023), 31, https://dash.harvard.edu/handle/1/37374909.
[37] Layla Ferris, "AI-generated Porn Site Mr. Deepfakes Shuts Down after Service Provider Pulls Support," *CBS News*, May 5, 2025, https://www.cbsnews.com/news/ai-generated-porn-site-mr-deepfakes-shuts-down.
[38] NCMEC, "2024 CyberTipline Report," National Center for Missing & Exploited Children, accessed May 19, 2025, https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.
[39] Internet Watch Foundation, *How AI is being Abused to Create Child Sexual Abuse Imagery* (Cambridge, UK: Internet Watch Foundation, October 2023), https://www.iwf.org.uk/media/q4zll2ya/iwf-ai-csam-report_public-oct23v1.pdf.

CSAM images assessed by IWF analysts were "realistic enough to be assessed as pseudo-photographs of children[.]"[40]

Websites dedicated to deepfake pornography use online advertising to profit,[41] just as more mainstream pornography sites do. Pornhub has been found hosting advertisements and referral links for deepfake pornography sites using nonconsensual deepfake depictions of people.[42]

B. Forged pornography is deeply gendered

Deepfake pornography is deeply gendered, and the difference is stark and growing. Between 2018 and 2020, 90% of deepfake pornography content targeted women, primarily.[43] Disturbingly, the 2023 State of Deepfakes report found 98% of all deepfake videos online are pornography-related and 99% of the individuals targeted in deepfake pornography are women.[44]

Nudify apps that strip people—overwhelming women and girls—of their clothes are numerous and easily accessible on Apple's App Store and Google's Play Store. These apps allow any image to be virtually stripped of clothing within seconds. In school districts across the US, boys are using AI-powered apps to transform clothed pictures of female classmates into nude images.[45] Research has revealed that 34 providers of nudifying technology received more than 24 million unique visitors to their websites during the month of September 2023.[46]

One AI bot "had only been trained on female genitalia and could only 'strip' or 'nudify' images/videos of women. Current 'nudifying' websites/applications advertise their strong opposition to creating training sets or bots that could strip different genders because it would interfere with the overarching goal of 'making men's dreams come true.'"[47]

---

[40] Internet Watch Foundation, *What Has Changed in the AI CSAM Landscape? AI CSAM Report Update in Conjunction with our Oct 23 Report* (Internet Watch Foundation, July 2024), https://www.iwf.org.uk/media/drufozvi/iwf-ai-csam-report_update-public-jul24v12.pdf.

[41] "For many adult websites that allow users to upload their own content, similar to MrDeepFakes, advertisements make up a considerable amount of income." Emma K. Chedwick, "Synthetic Seduction: Navigating AI-Generated Content and the Complexities of Name, Image, and Likeness Law," *The Business, Entrepreneurship & Tax Law Review* 8, no. 1 (2024): 168, 176, https://scholarship.law.missouri.edu/betr/vol8/iss1/8.

[42] Alyssa Mercante, "Popular Female Twitch Streamers Targeted In Deepfake Pornography Scandal," *Kotaku,* January 31, 2023, https://kotaku.com/deepfake-atrioc-twitch-streamer-apology-legal-action-1850055762?sm_guid=NzcxOTIyfDc4MzA5NjAxfC0xfGNlc2VAbmNvc2UuY29tfDcyMDIwMTJ8fDB8MHwyMjU0MzA0NTd8MTEzMnwwfDB8fDc2NjM5Nnww0.

[43] Victoria Rousay, "Sexual Deepfakes and Image-based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms" (Master's thesis, Harvard University, Division of Continuing Education, 2023), 21, https://dash.harvard.edu/handle/1/37374909, citing footnote 55.

[44] Home Security Heroes, "2023 State of Deepfakes," Infographic, accessed March 5, 2024, https://www.homesecurityheroes.com/state-of-deepfakes/assets/pdf/state-of-deepfake-infographic-2023.pdf.

[45] Natasha Singer, "Teen Girls Confront an Epidemic of Deepfake Nudes in Schools," *The New York Times,* April 8, 2024, https://www.nytimes.com/2024/04/08/technology/deepfake-ai-nudes-westfield-high-school.html; Caroline Haskins, "A Deepfake Nude Generator Reveals a Chilling Look at Its Victims," *Wired,* March 25, 2024, https://www.wired.com/story/deepfake-nude-generator-chilling-look-at-its-victims.

[46] Santiago Lakatos, "A Revealing Picture: AI-Generated 'Undressing' Images Move from Niche Pornography Discussion Forums to a Scaled and Monetized Online Business," *Graphika,* December 2023.

[47] Victoria Rousay, "Sexual Deepfakes and Image-based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms" (Master's thesis, Harvard University, Division of Continuing Education, 2023), 30 (internal citations omitted), https://dash.harvard.edu/handle/1/37374909.

Further, "the volume of referral link spam for these services has increased by more than 2,000% on platforms including Reddit and X since the beginning of 2023," and in September of 2023, there were at least 1 million users of 52 Telegram groups used to create AI-IBSA.[48]

As journalist Nicholas Kristof documented, the videos being "created are graphic and sometimes sadistic, depicting women tied up as they are raped or urinated on, for example. One site offers categories including 'rape' (472 items), 'crying' (655) and 'degradation' (822)."[49] Kristof also found one deepfake website that displays the official portrait of a female member of Congress, as well as more than two dozen forged pornographic videos of her.[50]

Perpetrators of pornographic deepfake sexual abuse are disproportionately male.[51]

The attitudes of men who create and consume this abusive content are telling. The owner of Mr. Deepfakes himself said: "'I think that as long as you're not trying to pass it off as a real thing, that should really matter because it's basically fake. I don't really feel that consent is required—it's a fantasy, it's not real.'"[52] Most consumers of the abuse agree, as the State of Deep Fakes report found "74% of deepfake pornography users don't feel guilty about it[.]"[53]

C. Forged pornography is devastatingly harmful

Deepfake pornography is a serious human rights abuse, which violates the dignity and autonomy of both the person whose face is depicted, and the person whose body is shown. These violations of privacy and the right to the integrity of one's own body have profound emotional and physical effects. Survivors report anxiety, PTSD, depression, shame, and humiliation. They feel robbed of their autonomy, their sexuality, and their trust in people and technology alike. These aren't just emotional scars; they are life-altering wounds: "In recent research, victims of IBSA and sexual deepfakes have portrayed their experiences as ones of irreparable harm that 'forever changed' their lives. Victims have described feelings of shock, fear, isolation, embarrassment, shame, powerlessness, and objectification after discovering deepfake pornography in their likeness."[54]

Some victims, overwhelmingly female, grapple with suicidal ideation because of the sheer magnitude of this violation. For some women and girls, the harm was ultimately too overwhelming and they died by suicide.[55]

---

[48] Santiago Lakatos, "A Revealing Picture: AI-Generated 'Undressing' Images Move from Niche Pornography Discussion Forums to a Scaled and Monetized Online Business," *Graphika,* December 2023.
[49] Nicholas Kristof, "The Online Degradation of Women and Girls that We Meet with a Shrug," *The New York Times*, March 23, 2024, https://www.nytimes.com/2024/03/23/opinion/deepfake-sex-videos.html?pgtype=Article&action=click&module=RelatedLinks.
[50] Ibid.
[51] Victoria Rousay, "Sexual Deepfakes and Image-based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms" (Master's thesis, Harvard University, Division of Continuing Education, 2023), 123, https://dash.harvard.edu/handle/1/37374909.
[52] Ibid, 47.
[53] Security Hero, "Key Findings," 2023 State of Deepfakes: Realities, Threats, and Impact, accessed May 19, 2025, https://www.securityhero.io/state-of-deepfakes/#key-findings.
[54] Victoria Rousay, "Sexual Deepfakes and Image-based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms" (Master's thesis, Harvard University, Division of Continuing Education, 2023), https://dash.harvard.edu/handle/1/37374909.
[55] Victoria Rousay, "Sexual Deepfakes and Image-based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms" (Master's thesis, Harvard University, Division of Continuing Education, 2023), 18-19, https://dash.harvard.edu/handle/1/37374909. See also BBC, "Two Arrested in Egypt after Teenage Girl's Suicide Sparks Outrage," *BBC,* January 4, 2022, https://www.bbc.com/news/world-middle-east-

Deepfakes also provide an additional avenue for obtaining or maintaining coercive control over a partner and could make relationships characterized by intimate partner violence even more dangerous.[56] Women have been targeted with deepfake pornography for speaking out about male violence.[57] In some cases, sex buyers harassed victims.[58]

Deepfakes and the harassing aftermath interferes with women and girls going to school, getting and maintaining jobs, and otherwise participating in public life,[59] often, ultimately, having a profound silencing effect.

This is a form of sexual exploitation from which it is impossible to fully exit, as that would require scrubbing the abuse content at issue from the entire internet, as well as from the hard drives of anyone who downloaded it. Harm stemming from the continuing nature of the violation seems to be a more common experience for female victims than male victims of deepfake pornography. [60] Thus, given the breadth, severity, and irreparable nature of these harms, deterrence and prevention are essential.

IV. Conclusion: the importance of acting now

Deepfakes are escalating rapidly, with devastating consequences, but there is time for Congress to act to set the terms and framework now, to signal to current and would-be perpetrators and facilitators that these abuses will not be tolerated.

Deterrence is particularly important in this space because of the irreparable nature of the damage. Deepfake pornography degrades, intimidates, and silences women and girls. That is what it is intended to do. There is a very old idea, that in order to protect more privileged women from

---

59868721?sm_guid=NzcxOTIyfDc4MzA5NjAxfC0xfGNlc2VAbmNvc2UuY29tfDcyMDIwMTJ8fDB8MHwyMjU0MzA0NTd8MTEzMnwwfDB8fDc2NjM5Nnww0.

[56] See, e.g., Megan Riesmeyer, "The Dark Side of Technological Advances: How Technology Has Enabled Domestic Violence and the Contributing Role of the First Amendment," *Gonzaga Law Review* 59, no. 1 (2024): 93, 128, https://gonzaga-law-review.scholasticahq.com/article/92486-the-dark-side-of-technological-advances-how-technology-has-enabled-domestic-violence-and-the-contributing-role-of-the-first-amendment; Stacey A. Cozewith, "How AI and Deepfakes Can Impact Domestic Violence Cases," N.J. Law., December 2024, at 29, 30, https://www.saiber.com/insights/publications/2024-12-16-how-ai-and-deepfakes-can-impact-domestic-violence-cases.

[57] Victoria Rousay, "Sexual Deepfakes and Image-based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms" (Master's thesis, Harvard University, Division of Continuing Education, 2023), 18 https://dash.harvard.edu/handle/1/37374909.

[58] Ibid.

[59] Abigail George, "Defamation in the Time of Deepfakes," *Columbia Journal of Gender and Law* 45, no. 1 (2024): 122, 167, https://doi.org/10.52214/cjgl.v45i1.13186 (describing a woman who was fired after her boss learned she was a victim of deepfake pornography); Emily Pascale, "Deeply Dehumanizing, Degrading, and Violating: Deepfake Pornography and the Path to Legal Recourse," *Syracuse Law Review* 73 (2023): 335, 341, https://lawreview.syr.edu/wp-content/uploads/2023/03/Pascale-335-366.pdf (describing the employment consequences for victims of deepfake pornography).

[60] Men in the study did not report the same level of lasting consequences. "Female participants did not describe the same sense of healing after the initial event, as their abuse was continuous, often escalating or radiating over time. The continuation of abuse often transcended the boundaries of the virtual and physical through the comments and threats women received long after the initial event had occurred." See Victoria Rousay, "Sexual Deepfakes and Image-based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms" (Master's thesis, Harvard University, Division of Continuing Education, 2023), 93-94, https://dash.harvard.edu/handle/1/37374909.

male violence, you need an underclass of women that men can violate with impunity.[61] This was always a morally inexcusable premise, and the rise of forged pornography shows that it was also a lie. The rapid increase and popularity of a technology that allows any man to turn any woman into his pornography represents a swift democratization of sexual objectification.

These are impossible conditions for equality. Andrea Dworkin stated in 1986, very presciently, what the effect would be on women, if pornography became ubiquitous:

> [W]e see the torture of women as a form of entertainment, and we see women also suffering the injury of objectification—that is to say we are dehumanized. We are treated as if we are subhuman, and that is a precondition for violence against us... When your rape is entertainment, your worthlessness is absolute. You have reached the nadir of social worthlessness. The civil impact of pornography on women is staggering. It keeps us socially silent, it keeps us socially compliant, it keeps us afraid in neighborhoods; and it creates a vast hopelessness for women, a vast despair. One lives inside a nightmare of sexual abuse that is both actual and potential, and you have the great joy of knowing that your nightmare is someone else's freedom and someone else's fun.[62]

This horrible reality, emerging before our eyes, is the reason why NCOSE helped lead the bipartisan legislative effort to pass the Take It Down Act, signed by President Trump on Monday [May 19]. NCOSE was honored to participate in this historic White House signing ceremony. The Take It Down Act targets not only the person who creates abuse videos and images, but anyone who uploads sexually explicit content without affirmative consent. This broadens the scope of accountability and protection.

In addition, the Act criminalizes both the publication of unauthorized sexually explicit content and the threat to publish such content on social media or any other online platforms, also known as sextortion. Sextortion has led to an astonishing increase in suicides, especially of young men; the FBI has seen a dramatic increase in financial sextortion cases targeting minor victims in the US.

The Take It Down Act also creates a "notice and takedown regime" similar to the Digital Millennium Copyright Act (DMCA). Under the Act, when a take-down request is sent to an online platform, the content must be removed within 48 hours. NCOSE has been part of legal cases because large platforms, such as Twitter (now X), have disregarded takedown requests made by parents on behalf of their children—meaning, Twitter ignored requests to takedown CSAM. Under Take It Down, websites must also make *reasonable efforts* to remove copies of the images, enforceable by the Federal Trade Commission.

NCOSE strongly supports three additional pieces of legislation that complement the Take It Down Act: the NO FAKES Act, Kids Online Safety Act (KOSA), reintroduced in the Senate last week, and the DEFIANCE Act, introduced in the Senate and House yesterday. Together, these

---

[61] Huasheng Gao and Vanya Petrova, "Do Prostitution Laws Turn a John into a Rapist? Evidence from Europe," *Journal of Law and Economics* (2022), http://dx.doi.org/10.2139/ssrn.3984596.
[62] Andrea Dworkin, "Pornography is a Civil Rights Issue," adapted slightly from testimony before the Attorney General's Commission on Pornography on January 22, 1986, available at http://www.nostatusquo.com/ACLU/dworkin/WarZoneChaptIVF1.html.

bills help protect individuals from the harmful effects of image based sexual abuse and increase pressure on tech companies to create and manage digital sites more responsibly.

The NO FAKES Act, which Senators Blackburn and Coons reintroduced last month, creates federal intellectual property protections for an individual's name, image, voice, and likeness. The law would apply to deepfakes involving everyone, both famous and non-famous individuals, including children. Currently, if a deepfake is created of a child or an adult that does not fall under the provisions of the Take It Down Act, the child or adult has no way to require a website or social media platform to remove it. This is concerning because the deepfake can still cause emotional harm to the victim, even though it is not sexual in nature.

Technological progress should not come at the expense of human dignity. It is our collective responsibility to protect the voice, face, and likeness of every individual from unauthorized exploitation.

Legislation should also compel more corporate accountability for the harms caused by social media platforms, an objective tackled by the Kids Online Safety Act, which creates a "duty of care" for platforms to prevent and mitigate harms to minors using these platforms. Thank you, Chairwoman Blackburn, for your relentless leadership on KOSA.

The DEFIANCE Act establishes civil liability for AI-generated sexually explicit deepfakes, allowing victims to seek justice in civil court. This legislation addresses not only the publication of such content but also its creation, distribution, and possession with the intent to distribute (which includes sextortion).

Finally, NCOSE is strongly concerned about the recent AI state moratorium language included in the House budget reconciliation bill. The House language is premature and creates a disincentive for AI companies to create products and services that put safety ahead of profits. It also creates a disincentive for AI companies to work with elected officials to pass meaningful legal guardrails to protect individuals from harm.

We must ensure that no one else falls victim to these devastating abuses.

○

A P P E N D I X

The following submissions are available at:

https://www.govinfo.gov/content/pkg/CHRG-119shrg61677/pdf/CHRG-119shrg61677-add1.pdf

Submitted by Chair Klobuchar: