

A MIDLIFE CRISIS? IP AND THE INTERNET AFTER 40

HEARING

BEFORE THE

SUBCOMMITTEE ON COURTS, INTELLECTUAL
PROPERTY, ARTIFICIAL INTELLIGENCE, AND
THE INTERNET

OF THE

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

SECOND SESSION

TUESDAY, JUNE 30, 2026

Serial No. 119–75

Printed for the use of the Committee on the Judiciary



Available via: <http://judiciary.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2026

COMMITTEE ON THE JUDICIARY

JIM JORDAN, Ohio, *Chair*

DARRELL ISSA, California	JAMIE RASKIN, Maryland, <i>Ranking Member</i>
ANDY BIGGS, Arizona	JERROLD NADLER, New York
TOM McCLINTOCK, California	ZOE LOFGREN, California
THOMAS P. TIFFANY, Wisconsin	STEVE COHEN, Tennessee
THOMAS MASSIE, Kentucky	HENRY C. “HANK” JOHNSON, JR., Georgia
CHIP ROY, Texas	TED LIEU, California
SCOTT FITZGERALD, Wisconsin	PRAMILA JAYAPAL, Washington
BEN CLINE, Virginia	J. LUIS CORREA, California
LANCE GOODEN, Texas	MARY GAY SCANLON, Pennsylvania
JEFFERSON VAN DREW, New Jersey	JOE NEGUSE, Colorado
TROY E. NEHLS, Texas	LUCY McBATH, Georgia
BARRY MOORE, Alabama	DEBORAH K. ROSS, North Carolina
HARRIET M. HAGEMAN, Wyoming	BECCA BALINT, Vermont
LAUREL M. LEE, Florida	JESÚS G. “CHUY” GARCÍA, Illinois
WESLEY HUNT, Texas	SYDNEY KAMLAGER-DOVE, California
RUSSELL FRY, South Carolina	JARED MOSKOWITZ, Florida
KEVIN KILEY, California	DANIEL S. GOLDMAN, New York
GLENN GROTHMAN, Wisconsin	JASMINE CROCKETT, Texas
BRAD KNOTT, North Carolina	SUMMER LEE, Pennsylvania
MARK HARRIS, North Carolina	
ROBERT F. ONDER, Jr., Missouri	
DEREK SCHMIDT, Kansas	
BRANDON GILL, Texas	
MICHAEL BAUMGARTNER, Washington	

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, ARTIFICIAL INTELLIGENCE, AND THE INTERNET

DARRELL ISSA, California, *Chair*

THOMAS MASSIE, Kentucky	HENRY C. “HANK” JOHNSON, JR., Georgia,
SCOTT FITZGERALD, Wisconsin	<i>Ranking Member</i>
BEN CLINE, Virginia	ZOE LOFGREN, California
LANCE GOODEN, Texas	TED LIEU, California
LAUREL LEE, Florida	JOE NEGUSE, Colorado
RUSSELL FRY, South Carolina	DEBORAH ROSS, North Carolina
KEVIN KILEY, California	SYDNEY KAMLAGER-DOVE, California
MICHAEL BAUMGARTNER, Washington	Vacancy

CHRISTOPHER HIXON, *Majority Staff Director*
ARTHUR EWENCZYK, *Minority Staff Director*

C O N T E N T S

TUESDAY, JUNE 30, 2026

OPENING STATEMENTS

	Page
The Honorable Darrell Issa, Chair of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California	1
The Honorable Henry C. “Hank” Johnson, Jr., Ranking Member of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of Georgia	4
The Honorable Jim Jordan, Chair of the Committee on the Judiciary from the State of Ohio	5
The Honorable Jamie Raskin, Ranking Member of the Committee on the Judiciary from the State of Maryland	5

WITNESSES

Sean Astin, President, Screen Actors Guild—American Federation of Television and Radio Artists (SAG–AFTRA)	
Oral Testimony	9
Prepared Testimony	11
Chris Floyd, Counsel, Amblin Entertainment	
Oral Testimony	14
Prepared Testimony	16
Steve K. Francis, Executive Chair, IP House	
Oral Testimony	20
Prepared Testimony	22
Christopher A. Mohr, President, Software and Information Industry Association (SIIA)	
Oral Testimony	31
Prepared Testimony	33
Bhamati Viswanathan, Visiting Assistant Professor, Suffolk University Law School	
Oral Testimony	51
Prepared Testimony	53

LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING

All materials submitted for the record by the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet are listed below	79
Materials submitted by the Honorable Darrell Issa, Chair of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California, for the record	
A letter to the Honorable Chuck Grassley and the Honorable Dick Durbin, from the Entertainment Software Association, Jun. 9, 2026	
An Appeal Case, <i>Vetter Communications Corporation v. Resnik Music Group</i> , United States District Court, Middle District of Louisiana, United States Court of Appeals Fifth Circuit, Jan. 12, 2026	
A statement from the Motion Picture Association, Inc., Jun. 30, 2026, submitted by the Honorable Sydney Kamlager-Dove, a Member of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California, for the record	

A letter to the Honorable Darrell Issa, Chair of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California, and submitted by the Honorable Henry C. “Hank” Johnson, Jr., Ranking Member of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of Georgia, from Frank Cullen, Executive Director of Council for Innovation Promotion (C4IP), Jun. 29, 2026, submitted by the Honorable Henry C. “Hank” Johnson, Jr., Ranking Member of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of Georgia, for the record

APPENDIX

Materials submitted by the Honorable Darrell Issa, Chair of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California, for the record

A letter to the Honorable Darrell Issa, Chair of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California, and submitted by the Honorable Henry C. “Hank” Johnson, Jr., Ranking Member of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of Georgia, from Council for Innovation Promotion (C4IP), June 29, 2026

An article entitled, “In Graphic Detail: New data shows publishers face growing AI bot, third-party scraper activity,” Apr. 13, 2026, *Digiday*

A letter to the Honorable Darrell Issa, Chair of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California, and submitted by the Honorable Henry C. “Hank” Johnson, Jr., Ranking Member of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of Georgia, from Stanley Pierre-Louis, President & CEO, Entertainment Software Association, Jun. 29, 2026

A letter to the Honorable Darrell Issa, Chair of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California, and the Honorable Jerrold Nadler, a Member of the Committee on the Judiciary from the State of New York, from several manufacturers, businesses, and other organizations

A report entitled, “Unboxing Fake Fashion Unleashing Real Dangers,” Feb. 2026, *American Apparel & Footwear Association*

QUESTIONS AND RESPONSES FOR THE RECORD

Questions submitted by the Honorable Darrell Issa, Chair of the Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet from the State of California, for the record

Questions for Sean Astin, President, Screen Actors Guild—American Federation of Television and Radio Artists (SAG–AFTRA)

Response to question from Sean Astin, President, Screen Actors Guild—American Federation of Television and Radio Artists (SAG–AFTRA)

Questions for Chris Floyd, Counsel, Amblin Entertainment

Response to question from Chris Floyd, Counsel, Amblin Entertainment

Questions for Steve K. Francis, Executive Chair, IP House

Response to question from Steve K. Francis, Executive Chair, IP House

Questions for Christopher A. Mohr, President, Software and Information Industry Association (SIIA)

Response to question from Christopher A. Mohr, President, Software and Information Industry Association (SIIA)

Questions for Bhamati Viswanathan, Visiting Assistant Professor, Suffolk University Law School

Response to question from Bhamati Viswanathan, Visiting Assistant Professor, Suffolk University Law School

A MIDLIFE CRISIS? IP AND THE INTERNET AFTER 40

Tuesday, June 30, 2026

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND
ARTIFICIAL INTELLIGENCE, AND THE INTERNET

COMMITTEE ON THE JUDICIARY

Washington, DC

The Committee met, pursuant to notice, at 10 a.m., in Room 2141, Rayburn House Office Building, the Hon. Darrell Issa [Chair of the Subcommittee] presiding.

Members present: Representatives Issa, Fitzgerald, Cline, Gooden, Kiley, Lee, Fry, Johnson, Lofgren, Ross, and Kamlager-Dove.

Mr. ISSA. The Committee will come to order. Today, the Subcommittee, without objection, will be authorized to declare a recess at any time. We welcome everyone here today for the Intellectual Property and Internet Subcommittee hearing which will cover a broad range of current, but important, issues.

Candidly, we in Congress often wait until there is a crisis to move. We are known for the expression what we do is nothing at all or overreact. We cannot afford to do it either at this time. The growth of various types of theft of intellectual property through counterfeiting and piracy, in fact, has become an epidemic. Most of the rest of the world has at least made efforts to deal with these problems. This hearing will establish once and for all that the various pieces of legislation need to move and need to move quickly. That means that this Committee must come together, along with the Senate, to deal with economic crimes around the world, but particularly those who come to our shores and take advantage of a weaker enforcement. Additionally, the growth of AI means that in the near future, what we see as a growing epidemic will rise even further.

I want to particularly to focus on something here today. It is not just the money that is stolen from people whose creative works are being taken. It is, in fact, the funding of criminal networks, whether it is Hamas and Hezbollah, ISIS, Al Qaeda, or others, almost all these groups in addition to the conventional drug cartels, are operating criminal syndicates that include various forms of intellectual property theft. That means that, in fact, not doing something in a

timely fashion is causing people to die. It is causing countries to live in terror. It is costing countless amount of dollars that U.S. citizens pay in addition to the loss of revenue to those who create intellectual property.

I want to make it clear. We all know that there are people who innocently think that watching on a bootleg channel something they would otherwise pay for, the cost is simply they are getting a deal of free. If that money is, in fact, going to syndicates that are involved in other illegal activities, you are funding criminals. You are funding people who hurt people.

Four decades ago, the Advanced Research Project Agency, ARPANET, adopted a communications protocol. I was a young lieutenant in those days and we used it. We used it in a very limited fashion. One day, somebody came up with the idea of a way to communicate that became known as email. In those decades, half a century or so, we have gone from a connection of military bases and universities for purposes of furthering research to the internet as we know today. In addition, the advantage of Moore's Law, in fact, has made almost anything that you have seen in science fiction all the way back to Jules Verne and all the way through to the *Terminator*, a reality today or in the near future.

Decades ago, we passed the Internet Freedom Act and the DMCA laws to protect fostering and nascent technology. They were good. They worked some. They have, in fact, been modified over time, and the notice and takedown orders have, in fact, made them more effective. The cooperation of all parties, including the internet providers for whom this is simply overhead, in fact, has been appreciated. It has come without a cost.

Recently, the Supreme Court made decisions that provide certainty as to, in fact, whether there is liability for various actions or inactions. We are not here to talk about that today. We are, in fact, recognizing that we have to all work together if we are going to stop copyright piracy over the internet.

Only a few days ago, I was honored to be at the White House to watch a UFC fight. It was amazing. The problem is all over the world people are watching those fights for free. The cost of that fight included \$3 million of set up and take down there at the White House. Somebody has to recognize that this is not without a cost. In addition, those who took the blows deserved to be compensated. To do so requires that, in fact, the purveyors be able to put that out in a streaming format and have it, in fact, only go to those who pay the small amount to get it.

Digital video piracy includes illegal downloads, streaming of films and television and has resulted in an estimate that of loss of over 230,000 jobs and conservatively \$47.5 billion reduced to our GDP. That is the economic cost. I have already covered, in fact, the cost that I am not overreacting to say people have died as a result of the money that is gained from that piracy.

While millions of listings for copyright-infringing content are removed every day under notice and takedown process set forth in the Digital Millennium Copyright Act, right holders have raised concerns with the speed. Today, our witnesses come prepared to answer the major question, what is the reasonable speed? Can we do it at the speed of sound? Can we do it at the speed of light?

More importantly, in a 45 minute or sometimes a fraction of that live sports broadcast, can we do it soon enough to make it no longer profitable for those who pop up and sell their clandestine wares.

The internet is open to substantial news sales revenues for brands. That is enabling the trafficking of fake brands, and I want to make it very clear. I live on the Mexican border. My district covers 80 miles of the Mexican border. In my district, we have a holding facility that holds up to 40,000 square feet, racked three and four high of illicit drugs. Those drugs often look like the real drug. They are in similar packaging. The pill or other container always seems to look very legitimate. It even has the right letters on it. When it is fentanyl, it has led to people dying.

Counterfeiting is not simply a matter of getting a purse that looks cool that you can take to a party and maybe no one will know or even you may even brag that it is a fake, it also includes the counterfeiting of pharmaceuticals that, in fact, once again lead to people dying.

The patchwork of laws in many of these cases, State by State, asks the question, should we continue to have States make decisions that make honest, law-abiding purveyors of products life difficult, while in fact, not effectively stopping the clandestine work? We made this decision in 1972 through both legislation and court that we were not going to do it with copyright for music. It has been a long time since and there has needed to be some additional items done. We have profited as a Nation from having not just one standard, but having the Federal Government being able to aid States in the enforcement of copyright protection. The same needs to happen relative to AI. We all know it has to happen and more importantly, if we are going to protect the law-abiding citizen, we can't have it be simply an additional law on top of hodge-podge laws that, in fact, can create conflicts or greater regulatory requirements.

There needs to be a congressional act targeted in a measured way, meaning don't overreact. Any Federal legislation must balance three goals to avoid hobbling American innovation in online services and AI technology which will, in fact, ensure the continued leadership around the globe of U.S. technology. Let us make sure, in closing, that there is one thing beyond all that I have mentioned that is at stake and that is global leadership. America leads the world in high tech. We do so because we welcome people from around the world to join us through immigration. Our universities are the envy of the world for both those who come and stay and those who come and go back. That leadership is challenged by many others, but particularly by a China that, in fact, does not respect intellectual property, but does appreciate the innovation. They appreciate it so much they steal it.

It is Congress' responsibility thus to, in fact, make clear that we are in a war, we are in a battle, we are in a competition against China, and we are determined to win.

Before I recognize the Ranking Member for his opening statement, I would like to set a tone quickly with a short video. If we could please run the video with audio.

[Video shown.]

Mr. ISSA. I now recognize the Ranking Member of the Subcommittee for his opening statement.

Mr. JOHNSON. Thank you, Mr. Chair. When the modern internet was born in January 1983, many considered it just another Department of Defense project for the military. Thanks to taxpayer funding, the United States was able to partner with research universities and eventually private companies to harness this innovation for use by the general public. Over its first 10 years, the internet evolved from an application to compete with the Soviets to a place where people could socially connect, conduct business, and communicate with others, and even through—it evolved into a medium for artistic expression.

Today, it is hard for many of us to imagine a world without new recipes at our fingertips, instant news updates, or pictures of our friends and family on or social media news feeds. Good or bad, it is no longer the question. The internet is inescapable from modern society. This is quickly becoming the same with generative artificial intelligence which has been adopted by businesses and consumers alike in just a few short years.

Even with widespread adoption of transformative technology, it is imperative that we continue to protect rights holders when technology is used to steal intellectual property, defraud consumers, and increase inequality. Products available online from a trusted website can seem identical to those at brick-and-mortar stores, but instead, are produced with harmful chemicals or contain dangerous malware. These nearly identical knockoffs can damage your favorite brand's reputation and harm their ability to stay in business.

Websites that miraculously have Project Hail Mary streaming for free really are too good to be true. That product with Tom Hanks in the commercial may not have actually been endorsed by Tom Hanks, just a replica created with AI. Some of these may seem harmless at first glance, but they matter to me and my constituents.

Film and TV spending in Georgia, the Hollywood of the South, hit \$4.4 billion in 2022 with 412 productions, but increased costs have devastated our film and TV market. Spending was down \$2.3 billion in the last Fiscal Year with just 245 productions. Our writers and actors need jobs to keep creating and market changes have made that all the more difficult to achieve. Across creative industries, innovators from writers and software developers to musicians and painters are watching their works used to train AI models for free, while the barrier to entry gets higher and higher.

If Congress' role today is to play armchair psychologist to the internet's mid-life crisis, it is imperative we view harms to creators as the symptom of a more pernicious disease. The question we should be asking ourselves is: Are the innovations before us serving the American people or do they exclusively benefit a small handful of the wealthiest, most powerful corporations and individuals in the world? Georgia's 11 million plus residents have a median household income of just under \$82,000. Mark Zuckerberg is worth \$220 billion as of December 2025. Groceries in Georgia were found to be the 11th highest in the country earlier this month. Elon Musk just became the world's first trillionaire. Homes in 79 percent of Georgia's counties are considered unaffordable for the average worker.

Jeff Bezos just spent an estimated nearly \$50 million on his wedding. Americans are clearly facing an affordability crisis, but those at the very top are doing well and getting wealthier and wealthier every day.

The price of everyday consumer devices such as your laptops and computers have continued to climb, now to an estimated 15–25 percent. Data centers are driving up utility costs, straining the grid and degrading the quality of the everyday appliances families depend on, like our air conditioning and heating system. Senior citizens are having to choose between paying their utility bills and their prescriptions and the rich get richer. The middle class shrinks and the poor get poorer.

The benefits from technological innovations, while impressive, are minimized if everyone can't enjoy their benefits. We can do this by meaningfully deploying technology in a way that uplifts us all. This means acknowledging creators as a key part of the ecosystem that is building AI and compensating them as such. This means enacting protections for American workers, building responsibility, and deploying equitably.

I look forward to hearing from the witnesses how we can better protect America's artists, innovators, and the creative fields. I thank Chair Issa for holding this important hearing and I yield back the balance of my time.

Mr. ISSA. The gentleman yields back. Thank you. We now recognize the Chair of the Full Committee, Mr. Jordan, for his opening statement.

Mr. JORDAN. Thank you, Mr. Chair. I will be brief. I just want to thank you for your work for now over two decades on trying to stop copyright piracy and harmful uses of AI while not harming choice, innovation, and maybe most importantly First Amendment liberties. We appreciate your tireless work, and I know this is your last session in Congress. We will probably have a few more hearings, but I did want to take the time to thank you for this issue and so many others that you have worked so hard on and I thank our witnesses for being here and look forward to hearing from today's panel. With that, I yield back.

Mr. ISSA. I thank the Chair. I profusely thank the Chair. We now recognize the Ranking Member of the Full Committee, Mr. Raskin, for his opening statement.

Mr. RASKIN. Thank you kindly, Mr. Chair. Welcome to our witnesses.

A couple of months ago, I got a postcard in my mailbox which let me know that three books I have written over the course of my career had been used to train Anthropic's Claude AI large language models, and because of this I was entitled to be part of the settlement in the *Bartz v. Anthropic* case. Now, this surprised me because first it reminded me that I used to write books. Now, I just post 280 characters every day. It also surprised me because I didn't know anything about the litigation, much less did I know anything about the fact that *Anthropic* had essentially swallowed up the contents of three of my books, apparently rejecting the relevance and utility of several books I had written.

Anthropic had never called to ask me to use my books, but a judge found that *Anthropic's* ingestion and digestion of my books

without payment was fair use. Claude AI may not be allowed to simply reprint my book and regurgitate line for line and sell it, but it may profit off my word choice, my cadence, my style such as it is, my conceptualizations, and my research, among other attributes of my writing for free.

Now, if I finally get around to filling out the form which means I have to finally get around to finding the postcard, I may get a *de minimis* check in the mail because the judge did find *Anthropic* had used pirated versions of the books that it used to train its large language model and the parties, including apparently me, settled shortly after this holding. Now, it would be cavalier to write these training episodes off as a random or minor incidence. AI companies intentionally select works with which to train their large language models, often with zero intention of paying the creators any royalties for use of their creative intellectual labor.

Bartz v. Anthropic is just one ominous decision floating in a sea of developing case law in this brave new world to engage in a fair use vernacular borrowing of H.G. Wells famous work of science fiction, but it is illustrative of the proliferating tensions between existing law and social values that have materialized as we live through this time of astonishing technological transformation. The advent of the internet and the explosive emergence of AI have fundamentally changed the way that we interact with each other, the way we conduct business, the way we think about human thought and human feelings and human work, and the way we create and consume books, songs, and other creative works.

Now, I tend much more to the heady enthusiast side of such changes over the brute and Luddite side when it comes to technological innovation, but that is only because I have a profound faith in democracy and our capacity to manage technological change when we put our minds to it. Now, is the time to pose and grapple with urgent and searching questions about the moment.

How do we integrate titanic new technological changes in a way that supports, rather than undermines, the basic needs and values of our society? We know from experience that innovations mean little if they are left to create inequality and domination, joblessness, and poverty.

How do we prevent the concentration of power and wealth, but instead work to fairly distribute the benefits of new technologies so they become part of our common life and inheritance? In this new era, we must ask ourselves what is fair, what is just, and what will secure the greatest good to the greatest number of people. That is what I hope we will be doing today.

When the DMCA became governing copyright law nearly 30 years ago, dangerous products and merchandise that infringed on intellectual property rights overwhelmingly had to be bought in person. Movie and music pirates created physical copies of recordings and literally sold them on the street corners. Our laws did not contemplate the spread of streaming where content piracy occurs on a daily basis all over the world as far away as Vietnam, the Philippines, and the pirates can create a new infringing site the moment one gets taken down. Consumer products used to be bought almost exclusively in stores with the occasionally counterfeit handbag on the street.

Today, harmful counterfeit products like exploding batteries, toxic baby cream, and asbestos-laden crayons can be bought often, usually unwittingly, by consumers online and they arrive at their doorsteps in a matter of hours. Even our music laws were designed for a world where listeners discovered music through their stereos, which is why we are left with laws that prevent performers from being paid when their music is being played on the radio. These issues affect not just the two million employees of the movie industry or the nearly \$12 billion in revenue from the music industry, but also the consumers who end up paying the cost of counterfeit goods that break or cause harm or just drive up the price of the real product.

The laws on the books may no longer be fair for these affected industries, and they are almost certainly unfair to consumers. I understand there are many proposals out there with ideas for improving the current situation. I am a proud cosponsor of one of them, the American Music Fairness Act, which would ensure that performers are paid when their music is actually played on the radio. In many ways, AI's supercharged problems have been percolating since the advent of internet. Generative AI models allow to use internet faster, more accurately, and beyond our individual technological capacities, but our laws have not kept pace with all the changes. Our intellectual property laws were created at a time when it was safe to presume that one must be human to have cognition and intellect. Some would argue that is no longer the case. It is long past time we considered how to protect the creative fields and address the ramifications of the proliferation of deep fakes, training AI models on copyrighted material, and other areas where AI may be unfair to both consumers and creators.

I know some of my colleagues want to do away with the regulation of AI companies altogether, but we can protect content creators and help businesses thrive at the same time. We don't have to choose. Congress should help provide for the safe adoption of generative AI models that take into account the environmental labor and social consequences of such technology and we should do so while allowing the States to experiment with different approaches.

I am dismayed by those who have caved to a small group of billionaires and now a trillionaire, who own these AI models and have proposed broad preemption of State common law causes of action and State legislative decisionmaking with no Federal regulation at all. There is no reason we should do away with common law tort claims that act as the basic national safety net for fairness.

The National Institute of Science and Technology should absolutely be allowed to test frontier models and if AI models are being built on the hard work of artists, writers, and inventors, we should be thinking long term to ensure that there are more artists, writers, and inventors a generation from now creating material to sustainably train the next wave of generative innovation to come.

The rational next step for this Committee is to ask ourselves how we can map a path forward for all Americans to use technology while ensuring laws that protect consumers and creators, workers, and families.

Thank you, Mr. Chair, I yield back to you.

Mr. ISSA. The gentleman yields back. Without objection, all other opening statements will be included in the record. We now go to our distinguished panel of witnesses.

Mr. Sean Astin. Mr. Astin is the President of the Screen Actors Guild. By the way, one of the few things I haven't done and I continue to say, I am available for a bit part. Am I allowed to do that?

Anyhow, the American Federation of Television and Radio Artists, commonly known as SAG-AFTRA, he is himself an actor and a long-distinguished career in film and television. To name just a few, he has appeared in the "Goonies," "Rudy"—by the way, we are going to talk about "Rudy." That is going to happen. How can we not? Even if you didn't go to the right college, the "Lord of the Rings" trilogy, "Stranger Things," "Teenage Mutant Ninja Turtles," and many more. Thank you for being here as a well knowledgeable expert witness, in addition to your current role.

Mr. Chris Floyd. Mr. Floyd is a legal and business strategy advisor to Amblin Entertainment, a film and television production company, basically, he is Steven Spielberg's most trusted advisor. He previously served as the Chief Operating Officer and General Counsel at his partnership for a decade and held various positions with Dreamworks Studios, Universal Pictures, Paramount, and Walt Disney Productions. Welcome.

Mr. Steve Francis. Mr. Francis is the Executive Chair and President of IP House, a global intellectual property enforcement company. He previously served as the acting Executive Associate Director of Homeland Security Investigations as the Director of National Intellectual Property Rights Coordinator. Thank you very much and welcome.

Mr. Christopher Mohr. Mr. Mohr is President and Chief Executive Officer of the Software and Information Industry Association, a collection of entertainment, consumer, and business software companies. He previously served as a Senior Vice President for Intellectual Property and General Counsel at the same organization where he led the association's intellectual property policy and antipiracy.

Last, but not least by a long shot, Dr. Bhamati Viswanathan, or close to it. The doctor is a nonresident fellow at the Kemochan Center for Law, Media, and the Arts at Columbia University. She is also a Visiting Assistant Professor at Suffolk University Law School where she teaches courses in contract and transactional law. The doctor is, in fact, the author of a number of books including, "How Creative Industries Can Harness Intellectual Property to Survive in a Digital Age." Welcome, and I apologize. As one left hander to another, I said I am not going to mess this up and between my hoarse throat and the other, I apologize.

I want to thank all of you for being here. Pursuant to the Committee rules, I would ask you to please rise, raise your right hand, to take the oath.

Do you solemnly swear or affirm under penalty of perjury that the testimony that you are about to give is true and correct to the best of your knowledge, information, and belief so help you God?

Thank you. You may be seated. Let the record reflect that all witnesses answered in the affirmative.

If you watch C-SPAN, you know I have to give this admonishment, that you will have five minutes in your opening statements, but 100 percent of all the material you brought with you and your opening statement plus additional material you may supplement with will be placed in the record, thus leaving you completely free not to just read what you brought, although some of you just might. With that, we begin, Mr. Astin.

STATEMENT OF SEAN K. ASTIN

Mr. ASTIN. Well, this is good stuff. You're going to want to hear it. Chair Issa, Ranking Member Johnson, the Members of the Committee, thank you very much for convening the hearing and for your continued work modernizing American intellectual property law.

Thank you, Representative Lofgren, for your leadership on combating foreign digital piracy, and Chair Issa, for all your work and for your work on the American Music Fairness Act. The issues therein matter to the livelihoods of the 160,000 union performers and media professionals I represent as President of SAG-AFTRA.

Today, I would like to speak about the abuse of nonconsensual digital replicas of our voices and likenesses. For all of human history, if someone saw your face and knew it was you, if they heard your voice and knew you had spoken, for thousands of years that simple connection was enough, your face, your voice, and your presence, reality itself was affirmed and simply put we knew who we were to each other.

Artificial intelligence has begun to intervene and break that ancient connection. Today, someone can realistically make you appear to say something you never said, to endorse something you don't believe in, or even convincingly depict you confessing to something you had no knowledge of. For the first time in human history, the experiences we have always shared are no longer secure. Our relationship with the community is distorting thanks to a wave of technology made widely available without much concern for public safety.

In my line of work, we deal with emotions, so on behalf of our performers I am here to tell you what this moment feels like. To begin, we make our livings by granting the use of our voices and likenesses to our employers. That is what they pay us for. Through every audition and with every career setback, we know, we rely on the fact that when the jobs finally come, we have something uniquely ours to offer. Now, imagine a performer waking up one morning to discover on their phone a version of themselves that never was, but they are watching it and so is the rest of the world. The voice and the face are a perfect match. For the performer, it is a moment of terror. Who is seeing it? Will anyone ever hire them again? Will their reputation that was built over a lifetime be destroyed in a moment? Every casting director, every producer, every executive, and every member of the public can see it. Even their family may hesitate for a moment. They can reach for something deeper. He would never say that. That is not who she is, but who are we?

Think about anyone you love. Your understanding of them is built from memory. Imagine that memory being contaminated. The

thing that brings us back to the real person is our faith in who they truly are. In the world of deep fakes, the damage is done instantly and without mercy. The public has no obligation to discover the truth about someone. They just keep scrolling. Our members have no ability to protect themselves from this kind of abuse, and neither does the teenager humiliated by a fabricated image, neither do parents trying to protect their children, neither does anyone whose reputation can be threatened by a digital replica they never authorized.

Artificial intelligence is changing the way human beings experience life. We all know that this moment demands wisdom and action. Technology is not our enemy. Throughout our history, America has chosen both innovation and responsibility, usually sadly, only after ordinary people have suffered some calamity, but there is a right path. It is obvious that civilization is in the throes of a technological whirlwind the likes of which we have never seen and as of this moment, Americans are being forced to surrender their basic relationship to one another.

We don't want to stop progress. We need to civilize it. Many Americans may never own a home or accumulate significant financial wealth, but every American does possess something of immeasurable value, their identity. That God-given gift really should belong to us and surely, we can all agree that no one else should be permitted to commercially exploit our identity without consent.

In the world of entertainment, our image and likeness have been the substance of our transactions, but in the wild, we do not own them. We should, and you can make it so.

Members of the Committee, what I am saying about this moment and about who we are is that every human being should remain the author of their own existence. Reality should remain verifiable. Consent is not a nuisance. Reputation matters, and truth is truth, and it is worth protecting. Thank you very much.

[The prepared statement of Mr. Astin follows:]

Testimony of Sean Astin
House Judiciary Committee
Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet
"A Midlife Crisis? IP and the Internet After 40"

Chairman Issa, Ranking Member Johnson, Members of the Committee:

Thank you for convening this hearing and for your continued work modernizing American intellectual property law. Thank you, Representative Lofgren, for your leadership on combating foreign digital piracy, and Chairman Issa, for all of your work on the American Music Fairness Act. These issues matter to the livelihoods of the 160,000 union performers and media professionals I represent as President of SAG-AFTRA.

My focus today is on nonconsensual digital replicas.

For all of human history, if someone saw your face, they knew it was you.

If they heard your voice, they knew you had spoken.

For thousands of years, that simple connection was enough. Your face. Your voice. Your presence. Reality itself was affirmed and, simply put, we knew who we were to each other.

Artificial intelligence has begun to intervene and break that ancient connection.

Today, someone can realistically make you appear to say something you never said. To endorse something you don't believe in, or even convincingly depict you confessing to something you had no knowledge of.

For the first time in human history, the experiences we've always shared are no longer secure. Our relationship to community is becoming distorted thanks to a wave of technology that was recklessly brought to the public without care as to how it might be used to hurt people.

In my line of work, we deal with emotions. On behalf of our performers, I'm here to tell you what this moment feels like.

To begin, we make our livings by granting the use of our voices and likenesses to our employers. That's what they pay us for. Through every audition and with every setback,

we know, we rely on the fact that when the jobs finally come, we have something uniquely ours to offer.

Now, imagine a performer waking up one morning to discover, on their phone, a version of themselves that never was.

But they are watching it.

1

And so is the rest of the world.

The voice and face are a perfect match.

For the performer, it's a moment of terror.

Who is seeing it?

Will anyone ever hire them again?

Will their reputation—built over a lifetime—be destroyed in a moment?

Every casting director.

Every producer.

Every executive.

Every member of the public can see it.

Even their family may hesitate for a moment.

But they can reach for something deeper.

"He would never say that."

"That's not who he is."

But who are we?

Think about anyone you love.

Your understanding of them is built from memory.

Imagine that memory being contaminated.

The thing that brings us back to the real person is our faith in who they truly are.

In the world of deepfakes, the damage is done quickly and without mercy.

The public has no obligation to discover the truth about someone.

They just keep scrolling.

Our members have almost no ability to protect themselves from this kind of abuse.

2

Neither does the teenager humiliated by a fabricated image.
Neither do parents trying to protect their children.
Neither does anyone whose reputation can be threatened by a digital replica they never authorized.
Artificial intelligence is changing the way human beings experience life. And it's doing so very quickly. We all know that this moment demands wisdom and action.
To be clear, technology is not our enemy.
Throughout our history, America has chosen both innovation and responsibility.
Usually, sadly, only after ordinary people have suffered some calamity. But there is a right path.
In our time, it is obvious that civilization is in the throes of a technological maelstrom, and as of this moment, Americans are being forced to surrender their basic relationship to one another.
We don't want to stop progress.
We need to civilize it.
Many Americans may never own property or accumulate significant financial assets.
But surely the God-given gift of who they are should belong to them. And that means ownership.
In the world of entertainment, our image and likenesses have been the substance of our transactions. But in the wild, we do not own them.
Every American deserves the right to own, as property, their voice and likeness.
Members of the Committee, what I'm saying about this moment, and who we are, is that:
Every human being should remain the author of their own existence.
Reality should remain verifiable.
Consent is not a nuisance.
Reputation matters.
Truth is truth.
And it is worth protecting.
Thank you.

Mr. ISSA. I thank the gentleman. Mr. Floyd.

STATEMENT OF CHRIS FLOYD

Mr. FLOYD. Chair Issa, Ranking Member Johnson, and the distinguished Members of the Subcommittee, thank you for inviting me here today. I am of counsel at Amblin Entertainment, Steven Spielberg's film and television company. I have worked in the Amblin family for 20 years, including a decade as Chief Operating Officer and General Counsel. I have overseen many business and legal functions including content protection.

Two weeks ago, Amblin and Universal released Steven's film "Disclosure Day," adding to his legacy of films like "War of the Worlds" and "Minority Report." "Disclosure Day" fully embodies Steven's beloved sci-fi genre, embracing modern technology that makes transporting audiences to another world even more thrilling. However, these technological advancements also present challenges. Steven's prior sci-fi movies were released in a drastically different marketplace, before the internet super charged digital piracy.

When "Minority Report" was released in 2002, piracy was still limited largely to hard goods, DVD bootlegs from camcorders in a theater with muddled sound and shaky video, then sold on street corners. They were poor knockoffs and customers knew it. While the scale of piracy was reason for some concern then, today, digital piracy costs the U.S. economy a staggering amount at least \$29 billion annually. We now expect each release will be made available immediately in perfect digital form from offshore pirate sites with global reach. This substantial increase in quality, coupled with wide and immediate availability on any device, makes this an urgent economic and consumer safety problem.

Together with our studio distribution partners, we spend hours seeking removal of these infringing videos. Additionally, all the studios and streamers created the Alliance for Creativity and Entertainment to work with global law enforcement to combat piracy, but even with these extensive efforts, representing tens of millions of dollars and countless work hours, piracy still inflicts huge harm on the market for our films.

When we find "Disclosure Day" online, we have limited recourse, primarily because most pirate sites are operated by overseas criminal enterprises. We have laws that enable us to go after pirate sites in the U.S., but Bulgaria, Vietnam, the Philippines, these jurisdictions sit outside the practical reach of U.S. law enforcement, but easily reach U.S. consumers online.

The global revenues from U.S. films are shared with cast and crew in residuals and pension, health, and welfare payments. Profits are poured into new productions in every State of the union, including with local businesses. Shooting a one-hour television episode generates around \$475,000 per day locally, while a feature film generates \$670,000 per day. The billions siphoned from our economy by these overseas criminals should be available for these future productions and payments to industry workers, but they are not.

Today, piracy detrimentally impacts millions of creators in the U.S. entertainment industry and the economy as a whole while

funding a global network of crime. According to Digital Citizens Alliance, European authorities dismantled a piracy operation across 11 countries in 2024 that generated \$3.5 billion yearly seizing drugs, weapons, and millions in crypto currency. In Spain, Operation Fake exposed another site that also dealt in drug trafficking and money laundering, resulting in 30 arrests and millions in frozen assets.

What is to be done? Well, I ask you today for the tool proven effective in nearly 60 countries globally, but still lacking in the U.S, judicial site blocking. Under these laws, when a court determines there was full and transparent process that an off-shore site is dedicated to piracy, it can direct internet providers to block local access. Studies prove site blocking results in fewer visits to piracy sites and an increase to legitimate sites. Portugal witnessed a 70 percent drop in traffic. Australia saw a 25 percent decrease. The U.K. experienced a 10 percent surge to legal services. This would be a game changer for our industry's 2.3 million workers and America's creative economy.

Historically, the U.S. led the world in IP enforcement, but we have lagged behind for the past decade. Other countries have shown us how to do this without impacting speech, due process, or the internet. It is time the U.S. reasserts its leadership role in antipiracy.

Finally, allow me to turn briefly to artificial intelligence where the U.S. is the leader in innovation as it should be. As a tool, AI can further empower us to tell compelling stories and reach audiences, but as we consider how to maintain America's competitive advantage against China and other countries, we must also remain the global leader in both the innovation and creative industries. How these AI companies win the AI race and how they treat copyrighted work will affect the course of human creativity in the future. We will never maintain America's lead by lowering our IP standards to match those of the Chinese. That is why our industry supports the NO FAKES Act, which combats dissemination of unauthorized AI-generated deep fakes while safeguarding protected expression such as parody, news, and biopics.

I would like to thank the Subcommittee for your dedication, as we look forward to working together rebuilding a vibrant U.S. entertainment industry. Thank you.

[The prepared statement of Mr. Floyd follows:]



25 June 2026

The Honorable Darrell Issa
Chairman
Subcommittee on Courts, Intellectual Property,
Artificial Intelligence, and the Internet of the
Committee on the Judiciary
2108 Rayburn House Office Building
Washington, DC 20515

The Honorable Hank Johnson
Ranking Member
Subcommittee on Courts, Intellectual Property,
Artificial Intelligence, and the Internet of the
Committee on the Judiciary
2240 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Issa, Ranking Member Johnson, and Distinguished Members of this IP Subcommittee:

Thank you for inviting me to speak today.

I am Of Counsel at Amblin Entertainment, Steven Spielberg's film and television production company. I have worked in the Amblin family of companies for nearly two decades, including a decade as the Chief Operating Officer and General Counsel of Amblin Partners. At Amblin, I have overseen international distribution, business and legal affairs, and various other company operations, including content protection.

Two weeks ago, Amblin and Universal released Steven Spielberg's most recent film, *Disclosure Day*. Adding to his legacy of films like *Ready Player One* in 2018, *War of the Worlds* in 2005, and *Minority Report* in 2002, Steven has made a film that fully embodies his beloved sci-fi genre – this time, embracing the modern advances in filmmaking technology that make transporting audiences to another world even more thrilling.

However, these advancements also present challenges. Each of Steven's prior sci-fi movies was released in a drastically different marketplace than we live in today, largely due to changes in technology and the internet that have supercharged digital piracy.

When *Minority Report* was released in 2002, our piracy concerns were limited to hard goods: DVD bootlegs of the film from camcorders in a theater with muddled sound and inferior video and then clumsily sold on street corners. They were poor knockoffs of the film and consumers knew it. The scale of that operation caused financial concerns. However, today digital piracy alone costs the U.S. economy at least \$29.2 billion annually.¹

¹ [U.S. Chamber of Commerce, Impacts of Digital Video Piracy on the U.S. Economy.](#)

Today, we expect each film we release to be pirated and made available online *immediately* via offshore pirate sites that look legitimate and make the viewer think it is an authorized version. The substantial increase in quality, coupled with wide availability on any device, so soon after the initial release, makes today's piracy an urgent consumer safety and economic problem.

After a film's release, I field emails and calls from people who are seeing the film online. I have to enlist our IT team to discern what is pirated material without exposing our corporate systems to malware. And, of course, we have partners like Universal, Disney, or Warner Bros. to assist in our content protection efforts. In addition, all of the studios and streamers are part of the Alliance for Creativity and Entertainment (ACE), a global operation that works with law enforcement to combat digital piracy. Together, a tremendous amount of resources and work hours are devoted to protecting our film and television productions from online piracy.

But even with these extensive efforts – resources representing tens of millions of dollars and countless work hours – piracy still inflicts huge harm on the market for our films.

When we find copies of *Disclosure Day* online, we have limited recourse, primarily because most pirate sites are operated by overseas criminal enterprises. If the piracy originates in the U.S., we have laws that enable us to handle it. But Bulgaria? Vietnam? The Philippines? These jurisdictions sit outside the practical reach of U.S. law enforcement. And despite being located offshore, the piracy sites are directed to and can easily reach U.S. consumers over the internet.

These overseas criminal enterprises are making hundreds of millions of dollars that should be coming back to the American economy. Global profits from U.S. films are shared with cast and crew in the form of pension, health, and welfare benefits. Profits are poured back into production in every state of the Union, including production spending with local businesses. Shooting on location for a one-hour television episode generates an average of \$475,000 per day for the local community. Shooting a feature film generates an average of \$670,000 per day.²

Today, the harm from digital piracy impacts millions of creatives in the U.S. film and television industry and the economy as a whole, while also funding a global network of crime. A recent and chilling report from Digital Citizens Alliance and IP House³ connects these overseas piracy networks to even larger criminal enterprises. In November 2024, European authorities dismantled a piracy operation that generated \$3.5 billion every year. When police executed raids on that operation across 11 countries, they seized drugs, weapons, and millions in cryptocurrency.

In Spain, Operation Fake exposed a piracy enterprise that also dealt in property fraud, drug trafficking, and money laundering – resulting in 30 arrests and \$12.7 million in frozen assets. And in Italy, a former piracy operator turned informant recently warned: “Those who pay for [piracy] are funding the Camorra,” one of the nation's most powerful crime syndicates.

² Motion Picture Association, *The American Motion Picture and Television Industry Creating Jobs, Exporting Around the World*.

³ Digital Citizens Alliance, *Organized. Piracy. Crime.: How Global Piracy Networks Became Organized Crime Syndicates – And What Needs to be Done About It*.

We are a long way from the days of shaky camera footage burned onto a bootleg DVD. Today, digital piracy harms the millions of creatives in the U.S. film and television industry and the American economy as a whole, all while funding a global network of crime that sees billions of dollars in profits every year.

So, what is to be done? I ask you today for a tool that has proven effective for more than a decade in the fight against piracy in nearly 60 countries around the world, a tool that we currently do not have in the U.S. judicial site blocking.

Under the laws in these countries, once a court has determined through a full and transparent judicial process that an offshore site is dedicated to piracy, it can direct internet service providers to block local access.

Studies prove that site blocking is effective – resulting in a decrease in visits to piracy sites *and* a corresponding increase to legitimate sites, without harming free expression or the internet. When faced with a blocked pirate site, consumers often move to one of the many legitimate options that are widely available – options that actually compensate creatives for their work.⁴ The results speak volumes: Portugal witnessed a 70% drop in traffic to targeted pirate sites; Australia saw a 25% decrease in a single year; the U.K. experienced a 10% surge in views on legal services.⁵

This would be a game-changer for our industry's 2.32 million workers and America's creative economy as a whole.⁶ Historically, the U.S. led the world in IP enforcement standards. But in lacking effective remedies against overseas pirate sites, the U.S. has lagged behind for the past decade, doing irreparable harm to the creative community.

The upside is that we now have a decade of experience in other jurisdictions and know how to do this effectively and without negative impacts on speech, due process, and the health of the internet. It is time for the U.S. to reassert its leadership role.

I would be remiss if I didn't say a few words about Artificial Intelligence. The U.S. is the leader in AI innovation, as it should be. Studios like Amblin have embraced its promise to empower us to tell compelling stories and reach audiences in innovative ways.

As we consider how to maintain America's competitive advantage against other countries, including China, we must ensure that America remains the global leader in BOTH the innovation and creative industries. *How* these AI companies compete to win the AI race does impact our creative community. How they treat our copyrighted work will make all the difference to the future of human creativity. The need for America to "win" the AI race is real, and it must be done correctly. We will never maintain America's competitive advantage in these uniquely American industries by lowering our IP standards to match those of the Chinese.

⁴ [Carnegie Mellon University's Initiative for Digital Entertainment Analytics \(IDEA\), *The Effect of Piracy Website Blocking on Consumer Behavior*](#).

⁵ [Information Technology & Innovation Foundation \(ITIF\), *The Normalization of Website Blocking Around the World in the Fight Against Piracy Online*](#).

⁶ [Motion Picture Association, *The American Motion Picture and Television Industry Creating Jobs, Exporting Around the World*](#).

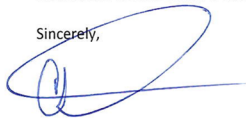
Chris Floyd Written Testimony for 6.30.26 Hearing
25 June 2026

4

That is why our industry supports policies to ensure *responsible* AI innovation, not AI innovation at all costs. A good example is the NO FAKES Act. That legislation would combat dissemination of unauthorized AI-generated deep fakes while safeguarding protected expression, such as satire, parody, news, documentaries, biopics, and historical fiction.

Protecting intellectual property and the creative industries has always been a bipartisan issue. My community is incredibly grateful to this Subcommittee for your dedication and focus to protect our livelihoods. Let us rebuild a vibrant and thriving U.S. entertainment industry together.

Sincerely,

A handwritten signature in blue ink, consisting of a stylized 'C' followed by a horizontal line that loops back under the 'C'.

Chris Floyd
Of Counsel, Amblin Entertainment

Mr. ISSA. I thank the gentleman. Mr. Francis.

STATEMENT OF STEVE K. FRANCIS

Mr. FRANCIS. Chair Issa, Ranking Member Johnson, and the distinguished Members of the Subcommittee, thank you for the opportunity to testify today.

I spent over 25 years in Federal law enforcement, including as the Director of the National IPR Center, working alongside colleagues from Homeland Security investigations, U.S. Customs and Border Protection, the Department of Justice, and law enforcement partners across more than 30 countries. I have seen IP enforcement from multiple angles. I know where the government excels and where prioritization creates challenges for enforcement.

I appear today on behalf of IP House, a global IP protection enforcement company I cofounded, after recognizing critical gaps in the enforcement landscape. IP House operates across every major jurisdiction because IP crime is truly global. We detect and disrupt infringement networks at scale, bringing global intelligence and operational visibility that complements the work of governments and rights holders worldwide.

IP House confirms what I witnessed throughout my career. As commerce has moved online, IP crime has grown more sophisticated, more organized, and harder to disrupt. Criminal networks now exploit the speed, scale, and anonymity of the internet to steal IP and endanger consumers on a global scale. Today's hearing is incredibly timely.

Counterfeiters operate through anonymous digital storefronts on the trust, online marketplace that American consumers use every day. They rapidly cycle through the seller's identities, domains, and payment processors to evade enforcement, often moving illicit proceeds long before traditional legal remedies can take effect. That is why IP House focuses on following the networks and the money, not just removing individual listings. It dismantles criminal organizations rather than chasing one product at a time. They are not harmless knockoffs. They include counterfeit pharmaceuticals, automotive parts, electronics, children's toys, and household products that threaten the health and safety of the American consumers.

One of the most effective U.S. civil tools against counterfeiting is what practitioners call Schedule A litigation. It allows rights holders to bring a single action against multiple, anonymous foreign sellers engaged in the same infringing conduct. Just as importantly, it allows the courts to quickly freeze the seller accounts and related assets before these proceeds disappear beyond the reach of U.S. jurisdiction. That changes the economics of infringement. Without this tool, rights holders are forced to file dozens or even hundreds of nearly identical lawsuits against anonymous defendants who have moved assets and simply reappear under new identities faster than the courts can reach a judgment.

Schedule A is one of the few law enforcement tools capable of matching the speed, scale, and anonymity of today's online infringers while preserving judicial efficiency and due process.

Online piracy presents an equally sophisticated challenge. Our recent organized piracy crime report published with the Digital

Citizens Alliance demonstrates that many of today's piracy operations have evolved in the criminal enterprises, built on a systematic theft of American intellectual property. A single network we examined reached more than 22 million subscribers and generated roughly \$288 million a month. When law enforcement dismantled that operation, they uncovered drugs, weapons, and crypto currency, evidence that these organizations are engaged in far more copyright infringement. Large scale piracy networks view IP theft as low risk, high reward criminal enterprise and changing the calculation is what IP House is built to do.

The enforcement gap is real and measurable. Rights holders are stuck with reactive platform tools that provide relief measured in just hours. More than 40 peer Nations now use court ordered site blocking to cutoff foreign, fully infringing content sites and services at the stores. The results have been significant. In the U.K., traffic to the targeted piracy fell nearly 89 percent after blocking orders took effect. The United States has not kept pace with its international partners, leaving creators, consumers, and businesses at a competitive disadvantage.

Meanwhile, criminal organizations are now using generative AI to accelerate infringement to an unprecedented scale. These include mass produced counterfeit listings and brand presentation to synthetic media as well the name, image, and likeness violation. While the technology is new, the underlying challenge is not. Bad actors continue to exploit innovation faster than our enforcement tools can adapt.

I hope my testimony today provides the Subcommittee with an operational perspective on how today's online infringement networks actually function, where the current enforcement tools are succeeding and where meaningful gaps remain. IP House is committed to working with Congress to ensure American innovators, creators, consumers, and businesses are protected in the digital age. Thank you.

[The prepared statement of Mr. Francis follows:]

House Judiciary Subcommittee on Courts, IP, AI & the Internet**Hearing: “A Midlife Crisis? IP and the Internet After 40” | June 30, 2026****Written Testimony of Steve K. Francis, Executive Chairman, IP House**

Chairman Issa, Ranking Member Johnson, and distinguished Members of the Subcommittee, thank you for the opportunity to submit this statement on the state of intellectual property (“IP”) theft on the internet. My name is Steve Francis. I am the Executive Chairman of IP House, a global IP investigations and enforcement firm that protects brands and creators online and offline from counterfeiting, piracy, and other forms of IP theft worldwide.

Before co-founding IP House, I spent over twenty-five years in federal law enforcement, including as Executive Associate Director of Homeland Security Investigations and as Director of the National Intellectual Property Rights Coordination Center (the “National IPR Center”). In that role I saw, day in and day out, how IP theft endangers the safety and security of the American public, drains our economy, and erodes the national and economic security of the United States. I bring that same mission to my work today.

My experience from both the public and private sectors affords me a unique perspective on the global IP theft problem: what online IP theft actually looks like in 2026, how profoundly it has changed in the evolving digital age, what it costs American rights holders and consumers, and how the tools available to confront it are working, and where they fall short.

I. The Scale of the Threat

The sale of infringing goods is one of the largest and fastest-growing forms of illicit commerce in the world. The most recent joint study by the Organization for Economic Cooperation and Development (“OECD”) and the European Union Intellectual Property Office (“EUIPO”) estimates that trade in infringing goods reached approximately USD 467 billion in 2021, accounting for roughly 2.3 percent of all global trade.¹

Broader estimates that account for infringing content place the total drag on the global economy far higher, estimated between USD 1.7 trillion and USD 4.5 trillion annually. This directly impacts the United States: IP accounts for an estimated 65 percent

¹ OECD/EUIPO, [Mapping Global Trade in Fakes 2025](#): Global Trends and Enforcement Challenges (OECD Publishing, 2025).

of the value of Fortune 500 companies. When IP is stolen at scale, the loss is real and tangible. American jobs, innovation, economic competitiveness, national security, and consumer safety are all directly undermined.²

China remains the dominant source of infringing goods, accounting for some 45 percent of reported seizures, increased to roughly 62 percent when goods routed through Hong Kong are considered. It is just as important to consider how infringing goods move. Bad actors have shifted decisively to small parcels and the mail: by 2020–21, shipments containing fewer than ten items accounted for 79 percent of all seizures, up from 61 percent only a few years earlier. By breaking shipments into thousands of small, low-value parcels, bad actors have engineered a distribution system designed to slip beneath the threshold of inspection despite the best efforts of U.S. customs inspectors.³

Infringing goods, however, are only part of the picture. Content theft inflicts a comparable toll on American creators and the broader economy. Infringing websites drew nearly 230 billion visits worldwide in 2023, a 6.7 percent increase from the previous year, with the United States consistently among the largest sources of that traffic.⁴ Industry analysts estimate that infringing content drains well over USD 75 billion each year from the film, television, music, software, and publishing sectors that are among America's most valuable exports.⁵

Gone are the days when counterfeits and bootleg DVDs moved mainly on street corners, in back alleys, and at weekend swap meets. The storefront has moved online, and it is far larger than the sidewalk ever was. Today it is twofold: legitimate online marketplaces that bad actors exploit to reach unsuspecting consumers, and fully infringing sites built for no purpose other than theft.

II. Infringing Goods - A Threat to Consumer Safety and Public Health

Infringing goods have crossed the line from a brand-protection problem into a systemic threat to consumer safety and public health. Our research into the infringing goods market identifies six categories where counterfeits routinely endanger lives: cosmetics and personal-care products containing toxic ingredients; food and beverages, including spurious liquor that has caused mass hospitalizations and deaths;

² Global economic-impact range (USD 1.7–4.5 trillion) as reported by Forbes (2018) and compiled in the U.S. Patent and Trademark Office / Library of Congress [Federal Research Division report on counterfeiting](#) (2020)

³ OECD/EUIPO, [Mapping Global Trade in Fakes 2025](#) (China-source, small-parcel, and de minimis figures).

⁴ MUSO and Kearney, [Global Piracy By Industry Report 2023](#)

⁵ Kearney estimates that digital piracy costs the global media and entertainment industry upward of USD 75 billion annually, with losses projected to approach USD 125 billion by 2028. See MUSO and Kearney, [Global Piracy By Industry Report 2023](#); ElectroIQ, [Piracy Statistics](#) (2025).

pharmaceuticals, including fake cancer drugs and antibiotics; electronics that cause fires and electrocution; children's toys that present choking and poisoning hazards; and automotive components such as infringing brake pads and airbags that fail at the worst possible moment.⁶

These are not hypothetical harms. An estimated one in four American consumers has purchased an infringing good, often without ever knowing it. A teenager buying a phone charger, a taxi driver replacing brake pads, a parent filling a prescription for their sick infant: each is a potential victim of a crime they cannot see. Recent work by the OECD has gone further, documenting how the infringing goods economy is sustained by forced labor embedded deep in global supply chains, meaning cheap fakes are not only dangerous to the buyer, but a product of systemic human exploitation and abuse.⁷

III. From Infringing Goods and Content to Organized Crime

Alarming, the networks behind large-scale online IP theft have in some cases matured into transnational organized crime. This is the central finding of a joint investigation IP House conducted with the Digital Citizens Alliance, published this year, drawing on interviews with law enforcement agencies across the globe and a review of criminal cases linking content theft operations to known organized-crime entities.⁸

The scale is staggering. In November 2024, European authorities dismantled what investigators called the continent's largest content theft operation, a network serving more than 22 million subscribers and generating roughly USD 288 million per month, about USD 3.5 billion per year. When police executed coordinated raids across eleven countries, they seized not only cryptocurrency and cash, but drugs and weapons. The operation was structured like a traditional crime syndicate: technical administrators managing servers across multiple countries, resellers distributing through pyramid-like networks, and organizers using encrypted communications and false identities to stay beyond reach.⁹

That convergence repeats across jurisdictions. In Operation Fake, Spanish law enforcement exposed an enterprise that combined content theft with cryptocurrency mining, property fraud, drug trafficking, and industrial-scale money laundering, resulting in 30 arrests and USD 12.7 million in frozen assets. A parallel Spanish case, Operation Atria,

⁶ IP House and ISB Institute of Data Science, *Counterfeit Crisis in India: Consumers, Consumption and Consequences* (2026).

⁷ Deaths/injuries and U.S.-consumer-purchase figures per published anti-counterfeiting research; OECD, [How counterfeit goods fuel forced labour](#) across global supply chains (January 2026).

⁸ Digital Citizens Alliance and IP House, [Organized. Piracy. Crime.](#): How Global Piracy Networks Became Organized Crime Syndicates — And What Needs to Be Done About It (April 2026).

⁹ Europol, [European law enforcement stops illegal IPTV service providers](#) (Nov. 27, 2024)

traced illicit revenues through the same payment rails used to evade international sanctions. Italy's notorious criminal gang Camorra has moved directly into illicit streaming as a means of low-risk, high-value revenue generation. In Canada, the operator of an illicit subscription service was separately convicted of cocaine trafficking. In Brazil, federal raids on an illicit streaming network seized firearms and ammunition alongside the subscription servers. In the United States, prosecutors pursued the KickassTorrents and Sparks Group cases under racketeering and organized-crime frameworks.¹⁰

International bodies have reached a worrisome conclusion. INTERPOL, Europol, and the United Nations Office on Drugs and Crime all recognize that major infringing content networks now meet the established criteria for organized crime syndicates: structure, scale, cross-border activity, profit motive, serious associated crimes, duration, and the use of violence and corruption. Investigators have also begun to connect these networks to the vast forced-labor 'scam compounds' in Southeast Asia, where the United Nations estimates hundreds of thousands of people are held and compelled to run online criminal operations.¹¹

While not all online infringers operate as part of a large organized criminal enterprise, the force driving both the syndicates and the individuals is the same: the enormous perceived financial reward. Gone are the days of the lone hobbyist assembling a small infringing site in a basement. Consider the Gears TV illicit-streaming business takedown: operating from 2016 to 2019, a single operator personally amassed roughly USD 30 million before federal authorities shut him down, and in 2023 he was sentenced to 66 months in prison and ordered to forfeit more than USD 30 million and pay over USD 15 million in restitution.¹² Whether or not a given operator carries an organized-crime label, the harm to rights holders is substantial and the illicit profits are very real.

For American families, the harm is immediate. Consumers who subscribe to an illicit content service with a credit card are roughly four times more likely to report unwanted charges, and in one study 72 percent reported fraud. A single investigation documented USD 121 million in malicious advertising on infringing sites engineered to infect consumer devices. And the so-called BadBox botnet — cheap off-brand streaming boxes sold to Americans as a gateway to free movies — arrived preloaded with malware.

¹⁰ DCA/IP House, [Organized. Piracy. Crime](#). (2026): Operations Fake and Atria (Spain); Camorra/IPTV (Italy); Arubox (Canada); MeuPlayer (Brazil); KickassTorrents and Sparks Group (United States).

¹¹ DCA/IP House, [Organized. Piracy. Crime](#). (2026), citing INTERPOL, Europol, and UNODC criteria and Southeast Asian forced-labour compound estimates.

¹² U.S. Department of Justice, U.S. Attorney's Office for the Eastern District of Pennsylvania, [Leader of Illegal Copyright Infringement Scheme](#) Sentenced to 5½ Years' Imprisonment (March 2023); *United States v. Carrasquillo* (E.D. Pa.).

The FBI concluded that more than one million devices worldwide were silently conscripted into a criminal proxy network. When an American reaches for an infringing good or an illicit stream, they are too often handing their money and their personal data to the same organizations that move drugs, launder money, and traffic human beings.¹³

IV. A National and Economic Security Problem

Because so much of this activity originates overseas and intersects with sanctions evasion, money laundering, and the financing of other serious crimes, online IP theft is properly understood as a national and economic security problem, not merely a commercial one. The same compromised supply chains that deliver a counterfeit airbag can deliver a counterfeit component into a critical military defense system. The same payment rails that launder illicit revenue can move money for sanctioned actors. When we allow anonymous foreign networks to operate against American brands with impunity, we are not only tolerating consumer fraud; we are ceding ground in the contest over secure supply chains and economic security that this Subcommittee and the broader U.S. Congress rightly take seriously.

These same dynamics are now driving the newest frontier of IP theft: the use of generative artificial intelligence to mass-produce infringing listings, impersonate trusted brands, and exploit an individual's name, image, and likeness through synthetic media. Our detection work at IP House increasingly surfaces generative AI-enabled infringement, and the underlying challenge looks quite similar to challenges surrounding infringing goods and content: anonymous actors, operating at scale and across borders, moving faster than any remedy currently available can reach them.

V. How Enforcement Works Today, and Where It Falls Short

Confronting this threat requires a layered toolkit, and this Subcommittee has been a leader in building it. For example, judicial site blocking is not a theoretical remedy. More than forty countries already use some form of it, and the results are measurable: IP House's own analysis found that traffic to blocked infringing sites fell 89 percent in the United Kingdom, 70 percent in Portugal, and 69 percent in Australia as a result of judicial site blocking. The mechanism is often narrow by design, requiring a court order to reach overseas operators beyond the practical reach of U.S. process, and it includes safeguards for legitimate intermediaries.¹⁴

¹³ Federal Bureau of Investigation, [Home Internet-Connected Devices Facilitate Criminal Activity](#) (2025)

¹⁴ IP House, [Overseas and Out of Reach](#), documenting traffic reductions following judicial site-blocking in the United Kingdom, Portugal, and Australia.

When it comes to online infringement of goods, one of the most effective civil tools American rights holders have, and which is currently under scrutiny in some courts, is what practitioners call Schedule A litigation. It lets rights holders of every size, from independent designers to national brands, bring a single civil action against numerous infringing foreign sellers operating through online marketplaces and standalone websites. In practice, it lets a court freeze the infringing sellers' assets before they can move funds out of reach and permits alternative service when traditional process is impractical against foreign defendants who deliberately hide. And, critically, it allows related cases to be joined — a point whose importance is hard to overstate. Without joinder, a brand facing a hundred anonymous foreign sellers on a single platform would have to bring a hundred near-identical lawsuits. That means a hundred dockets, a hundred hearings across dozens of judges, all on a hundred separate timelines — each draining the courts' resources and each likely to proceed in similar fashion.

Schedule A litigation provides rights holders of all shapes and sizes a clear path to justice. The economics of online IP infringement are punishing for smaller rights holders. Without joinder, meaningful enforcement becomes practical only for the largest companies with the deepest litigation budgets; leaving independent designers, creators, and small and mid-sized businesses to watch their rights be infringed with little realistic recourse. Allowing related claims to proceed in a single action enables rights holders to defend their IP and recoup lost revenue regardless of the size of their legal budget. In our experience, financial disruption is what produces lasting results: taking down individual listings matters, but it does not disincentivize the conduct on its own. Durable deterrence comes from reaching the money and, ultimately, the people behind it.

Financial recovery is only the first layer of deterrence. Because IP House maintains global investigative capability, expertise, and enforcement partnerships across major global jurisdictions, we can sometimes move from online detection to offline action using evidence lawfully obtained through discovery to trace major infringers to the source and, in some cases, support their arrest and prosecution in their home countries. This kind of source-level disruption, paired with freezing illicit proceeds, is among the most effective remedies available: it reaches not only the wrongdoer's profits but the individuals and supply networks behind the goods.

Beyond the benefits of recovered revenue, every illicit operation disrupted is a stream of dangerous or defective goods — the unsafe electronics, fake medications, and substandard auto parts I described earlier — that never reaches an American family. And because enforcement resources are finite, rights holders who bring these cases act as a force multiplier, reaching bad actors the government cannot pursue on its own. Schedule A

litigation is thus not just a private remedy; it is among the most effective civilian tools for curbing the supply of online infringing goods at scale, with the American consumer as the ultimate beneficiary.

Schedule A has been largely accepted and used in the federal courts since the early 2010s,¹⁵ but only recently has it drawn real scrutiny by some judges reconsidering how existing rules apply to the digital marketplace. It is not codified in any single statute; it is a practical application of existing Federal Rules, which is why its treatment can vary from court to court. Two areas of scrutiny deserve particular emphasis. First is the *ex parte* temporary restraining order which freezes an infringing foreign seller's accounts before the seller is notified of the suit. Some courts have begun to ask whether that relief is necessary, suggesting that a case proceed as normal federal litigation without *ex parte* relief from the outset. However, the entire value of the *ex parte* freeze lies in acting before the seller knows a lawsuit is coming, because these sellers move infringing listings and money within hours of learning they have been sued, not only to evade a freeze but to defy U.S. court orders outright. The risk is not hypothetical: there are Chinese online services that alert sellers of illicit goods to new lawsuits in real time, so they can shift assets before a court can act.¹⁶

Secondly, some courts have been questioning the use of Rule 20 joinder, which permits joining defendants when the relief asserted arises out of the same transaction, occurrence, or series of transactions or occurrences and share a common question of law or fact. Critics say these cases improperly group foreign anonymous sellers who should be sued separately because they are separate transactions from presumably different sellers. But that view reads the rule too narrowly. Rule 20 reaches not only a single transaction but also a single occurrence, or series of occurrences, the latter being a related pattern of conduct that produces common harm.¹⁷

Consider how online shopping actually works: a single checkout can pull together products from many different sellers, all operating on the same platform and moving through the same payment and shipping systems. The defendants in these cases exploit that same marketplace to infringe the same IP and harm the same brand, at the same time,

¹⁵ Schedule A litigation traces to the online counterfeiting cases of the early 2010s, including the Tory Burch (River Light V, L.P.) actions against anonymous online sellers in the U.S. District Court for the Northern District of Illinois (2010–2011).

¹⁶ <https://sellerdefense.cn/>.

¹⁷ *Chrome Cherry Limited v. Partnerships and Unincorporated Associations Identified on Schedule "A"*, 2021 WL 6752296, at *1 (N.D. Ill. 2021) (finding joinder of the Schedule A defendants proper at the preliminary stage because the claims arise out of the same occurrence or series of occurrences, Fed. R. Civ. P. 20(a)(2)(A)); see also *Bose Corp. v. Partnerships & Unincorporated Associations Identified on Schedule "A"*, 334 F.R.D. 511, 517 (N.D. Ill. 2020) (Durkin, J.) (finding no prejudice in permitting joinder of 17 internet alias defendants where none had appeared).

and in the same way. They need not be physically connected to one another: it is their use of the same vehicle to commit the same wrong, all at once, that makes their conduct a single occurrence or series of occurrences under Rule 20 – not any physical relationship among them. When courts read these rules too narrowly, demanding clear proof at the pleading stage that anonymous foreign sellers coordinate directly with one another, the result is not fairness but forcing rights holders to sue clearly infringing anonymous sellers one at a time while they dissipate funds and reappear under new seller accounts. The answer is not to abandon the tool but to apply it with discipline — requiring real evidence, meaningful jurisdiction, diligent efforts to identify defendants, and severance where joinder falls outside Rule 20's requirements. Refinement, not retreat, is the right course.

VI. The Indispensable Role of Public-Private Partnership

If I had to distill one lesson I carried out of my twenty-five years in federal law enforcement, it is that this fight cannot be won by government alone, or by the private sector alone. IP criminals operate across innumerable jurisdictions simultaneously; law enforcement is bound by borders, competing priorities, and understandably finite resources. Closing that gap requires genuine public-private partnership which is the model the National IPR Center was built on, and the model that has produced the most durable results in my professional experience.

IP House was founded to be a partner in exactly that sense. While we collaborate routinely with law enforcement globally on behalf of our clients, we also maintain a formal memorandum of understanding with the National IPR Center and recently entered into a similar memorandum of understanding with the United Kingdom Intellectual Property Office. Additional global partnerships are forthcoming as IP House continues to identify public sector partners to engage in this fight with us. Our role is to bring global intelligence, monitoring, evidence, and on-the-ground investigative capability to the table, and package it so that it is actionable for law enforcement and legitimate online platforms working to disarm the bad actors who manipulate e-commerce for illicit purposes. We do not seek to replicate or replace government and law enforcement; we seek to multiply its reach.¹⁸

That is the spirit in which I offer this testimony. IP House's value to this Subcommittee is as a source of truth on the reality of what is actually happening in the global market, what the illicit networks look like, how they move money and goods, and which enforcement tools are bending the curve. We are glad to make that visibility

¹⁸ [National IPR Center–IP House Memorandum of Understanding \(December 2024\)](#); [IP House–UK Intellectual Property Office Memorandum of Understanding \(2025\)](#).

available to the Subcommittee and to our federal enforcement partners whenever it is useful.

VII. Conclusion

Online IP theft has outgrown the frameworks built to contain it. Infringing goods and content operations endanger American consumers, drain the American economy, exploit forced labor abroad, and increasingly undermine our national and economic security. The good news is that effective tools exist, and IP House is committed to working with the Subcommittee to see these tools implemented, and for those that already exist, to remain. American rights holders, consumers, and courts deserve clarity and consistency in how those tools are applied. To that end, we respectfully encourage the Subcommittee to pursue three things: first, support durable judicial site blocking authority that includes safeguards for legitimate intermediaries; second, recognize the legitimacy of Schedule A litigation and encourage its consistent and disciplined application; and third, continue investing in the public-private partnership model embodied by the National IPR Center. The foreign criminals pushing dangerous IP infringing goods and stolen content into our market should not enjoy a procedural advantage over the U.S. rights holders working to safeguard their brands, their consumers, and the U.S. economy. IP House stands ready to assist this Subcommittee, federal law enforcement, and our partners with the intelligence and operational expertise to meet this threat. Thank you for the opportunity to submit this statement.

Mr. ISSA. Thank you. The gentleman yields back. Mr. Mohr.

STATEMENT OF CHRIS A. MOHR

Mr. MOHR. Chair Issa, Ranking Member Johnson, and the Members of the Subcommittee, thank you for the opportunity to appear here today.

Before I get into the substance, I just want to take a moment to thank you, Mr. Chair, on behalf of our Members. You have been a genuine ally to us on patents and a straight shooter even when we have disagreed. That leadership shows up here, too, convening round tables on foreign piracy, advancing thoughtful, site-blocking discussions, and choosing an educational hearing over a rush to markup. It has been a privilege to work with you, and we are grateful for the way that you have sought to both protect and advance American innovation.

SIIA represents more than 350 companies in the business of information, AI developers, publishers, financial data firms, and software creators. Unusually for a technology trade association, our members sit on both sides of many IP issues. We have platforms that distribute works and their rights holders. Some of our members have both functions.

Over the course of our 40-year existence, we have seen a lot of technological changes that have affected member operations, some of which caused them to bring competing world views. When examining new IP and other policy proposals, we tend to ask the same questions every time. Does existing law already address the harm? What new risks does the technology create? What limits make a statute both effective and constitutional?

I am going to briefly highlight two areas. Two years ago, SIIA testified in front of this Committee about unauthorized digital replicas. On digital replicas, the harm that these unauthorized uses cause is real. These AI-generated voices and likenesses are already defrauding consumers and exploiting performers. We support the creation of a Federal right here and we supported the TAKE IT DOWN Act last year as proof Congress can build precise, targeted tools for AI-enabled harms.

In terms of vehicles that have recently moved, the NO FAKES Act has received a lot of attention. From our perspective there are four problems that remain and each one is fixable.

First, the preemption clause grandfathers in existing State law and only displaces State regimes for expressive works. The bill doesn't really deliver on the promise of a national standard.

Second, the counter notification safeguard against wrongful takedowns only exists inside the bill's safe harbor framework, statutory damages up to \$750,000 per work and a life plus 70 terms, no company will risk staying outside that framework. In practice, this isn't a narrow opt-in category. It is close to the entire digital ecosystem operating under a takedown regime with no guarantee necessarily to put wrongly removed content back up. That raises concerns over speech at scale.

Third, there is no general intent requirement risking liability for general-purpose AI tools and inadvertent look-alikes alongside the actual bad actors.

Fourth, again, this goes to scope. The bill's frame is touching user-content platforms, but it reaches deep into the broader digital economy and shifts Section 230 treatment along the way. We don't have a problem with that resolution, but it emphasizes the importance of getting the details right.

Now, we have supplied red-line language on these issues. These are fixes, not objections to the bill's premise, and we are ready to keep working on it until we handle these problems correctly.

The second topic that I am going to address is foreign piracy and site blocking specifically. This is a different question, and our members are generally split onsite blocking as a remedy and my goal here is not to advocate a specific solution, but to present the equities that Congress has already begun to consider.

First, the underlying problem is real. These pirate sites sit outside U.S. courts' reach, and they keep operating through mirror domains and offshore hosting, no matter how many times they are shut down. The concerns over how blocking gets implemented are just as real. Blocking is a level of DNS resolvers, doesn't respect borders. Targets increasingly share cloud infrastructure with thousands of unrelated lawful sites, so a narrow order can have overbroad effects. Foreign experience shows that legitimate services can get swept up by mistake. We are not here to endorse or oppose a specific proposal. We are here to say that if Congress moves forward, four guardrails should be nonnegotiable: Real judicial process with some adversarial testing, not rubber-stamp petitions; targeting precise enough to protect shared infrastructure and lawful content; strong, good-faith safe harbors for the providers required to comply; and no mandate for a single government-prescribed technical method.

On both issues, our position is the same: Get the goal right, get the mechanism right, and we all win. Our members are going to have to operate under whatever regime Congress creates.

Thank you again for the opportunity to testify, and I welcome your questions.

[The prepared statement of Mr. Mohr follows:]



WRITTEN TESTIMONY OF

**Christopher A. Mohr, President & CEO
Software & Information Industry Association**

Before the
**United States House of Representatives
Committee on the Judiciary
Subcommittee on Courts, Intellectual Property,
Artificial Intelligence, and the Internet**

Hearing on
"A Midlife Crisis? IP and the Internet After 40"

June 30, 2026

I. INTRODUCTION

Chairman Issa, Ranking Member Johnson, and members of the Subcommittee: thank you for the opportunity to testify on behalf of the Software & Information Industry Association ("SIIA").

SIIA represents more than 350 companies in the business of information.¹ Our members include AI developers, publishers, educational-content companies, financial-data firms, and software creators whose works depend on strong intellectual-property protection. In the mid-1990s when we were known as the Software Publishers Association, we began helping our members enforce their IP rights and combat piracy, a practice we continue.

The business of information, however, has changed over time. SIIA is somewhat unique in the world of technology trade associations in that our membership includes both publishers and platforms. We have firms that act as services for the distribution of information, and those who hold the rights in that information. We come as an association whose members will have to *live under* whatever rules Congress writes—as claimants and as defendants, as rights holders and as services. Over the years, we have seen several new technologies introduced, all of which has caused this Subcommittee to look at existing law and determine whether it continues to provide the foundation needed to protect IP and promote innovation.

Indeed, over the last four decades, we have seen so much technological change that the phrase "digital revolution" has become a cliché. And in each instance, there have been demands for changes in the law to respond to that technology. But in each instance, we (and the House Judiciary Committee) have considered these demands based on three foundational questions:

- First, are the harms that Congress seeks to remedy already addressed by existing law?
- Second, does the new technology create unique risks that current law does not address?
- Third, what explicit limits—above all, First Amendment limits—must the statute contain to be both effective and constitutional?

A perfect example of this approach involves the passage of the Digital Millennium Copyright Act (DMCA) in 1998. At that time, the effect of advances in digital technology on the dissemination of SIIA members' works created a tremendous opportunity and a tremendous risk: opportunity, in that the advances created the

¹ SIIA represents more than 350 companies spanning the information lifecycle, from startups to the world's largest technology and content firms. See [Software & Information Industry Association](#).

ability for companies to reach a whole mass of users that they could not reach before, and risk, in that through the use of the technology, their works could be subject to large-scale misappropriation and made available without permission or payment. Congress recognized that without adjusting the ecosystem in which these works would live, the promise of the Internet as an online market for copyrighted works would never be reached.² At the same time, however, the Committee feared that without a certain degree of legal clarity—and insulation from copyright liability—online service providers would not make the necessary investments in infrastructure that would permit the widespread dissemination of copyrighted works.³

The DMCA advanced these goals through two principal means. The first involves section 1201, which prohibits the circumvention of devices that control access to a copyrighted work, or trafficking in such devices, subject to a specific list of detailed exceptions such as encryption research, security testing, reverse engineering, and law enforcement.⁴ The second involves section 512, which the Committee enacted to give online service providers a safe harbor from copyright liability if, once informed, they expeditiously remove access to infringing material and comply with the statute's other requirements.⁵ It also contains a put-back procedure: if the user files a counter-notice, the service provider must restore access to the material within 10 to 14 days unless it receives notice that the copyright owner has sought a court order seeking to restrain alleged infringement.⁶

Experience has demonstrated the soundness of the animating principles that motivated the DMCA's passage. The copyright industries have grown in the intervening years, and online content has increased considerably. Although piracy remains a problem, it is also true that paid services have flourished: from database subscriptions to cloud software to online streaming. And many of our members have both sets of interests: in some circumstances, they are content providers and in others act as service providers. And the inclusion of a counter-notification process properly recognized that not every claim of infringement will have merit,

² See S. Rep. 105-190 (May 11, 1998), at 8-9 (noting Congressional intent that the DMCA would form "the legal platform for launching the global digital on-line marketplace for copyrighted works. It will facilitate making available quickly and conveniently via the Internet the movies, music, software, and literary works that are the fruit of American creative genius. It will also encourage the continued growth of the existing off-line global marketplace for copyrighted works in digital format by setting strong international copyright standards.").

³ *Id.*

⁴ See 17 U.S.C. §§ 1201 (g) (encryption research); 1201(j) (security testing); 1201(f) (reverse engineering). Section 1202 prohibits the alteration or removal of copyright management information.

⁵ 17 U.S.C. § 512. See also S. Rep. 105-190, at 19-20.

⁶ 17 U.S.C. § 512(g).

and that platforms should not be in the position of having to judge that merit. While there is no First Amendment right to piracy, this procedure respected the speech policy interests implicated by overbroad infringement claims.

With the growth of AI, we find ourselves in a similar moment to 1998. When SIIA appeared before this Subcommittee about two years ago, we offered Congress three questions to ask before legislating in this area, questions very similar to those that we asked above. That framework remains sound, and we reiterate it today, because it explains both why we support a federal digital-replica right and why the details of the NO FAKES Act still require work. We appreciate the way this Subcommittee has approached both issues and thank the Chairman for his leadership.

AI is a revolutionary technology. In the same way that the Internet's adoption created widespread risks and opportunities, AI has created the same kinds of problems around digital replicas. SIIA championed the TAKE IT DOWN Act, signed into law in 2025, precisely because we believe Congress can and should act against discrete, well-defined AI-enabled harms.⁷ We support a predictable federal framework that preserves the integrity of a person's identity online. The harms that motivate digital replica legislation are real, concrete, and economically disruptive. Unauthorized digital replicas are already being used to defraud consumers, to exploit performers, and to damage personal reputations. The question is not whether Congress should act, but how precisely.

The Subcommittee has highlighted two areas that require legislative consideration. The first involves digital replicas. The NO FAKES Act of 2026 (S. 4591) represents a significant structural evolution toward a workable federal right, and the Senate Judiciary Committee's unanimous vote to advance it reflects genuine progress.⁸ But there are still many in industry, including SIIA, who agree that the bill as currently drafted requires critical improvements. Four specific, operational flaws in the current substitute text would create severe market frictions and unintended legal exposure for software infrastructure, developers, and ordinary users if the bill is enacted without adjustments.⁹ Each of the four flaws can be fixed with focused

⁷ TAKE IT DOWN Act, Pub. L. No. 119-12 (signed May 19, 2025); see S. 146, 119th Cong. (2025), [congress.gov/bills/119/congress/senate/bills/146](https://www.congress.gov/bills/119/congress/senate/bills/146). The statute criminalizes nonconsensual intimate imagery, including AI-generated "digital forgeries," and directs covered platforms to establish a notice-and-removal process.

⁸ The Senate Judiciary Committee advanced S. 4591 by unanimous voice vote on June 18, 2026; three members raised First Amendment concerns without opposing passage. See [AI deepfakes bill advanced by Senate Judiciary Committee](#), Roll Call (June 18, 2026).

⁹ See [Letter from SIIA, the Computer & Communications Industry Association, NetChoice, and TechNet to Chairman Grassley, Ranking Member Durbin, Chairman Jordan, and Ranking Member](#)

drafting. We respectfully urge the Subcommittee to look closely at the bill before advancing it.

The Subcommittee has also signaled interest in a second, distinct topic—one unrelated to digital replicas: judicial site blocking. Although offshore piracy is not new, it persists as a challenge that traditional domestic enforcement has failed to curb. In evaluating this issue, we return to the same foundational framework that has guided our advocacy since 2024: (1) does existing law cover the activity; (2) are there specific risks posed by the foreign nature of the conduct that current remedies cannot reach; and (3) what limits—chief among them those rooted in the First Amendment—must any new mechanism observe to be both effective and constitutional. Because our membership includes both rights holders pursuing infringers and the infrastructure providers that blocking orders would reach, we offer a candid assessment of where the case for a federal remedy is strongest, where the technical risks are most acute, and what guardrails remain essential should Congress elect to move forward.

II. THE HARM OF DIGITAL REPLICAS IS REAL — AND PARTLY ALREADY ADDRESSED

The conversation about the need for a federal digital replica right should focus not on *whether* we need such a right but *how* to create it, including how precisely to draft legislation to prevent collateral damage and the impingement of lawful speech.

It helps to begin with what the existing law already does. As we explained in 2024, a substantial body of technology-neutral law already captures the core vectors of malicious exploitation. Section 43(a) of the Lanham Act reaches false endorsements that misuse a person's name, image, or likeness; the state rights of publicity reach unauthorized commercial uses of identity even absent consumer confusion; common-law privacy torts—defamation, false light, intentional infliction of emotional distress—reach reputational and dignitary harms; and federal law already provides a civil action for the nonconsensual disclosure of both real and forged intimate images.¹⁰ These doctrines are (with the exception of TAKE IT DOWN) technology neutral.

The TAKE IT DOWN Act is the model worth emulating. It was a targeted, consensus-driven federal response to a distinct AI-enabled harm—nonconsensual intimate imagery—and it achieved that end without rewriting the liability of upstream

[Raskin re: The NO FAKES Act of 2026](#) (June 16, 2026) (describing multi-trade concerns with the current state of NO FAKES) (hereinafter, "Coalition Letter").

¹⁰ See 15 U.S.C. § 1125(a) (Lanham Act § 43(a), false endorsement); 15 U.S.C. § 6851 (federal civil action for nonconsensual disclosure of intimate images); Restatement (Third) of Unfair Competition §§ 46–47; *Carson v. Here's Johnny Portable Toilets, Inc.*, 698 F.2d 831 (6th Cir. 1983).

software developers or destabilizing the broader software ecosystem.¹¹ The contrast is instructive: Congress has proven that it can build a precise tool for a specific harm. The same discipline should govern replica legislation, including the NO FAKES Act, which can be read to sweep far more broadly than its sponsors intend.

Unlike copyright law, which preempts state activity, rights of publicity and affiliated rights exist under state statutes and common law. Protection for digital replicas does exist, but in many different flavors. We believe that AI development would greatly benefit from a uniform set of nationwide federal rules, instead of a fragmented legal landscape that creates compliance confusion and can deter innovation.¹² In our December 2025 Federal AI Legislative Roadmap,¹³ we urged Congress to preempt state laws on foundation models and state laws that single out AI-enabled products for different treatment. In contrast, we urged it to preserve technology-neutral laws of general applicability as well as traditional areas of state concern such as insurance and sectoral uses within state or local control. That same logic applies to a federal digital replica right.

S. 4591 would establish a federal property right in a person's voice and visual likeness that extends post-mortem—up to 70 years after death—and is transferable and licensable by heirs and assignees.¹⁴ At that scope and duration, with statutory damages attached, ambiguities in the liability and safe-harbor provisions are not minor technicalities. They are the difference between a workable national standard and a decades-long source of litigation risk.

So, we return to the three framing questions we offered in 2024, now repurposed as a test of the *mechanism* rather than the premise:

- (1) Are the targeted injuries already addressed by existing law, including as applied to technologies that predate generative AI?
- (2) Are there areas of specific risk that are genuinely unique to generative AI and left unaddressed by current law?
- (3) What explicit limits—above all, First Amendment limits—must the statute contain to be both effective and constitutional?

¹¹ TAKE IT DOWN Act, *supra* note 7.

¹² SIIA, [The SIIA Federal AI Legislative Roadmap](#) (Dec. 2025) (Pillar 3, Promoting Federal-Led Harmonization). SIIA supports strong federal preemption so that a single, clear set of rules applies nationwide in place of a fragmented state patchwork.

¹³ *Id.*

¹⁴ S. 4591 § 2(b)(2)(A) (post-mortem right terminating no later than 70 years after death; transferable and licensable by heirs and assignees). See also [Senate Judiciary advances NO FAKES Act on unanimous vote](#), S&P Global (June 18, 2026).

The NO FAKES Act answers the first two questions well enough to justify a federal right. Federal law does not contain a right of publicity, and uniformity is needed. Similarly, in the same way that widespread internet deployment created piracy risk, the misuse of digital replicas using readily available AI tools warrants a federal solution. It is the third question—limits and precision—where the current text falls short.

A. The No Fakes Act Requires Four Structural Corrections

S. 4591 would create a federal “digital replica” right: each individual (and, after death, the right holder) may authorize the use of a computer-generated, highly realistic representation that is readily identifiable as that person’s voice or visual likeness.¹⁵ The Act imposes civil liability on those who make unauthorized replicas available to the public, and on those who distribute tools primarily designed to produce them.

It then layers on a notice-and-takedown system modeled on the DMCA but with less balance: providers of a defined class of “online services” receive a safe harbor if they register an agent, adopt a repeat-infringer policy, and remove or disable material upon proper notice, subject to a counter-notification process. It exempts libraries, archives, and accredited educational institutions, and it excludes news, documentary, commentary, criticism, satire, and parody under First Amendment principles. Statutory damages range from \$5,000 per work to as much as \$750,000 per work for services that fail to make a good-faith effort to comply—much higher than the statutory damages available for standard copyright infringement under 17 U.S.C. § 504(c).¹⁶

The current substitute amendment adds a counter-notification process, exemptions for libraries, archives, and educational institutions, and First Amendment-based exclusions for news, commentary, satire, and parody.¹⁷ We do not take that progress for granted. But four problems remain, and each would undermine the bill’s own objectives if left unaddressed.

¹⁵ NO FAKES Act of 2026, S. 4591, 119th Cong. (Coons-Blackburn substitute amendment). Section references throughout are to that substitute text.

¹⁶ S. 4591 § 2(e)(5) (statutory damages ranging from \$5,000 per work to as much as \$750,000 per work for an online service that fails to make a good-faith effort to satisfy the safe-harbor obligations). See also [AI deepfakes bill advanced by Senate Judiciary Committee](#), Roll Call (June 18, 2026).

¹⁷ Coalition Letter, *supra* note 9.

1. The preemption clause fails to establish a true national standard.

The central promise of a federal bill—the reason one is needed at all—is a single, uniform national rule in place of a growing state patchwork. The current text does not deliver that. Section 2(g) preempts state causes of action only as to a digital replica “in an expressive work,” and a rule of construction expressly preserves every state statute and common-law cause of action regarding digital replicas that was in existence as of January 2, 2025.¹⁸ The preemption clause thus carries two defects at once: it grandfathers in the entire existing body of state law, and it limits federal exclusivity to the ambiguous category of “expressive” works, leaving non-expressive and general commercial uses potentially outside the federal standard.

Tennessee’s Ensuring Likeness, Voice, and Image Security Act of 2024 (the “ELVIS Act”) shows why this matters. The ELVIS Act expanded the state’s property right to cover voice simulations, established broad civil liability for distributing unauthorized tools and software, and extended liability in certain advertising contexts to anyone who “reasonably should have known” of an unauthorized use—a subjective standard well beyond actual knowledge.¹⁹ Because the NO FAKES preemption clause grandfathers laws in existence as of January 2, 2025, a sweeping state regime like the ELVIS Act would continue to operate *underneath* the new federal right, including its liability for software tools.

By omitting existing state laws and by limiting preemption to “expressive” works, the bill affirmatively permits a fragmented, state-by-state compliance landscape to persist. A company seeking in good faith to comply would still face one federal standard *plus* multiple state regimes, each with its own definitions, exceptions, knowledge standards, and remedies. That is the opposite of uniformity, and it undercuts the bill’s central sales pitch. Notably, the lead Senate sponsor has described NO FAKES as one component of a single national “rulebook” for AI.²⁰ The preemption language should match that ambition.

¹⁸ S. 4591 § 2(g). The rights established by the Act preempt state causes of action only as to a digital replica “in an expressive work,” and a rule of construction expressly preserves state statutes and common-law causes of action in existence as of January 2, 2025.

¹⁹ Ensuring Likeness, Voice, and Image Security Act of 2024 (ELVIS Act), Tenn. Pub. Acts ch. 1004 (eff. July 1, 2024), amending the Tennessee Personal Rights Protection Act. The Act extends liability to the distribution of an “algorithm, software, tool, or other technology, service, or device, the primary purpose or function” of which is producing an identifiable individual’s voice or likeness and applies a “reasonably should have known” standard to certain advertising. See Manatt, Phelps & Phillips, [Tennessee’s ELVIS Act Expands Publicity Rights](#) (2024).

²⁰ Senator Marsha Blackburn has framed NO FAKES as one component of a single national “rulebook” for AI. See [AI deepfakes bill advanced by Senate Judiciary Committee](#), Roll Call (June 18, 2026).

This problem is not insoluble. Broadening the preemption provision to preempt state common-law and statutory rights of publicity as applied to digital replicas would provide uniform standards that businesses can operationalize.

2. Counter-notification scope and procedural asymmetry.

Section 2(a)(5)(A) defines “online services” to reach three categories: services that predominantly provide public access to user-uploaded material; certain digital music providers; and other interactive computer services that affirmatively opt in by registering a designated agent.²¹ Everything else falls outside the definition—including services that host professionally produced rather than user-uploaded content, and services that host private content. Familiar examples include most video-streaming services, app stores, video-game stores, and private cloud services. The problem is that the bill’s counter-notification mechanism runs only through the online-service safe harbor, so it is unavailable within this large category of services, and to the creators who depend on them but do not meet the definition of online services.²²

This differs from the DMCA considerably, and it creates incentives towards over-removal. The safe harbor is the rational way to manage statutory-damages exposure. As a result, services will default to taking content down upon receiving a notice—whether or not the material is actually unauthorized, actually depicts the claimed individual, or is even AI-generated at all.

Where an out-of-scope service has no counter-notice right to restore wrongly removed work, the asymmetry is total: easy to remove, nearly impossible to restore. The public will experience this as censorship by the platforms, and lawful online speech will be measurably less robust.

In addition, the bill’s procedural flaws are actively speech-detering. Section 2(d)(4)(B)(i) requires a counter-notification to bear a physical signature “witnessed or attested to in person by a licensed notary public.”²³ Current law provides ample opportunities to instill the requisite gravity into counter-notice representations. First,

²¹ S. 4591 § 2(a)(5)(A) (defining “online service” to reach (i) services predominantly providing public access to user-uploaded material, (ii) certain digital music providers, and (iii) other interactive computer services only if they register a designated agent). Services outside this definition include many video-streaming services, app and game stores, and private cloud services.

²² S. 4591 § 2(d)(1)(B)(ii)(II), (d)(4). The counter-notification mechanism operates through the safe harbor available to providers of an “online service,” leaving creators on out-of-scope services without an equivalent restoration mechanism.

²³ S. 4591 § 2(d)(4)(B)(i) (requiring a counter-notification to bear “[a] physical signature, witnessed or attested to in person by a licensed notary public”). By contrast, an initial takedown notification under § 2(d)(3) requires only a physical or electronic signature.

28 USC 1746 permits an affiant to sign under penalty of perjury. Second, federal electronic signature laws, 15 USC 7001 *et seq.* permit the use of electronic signatures on all but certain specified kinds of documents.

In contrast, the initial takedown notice under Section 2(d)(3) requires only a physical or electronic signature. There is no plausible justification for the disparity. And this right is susceptible to abuse by people who may wish to have unflattering videos of themselves taken down. The risk is that a large amount of lawful speech will be unnecessarily suppressed.

Once again, the changes are straightforward. First, strike the in-person notary requirement in Section 2(d)(4)(B)(i) and align the procedural weight of notices and counter-notices, so that mistaken claims can be corrected. Second, make counter-notification available wherever content has been removed under the Act, including for the large categories of professionally produced and private content.

3. General-purpose tool safe harbor and the missing intent requirement.

The bill is meant to reach bad actors who deliberately make and traffic in unauthorized replicas. In two respects, however, it risks reaching parties who are not the intended targets. First, while Section 2(d)(1)(A) provides a safe harbor for products and services merely “capable of” producing replicas, the carve-back in Section 2(c)(2)(B)—for tools “primarily designed,” of “limited commercially significant purpose” other than, or “marketed” to produce unauthorized replicas—does not clearly and cleanly exclude general-purpose AI tools.²⁴ Second, because liability turns on whether content is “readily identifiable” as a particular person, the bill leaves the door open to liability for inadvertent lookalikes, with no general requirement of intent.²⁵

Our members advocate for an intent requirement. We recognize that these factors appear in section 1201 of title 17 around anti-circumvention tools and access controls. But consumer adoption and use of AI tools is far more widespread than the use of decryption tools and the use of AI to create replicas is in many cases completely legitimate. So long as a credible argument remains that general-purpose AI tools

²⁴ S. 4591 § 2(d)(1)(A) (safe harbor for products and services capable of producing digital replicas, except those described in § 2(c)(2)(B)); § 2(c)(2)(B) (liability for tools “primarily designed,” of “only limited commercially significant purpose” other than, or “marketed” to produce unauthorized replicas of a specifically identified individual). SIIA and allied organizations have provided redline text to clarify that providers of general-purpose tools are not liable.

²⁵ S. 4591 § 2(a)(2)(A) (digital replica must be “readily identifiable” as the individual). The Committee adopted a manager’s amendment addressing purely coincidental resemblance, *see* § 2(e)(3), but the Act does not require intent as a general element of liability for creating a replica. *See AI deepfakes bill advanced by Senate Judiciary Committee*, Roll Call (June 18, 2026).

could be swept in, enterprising class action litigators will use the in terrorem effect of statutory damage multipliers to harmfully tax AI development.

Unfortunately, the concern we raised in 2024 remains: an overbroad cause of action chills legitimate software development.²⁶ On balance, we believe an intent requirement better aims the bill against its real targets while protecting the developers and good-faith creators the bill was never meant to reach. SIIA and allied organizations have already supplied redline language accomplishing the general-purpose-tool and intent changes.²⁷

4. Ambiguity in the scope of the bill.

The Committee should have no illusions about the scope of NO FAKES: it represents a significant change to the entire information ecosystem, and not all that change is obvious. The bill organizes its safe harbor around "online services," but it leaves many services outside that definition—video-streaming services, app stores, private cloud providers, video-game stores, and more—exposed to liability based on an actual-knowledge standard.²⁸

While the language is subtle, the incentive is not: opt into the safe harbor or take your chances with the class action bar. And that reveals the deeper problem with how the bill is framed: presented as a focused measure for digital replicas on user-content services, it in fact creates pressures and incentives across the entire digital ecosystem. That framing matters because the bill redistributes the DMCA balance and shifts Section 230 immunity—and it does so, in some measure, for most of the digital economy while being couched as far more narrowly scoped.²⁹

²⁶ [Statement of Christopher A. Mohr](#), President, SIIA, before the H. Comm. on the Judiciary, Subcomm. on Courts, Intellectual Property, and the Internet, "Artificial Intelligence and Intellectual Property, Part II – Identity in the Age of AI" (Feb. 2, 2024).

²⁷ S. 4591 § 2(d)(1)(A), (c)(2)(B).

²⁸ S. 4591 § 2(c)(3)(B), (c)(4)(G) (entities that are not "online services" incur liability on a showing of actual knowledge, or willful avoidance of knowledge, and must act expeditiously upon obtaining actual knowledge). These services receive none of the Act's notice, counter-notice, or agent-registration framework.

²⁹ S. 4591 § 2(h)(1) (treating the section as "a law pertaining to intellectual property" for purposes of 47 U.S.C. § 230(e)(2)). The effect is to place covered conduct outside the Section 230 liability shield that otherwise governs much of the digital ecosystem. There is a circuit split regarding whether right of publicity claims against internet platforms are barred by Section 230 or fall outside of Section 230's scope because they are intellectual property claims. *Compare Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118–19 (9th Cir. 2007) (holding Section 230 immunity still applied for state-law based claims, including right of publicity, because the carve-out for Section 230 protection applied only to federal intellectual property laws) with *Hepp v. Facebook*, 14 F.4th 204, 210–12 (3d Cir. 2021) (holding Section 230 immunity did not apply for state-law based claims, including right of publicity, because the carve-out for Section 230 protection was not limited only to federal intellectual property laws and

The breadth of services affected is critical precisely because of the incentives the bill creates. As we discussed in our 2024 testimony, the rights of publicity implicate multiple kinds of interests. In the case of a digital replica creating a false endorsement that violates the Lanham Act, a strong argument exists that such a tort implicates an intellectual property right. Other cases, however, such as the use of a digital replica in a way that presents a non-public figure in a false light, implicate dignity interests. The bill treats both violations as “intellectual property,” to which section 230 immunity does not apply. Thus, the dynamic reaches across the whole digital ecosystem.

Faced with statutory damages that can reach \$750,000 per work,³⁰ a rational service will not risk a complex, fact-specific legal defense. The rational business choice is immediate, often automated, deletion of user content. Experience under the DMCA confirms the pattern: takedown regimes have been misused to force lawful works—independent games, for example—off the platforms they depend on.³¹ By remaining silent about how out-of-scope services should handle replica allegations, the bill risks increasing that problem across the digital ecosystem because counter notification is even more limited than under the DMCA.

Although there is generally no First Amendment right to distribute harmful digital replicas that infringe the rights of other individuals, the actions of a platform to determine what content it will host, remove, restrict, or prioritize represent protected editorial discretion. But while the legal system may categorize this as private content moderation based on private rights, the public will experience it as mass censorship. Political satirists, independent artists, and ordinary citizens will find lawful expression erased by risk-mitigation algorithms—not because Congress intended that result, but because the statutory framework rewards reflexive removal.

It may be that these results are unintended. This problem could be addressed by simply stating the intent around non-online services directly. At a minimum: (1) extend counter-notification to these services; (2) provide clear, service-by-service designation for registered agents, so that registering an agent for one service does not opt a company’s other, out-of-scope services into the regime; and (3) identify the non-online services explicitly in the bill text and state which requirements apply to them and which do not. Clarity here will reduce both litigation and over-removal.

included state intellectual property laws like right of publicity); see also Ned T. Himmelrich, [Right of Publicity May \(or May Not\) Be Intellectual Property Under Section 230](#), [gfrlaw.com](#) (Feb. 22, 2024).

³⁰ S. 4591 § 2(e)(5).

³¹ Experience under the Digital Millennium Copyright Act shows that takedown regimes can be misused to force lawful works—such as independent games—off distribution platforms.

B. These are Fixes to the NO FAKES Act, Not a Teardown

Again, we believe these problems are fixable. SIIA supports a federal digital replica right. Each of the four issues above shares a common thread—left unaddressed, the current text would generate fragmentation, uncertainty, and the suppression of lawful expression. Each can be cured with modest, targeted drafting changes of exactly the kind already reflected in the bill's evolution to date.³²

This is not an abstract offer. SIIA and other organizations have already supplied redline language on most of the issues identified, and we are prepared to supply redline language for the rest, so that the bill becomes operationally viable. We stand ready to work with Members and staff to finalize this important legislation.

III. JUDICIAL SITE BLOCKING

We turn now to a distinct topic—one unrelated to digital replicas—on which the Subcommittee has signaled growing interest: judicial site blocking. We return to the issues we posed before: (1) does existing law cover the activity; (2) are there specific risks posed that need to be addressed; and (3) the limits necessary to make proposed legislation both effective and constitutional.

The issue in this discussion is not whether digital piracy is illegal. It is and it should be, given the deep harm it causes to the creative and content sectors and, increasingly, to those who frequent pirate websites. And of course none of our members condone this sort of illegal online activity.

Currently, US copyright holders have no targeted judicial remedy when they find their protected content is being shared openly and illegally on a foreign pirate site because these web sites lie beyond the jurisdiction of U.S. courts. While a pirate website may be located in a jurisdiction that U.S. courts cannot reach—and there are many—there are domestic service providers who could, in theory, be asked to cease providing access to these sites. Section 512(j) of the DMCA contemplates an injunction against a service provider, but that procedure has not been successfully used and is widely viewed by copyright owners as well intended but practically useless. The most damaging pirate sites are deliberately established offshore and structured to evade domestic notice-and-takedown architecture and the reach of U.S. courts.

SciHub is a particularly notorious, but not isolated example. Since 2011, Sci-Hub has remained the world's largest repository of pirated journal articles, stolen from academic and research institutions. Its creator, who lives in Moscow, has used credentials phished from institutional users to access those systems. Sites like this

³² Coalition Letter, *supra* note 9.

create both piracy risks and cybersecurity risks.³³ The London Police, for example, have warned institutions not to use SciHub because of the risk of system compromise as well as IP theft, and there is evidence that its proprietor is working with Russian intelligence.³⁴ It has been the subject of several blocking orders in the EU and elsewhere,³⁵ and US judgments have been received against its proprietor—who is protected from these judgments by remaining in Russia.

All our members, no matter what their business models, oppose this kind of activity. Indeed, the controversy around site blocking does not involve the desirability of the activity or the lack of sufficient remedies. Instead, it typically relates to the efficacy and possible unintended consequences, which will be important to properly calibrate. We therefore commend the Chairman and other members of the Subcommittee for the thoughtful manner in which they have convened roundtables on this problem. In the House, Chairman Issa has issued a discussion draft of the American Copyright Protection Act (ACPA), Representative Lofgren introduced the Foreign Anti-Digital Piracy Act (FADPA), and a bipartisan discussion draft, the Block BEARD Act, has circulated in the Senate.³⁶

SIIA has no position on site blocking legislation. Because this is an evolving area and the equities are genuinely contested among our members, we offer an informed but deliberately balanced view.

A. The Case for a Blocking Remedy

Proponents, including some SIIA members in the publishing community, make a focused argument. The injunctive-relief authority already in the DMCA, 17 U.S.C. § 512(j)(1), has gone largely untested, and they contend it is overdue for judicial use. They point to the United Kingdom, where blocking orders have been implemented through the largest retail ISPs—the so-called “Big Six,” which serve more than 60% of the broadband market—as evidence that a workable framework is possible, while

³³ Daniel S. Himmelstein et al., [Research: Sci-Hub provides access to nearly all scholarly literature](#) (Feb. 9, 2018).

³⁴ Shane Harris & Devlin Barrett, [Justice Department investigates Sci-Hub founder on suspicion of working for Russian intelligence](#) (Dec. 19, 2019).

³⁵ See, e.g., The Hindu Bureau, [Delhi High Court Orders Sci-Hub to Be Blocked in India](#), The Hindu (Aug. 23, 2025); Ernesto Van der Sar, [French ISPs Ordered to Block Sci-Hub and LibGen](#), TorrentFreak (Mar. 31, 2019); [Les éditeurs scientifiques se liguent contre la piraterie](#), L’Echo (Oct. 16, 2019) (in French) (Belgium).

³⁶ Foreign Anti-Digital Piracy Act (FADPA), H.R. 791, 119th Cong. (2025) (Rep. Lofgren), [congress.gov/bill/119th-congress/house-bill/791/text](#). A bipartisan discussion draft, the Block BEARD Act of 2025 (Sens. Tillis, Coons, Blackburn, and Schiff), has also circulated in the Senate.

acknowledging that the U.S. market is more fragmented, with roughly a dozen large ISPs and some 3,000 smaller providers.³⁷

In addition to SciHub, among the strongest examples for the need to establish a statutory remedy are the dedicated “shadow libraries”—LibGen, Anna’s Archive, and Z-Library—which continue to operate through mirror sites, domain changes, and offshore hosting even after enforcement actions, including a U.S. criminal copyright prosecution arising from Z-Library.³⁸ For rights holders that spend \$1 million or more each year fighting an endless game of “whack-a-mole,” blocking can look like the only remaining effective remedy once all other avenues are exhausted. “From the standpoint of copyright owners, the availability of this kind of remedy has taken on increased importance because of the Supreme Court’s decision in *Cox Communications v. Sony Music**, which narrowed ISP contributory liability to cases of inducement or services tailored to infringement. Against that backdrop, many content owners believe that a statutory blocking mechanism—if properly bounded—is increasingly the only remaining tool rights holders have against offshore pirates. Supporters also note substantial international precedent: by some counts more than 50 countries permit website-blocking injunctions, and proponents argue that well-designed regimes reduce piracy and increase legitimate consumption without blocking lawful content.”³⁹

B. The Case for Caution

Critics—including infrastructure providers, some platforms, and civil-society organizations such as Public Knowledge and the Electronic Frontier Foundation—

³⁷ The injunctive-relief authority of 17 U.S.C. § 512(j)(1) of the DMCA remains largely untested. See generally U.S. Copyright Office, [Section 512 of Title 17: A Report of the Register of Copyrights](#) at 58–61 (May 2020). The United Kingdom has implemented judicial site blocking through its largest retail ISPs, while the U.S. market features roughly a dozen large ISPs and some 3,000 smaller providers. See Jeremy Blum & Andrew Butcher, [English High Court issues blocking order targeting movie-hosting cyberlocker](#), Kluwer Copyright Blog (Mar. 2, 2022); [List of All Internet Companies in the US](#), BroadbandNow (last visited Jun. 28, 2026).

³⁸ Despite aggressive enforcement efforts—including the Department of Justice’s criminal prosecution of the alleged operators of Z-Library and repeated domain seizures—major shadow libraries such as Z-Library, LibGen, and Anna’s Archive continue to reappear through mirror domains, alternative domain names, and distributed technical infrastructure. See Press Release, U.S. Dep’t of Just., [Two Russian Nationals Charged with Running Massive E-Book Piracy Website](#) (Nov. 16, 2022); Ernesto Van der Sar, [Z-Library Returns on the Clearnet in Full Hydra-Mode](#), TorrentFreak (Feb. 13, 2023); Andrew Albanese, [Elsevier Awarded \\$15M in Lawsuit Against Pirate Sites](#), Publishers Weekly (June 23, 2017); Off. of the U.S. Trade Representative, [2025 Review of Notorious Markets for Counterfeiting and Piracy](#) 33–34 (2026).

³⁹ See Information Technology and Innovation Foundation, [Blocking Access to Foreign Pirate Sites: A Long-Overdue Task for Congress](#) (June 9, 2025) (reporting that at least 50 countries permit website-blocking injunctions and 39 actively block pirate sites). See also Copyright Alliance, [The Facts About Judicial Blocking of Foreign Piracy Sites](#) (Feb. 10, 2025).

raise concerns about overblocking.⁴⁰ The first is technical. Blocking implemented at the level of "alt-DNS" resolvers (such as the public resolvers operated by major technology companies) cannot easily be geographically cabined, so a U.S. order can have global effect. In Europe, several providers chose to exit markets rather than comply. And because targets increasingly share cloud infrastructure and IP addresses, blocking one site can sweep in thousands of unrelated ones.⁴¹ Reported European experience bears this out—Italy's "Piracy Shield" has inadvertently blocked major cloud and productivity services, and Spain has over-blocked content-delivery networks.⁴² The second concern is efficacy: a French ARCOM/IFOP study found that roughly 98% of alt-DNS users who hit a block simply turned to other routes, such as VPNs. The third concern is abuse: critics warn that any system empowering private parties to cut off access to a website invites misuse—pointing to documented misuse of DMCA notice-and-takedown to suppress disfavored speech, and to the difficulty of policing "foreign" and "piratical" designations where anonymously operated or whistleblower sites could be swept in.⁴³

In particular, the constitutional dimension deserves dedicated attention. Site blocking implicates the First Amendment because it restricts Americans' access to information at the infrastructure level; any framework will be measured against the requirement that restrictions on lawful speech be narrowly tailored, that they not burden substantially more speech than necessary, and that they rest on adequate procedural safeguards. A regime that reliably swept in lawful or mixed-use content, or that lacked a meaningful pre-deprivation process, would face a steep constitutional climb.

C. Guardrails

If Congress elects to evaluate a foreign site-blocking mechanism, SIIA respectfully submits four structural criteria as non-negotiable. We note that many of the proposals

⁴⁰ Meredith Filak Rose, [Oh Look, a New Censorship Tool](#), Public Knowledge (June 13, 2025). Public Knowledge argues that blocking at the level of "alt-DNS" resolvers risks global over-blocking and is readily evaded, citing a French ARCOM/IFOP study finding that roughly 98% of alt-DNS users met with a block sought another route.

⁴¹ [DNS at Risk: How Network Blocking and Fragmentation Undermine the Global Internet](#), Internet Infrastructure Coalition (May 2025); Electronic Frontier Foundation, [Site-Blocking Legislation Is Back, It's Still a Terrible Idea \(Apr. 3, 2025\)](#) (warning of collateral over-blocking where targets share cloud infrastructure or IP addresses).

⁴² Reported European experience includes Italy's "Piracy Shield" inadvertently blocking Cloudflare and Google Drive services, and similar over-blocking in Spain. See Public Knowledge, *supra* note 40.

⁴³ Public Knowledge, *supra* note 40.

have made serious attempts to satisfy several of them, and the Congressional focus on a judicial-based process is a positive step.⁴⁴

1. Mandatory, robust judicial process before any blocking order issues, with clear evidentiary standards and meaningful adversarial testing rather than rubber-stamped ex parte petitions.
2. Narrow technical targeting that prevents over-blocking of legitimate or mixed-use infrastructure, with explicit protection for shared hosting, content delivery networks⁴⁵ and lawful content.
3. Strict safe harbors that protect intermediaries acting in good faith to comply, including immunity from collateral liability for compliance.
4. No government-mandated single technical architecture and no deep-packet-inspection or encryption-defeating mandates, which would impose disproportionate costs and create security and privacy risks.

Meaningful penalties for bad-faith petitions, and a workable way for affected parties to challenge an erroneous order, would further protect the system against the abuse that critics rightly fear. We take no position today on whether any particular bill clears these bars or whether these bars are enough to address the downsides of judicial site blocking.

IV. CONCLUSION

SIIA's position across both topics is consistent and, we hope, useful precisely because our members sit on both sides of these questions. On digital replicas, we favor a predictable, uniform federal market standard over state-level fragmentation—and we believe the four targeted corrections we have described are necessary to make the NO FAKES Act actually achieve the uniformity and protection its sponsors promise. Regarding site blocking, we favor a careful, evidence-based process that takes the harms of offshore piracy seriously while holding any remedy to rigorous judicial, technical, and constitutional guardrails.

Underlying both is the same conviction we brought to this Subcommittee in 2024: that the most durable solutions are targeted to the specific harm, respectful of free expression, and grounded in the interstate nature of the digital economy. For AI more

⁴⁴ The ACPA, FADPA and BEARD are intended to require a U.S. court order, to target only large-scale foreign-run piracy sites (not mixed-use platforms), and to require courts to verify that an order does not interfere with access to lawful material.

⁴⁵ A content delivery network is a geographically distributed network of servers designed to speed up the delivery of internet content—such as web pages, images, and videos—by bringing the data physically closer to the users requesting it.

broadly, that means a strong, federally-led approach that replaces a conflicting state patchwork with a single, clear standard, while preserving the states' authority in their traditional areas.⁴⁶ A national market deserves national rules. We thank the Subcommittee for its attention to these issues, and we stand ready to work with Members and staff—including by providing amendments—to get the details right.

Thank you again for the opportunity to testify today, and I welcome your questions.

⁴⁶ SIIA Federal AI Legislative Roadmap, *supra* note 12.

Mr. ISSA. Thank you. Dr. Viswanathan.

STATEMENT OF BHAMATI VISWANATHAN

Ms. VISWANATHAN. Chair Issa, Ranking Member Johnson, Ranking Member Raskin, thank you—pardon me, it is catching.

Thank you so much for having me. My name is Bhamati Viswanathan. I teach at Suffolk Law School where I teach copyright law, constitutional law, contracts, and Artificial Intelligence and the Law. Happily, for all of us, I am here today to talk about contracts and copyright, both, and not constitutional law.

I want to frame this with three thoughts quickly, and then I am going to move onto three potential solutions that I see.

The frame is—I am going to take it from the title of this hearing, which struck me—the “Mid-Life Crisis” question. Those of us who sit around thinking about our mid-life sometimes, think of mid-life as both a crisis sometimes, but also an opportunity. It is an opportunity to rethink. It is a very strategic moment for us to think.

Disruption, and since there was no internet 40 years ago, which is how we framed this hearing, begins with opportunity, and it begins with innovation. It also begins with disruption. We are at another moment and another inflection point.

I want to frame this by saying we are not talking about one industry, we are talking about two, two critical industries.

Mr. Issa, you said that America leads the world in high tech. Yes. We also lead the world in arts and entertainment, in culture. A \$2 billion industry for tech. Many people are surprised to hear \$3.3 trillion and more in 2024 was the estimate that was given. Two robust industries. We cannot kill the goose that lays the golden eggs. We need the goose to be alive, and we need the eggs to be gold; right? We need both sides.

Second, we believe in our IP system. We have a strong and robust IP system. It's the pride and joy of our country, and it is in our Constitution. Sorry. I said I wasn't going to talk about con law, and I just did.

We believe in the patent system. The patent system is strong and robust. We need to make sure that the copyright side is strong and robust, too. We can't just throw it off and scrap it at the behest of a few tech companies that say, “oh, we are going to lose the arms race.” There are multiple arms races going on here.

Our arts and culture, no one compares to it. K-pop, Bollywood, and Eurovision? Sorry. Nothing is as great as our export of IT in both areas of technology and culture.

For the new times we need new rights and, importantly, we need new enforcement mechanisms. Let me get to my three solutions that I think are strong on the table, and that we should really consecrate right now as urgent.

First, as you have heard my, my fellow panelists speak about, judicial site blocking. For those of you who don't know what that is, it's a process through which you ask a court to stop an infringing website. You know already that it exists almost exclusively to disseminate infringing material. You are worried about a bad actor here.

There are due process steps in place to say, OK, we need to make sure that is true. Once we've made sure that is true, what can we do?

We can ask a court to say, through a no-fault process, without seeking damages, you need to shut this down because we can't. We can't go after these bad actors.

They are often extraterritorial. We really have no other recourse. Over 50 countries have, have adopted it, as you have heard. The U.S. Copyright Office has written a letter of support to you in Congress about it. It is timely. It is a fair and reasonable, balanced solution.

Second, I am going to talk very quickly about digital replicas because I know you have heard about them a lot. They are a problem. They affect people. Because we are people, we have personal property rights in our identity and in our autonomy.

Let's not forget why this exists. It is rights in ourselves. As Mr. Astin said, "we have human rights." Those rights deserve to be Federalized. They deserve to be made into a Federal property right. This needs to be made something that occurs across the country.

We can carve out First Amendment concerns. We can carve out the scope of it, but it is something that needs to be addressed now.

Third, perhaps nearest and dearest to my heart, is the question of the treatment of the ingestion of copyrighted materials by large language models (LLMs).

What does that mean? We use this word a lot. We say LLMs train themselves on copyrighted material. Well, they can train, but just like the rest of us who train, they have to pay for the training.

Licensing agreements need to flourish. They are beginning to happen. We need to make sure that creators, creators who create the stuff that we consume, are compensated—small creators, too, not just large intermediaries. We need to do that now.

There's a lot of court cases pending, as Mr. Raskin said, various cases. We also need to make sure that there are licensing and market-based solutions that make it fair for all of us.

Thank you so much for giving me the time to hear.

[The prepared statement of Ms. Viswanathan follows:]

House of Representatives Committee of the Judiciary
Subcommittee on Courts, Intellectual Property, Artificial Intelligence, and the Internet
Hearing: “A Mid-Life Crisis? IP and The Internet After 40”

Professor Bhamati Viswanathan
Visiting Assistant Professor, Suffolk University Law School
Witness Testimony | June 30, 2026

Thank you for permitting me to speak on “A Mid-Life Crisis? IP and the Internet After 40.” My name is Bhamati Viswanathan, and I am a Visiting Assistant Professor at Suffolk University Law School in Boston, MA. I teach various courses in IP, including Copyright, Artificial Intelligence and the Law, Current Issues in IP, and Law and the Visual Arts, as well as Constitutional Law and Contracts Law. I serve on several non-profit boards, including the Copyright Alliance (Academic Advisory Board); News/Media Alliance (Faculty Partner); Copyright Society (Member/former Trustee); Volunteer Lawyers for the Arts (Education Advisor); Institute for Intellectual Property and Social Justice (Advisor); and the American Bar Association (Member/former Chair, Emerging Technologies Section). I speak, write, and advise on a range of matters involving IP, creative economies, and new technologies. I am speaking today on my own behalf, and the views I share here are solely my own.

Framing the issues we face today is a challenge: we are seeing the rapid emergence of innovative new technologies, from the Internet to Artificial Intelligence (AI), that are likely to change our lives in ways that are unimaginably vast. At the same time, we are seeing new pressures being brought to bear on industries that are central to our economic vitality and growth. Among those are creative industries, whose total value was recently estimated at **\$3.369 trillion**, or **12.3%** of the entire U.S. economy.¹ By comparison, the technology sector was estimated at **\$2.0 trillion**.² These two sectors are both pillars of the American economy. But we must recall that both sectors matter: we cannot do without both, or sacrifice the proverbial goose to get the golden eggs.

At the same time, we know that China is developing its technologies at lightning speed. Many argue that China is less “hampered” by regulation, caution, and safety measures than we are. Many argue that we will “lose the arm’s race” if we fetter our technological growth. But we can do better than to foreclose important measures that keep all of our sectors strong, our people safe, and our artists creating. We must proceed freely, but not without caution and, where necessary, regulation. Free markets, private ordering solutions, entrepreneurship, and innovation are paramount. But regulation works best when it solves market failures, protects against bad actors, and protects vulnerable populations. After 40 years of digital transformation, we have implemented successful bipartisan regulations, such as the Digital Millennium Copyright Act

¹ International Intellectual Property Alliance (IIPA) (2024 report).

² Computing Technology Industry Association (CompTIA) (2023 report).

(DMCA). But those regulations have been overtaken by changes in technologies, judicial decisions, and market realities. New course corrections that are responsive to present needs but narrowly tailored are timely and required. I propose three areas for legislative change: judicial site-blocking; clarity surrounding treatment of the ingestion of copyrighted materials to “train” large learning models (LLMs); and regulation of digital replicas.

1. Judicial Site Blocking and Expeditious Removal

The theft of copyrighted works by foreign piracy websites is a well-recognized problem that harms copyright owners and creators, damages creative industries, and constantly threatens to undermine the U.S. economy.³ There is a solution that over 50 developed countries have adopted and implemented: judicial site blocking. Judicial site blocking is a process through which courts issue an order to stop websites or online services that are primarily designed for the purpose of infringing copyright. The U.S. Copyright Office has recognized the importance of judicial site blocking regimes, and has written a letter to Congress in support of wielding judicial site blocking to reduce large-scale online infringement.⁴

Judicial blocking is a process through which a court issues an order to stop websites or online services that are primarily designed or provided for the purpose of infringing copyright from accessing a market when other enforcement mechanisms are ineffective. It is a no-fault process in which blame is not assigned and damages are not sought. Proposed site-blocking legislation includes numerous safeguards to ensure that the due process rights of intermediaries are fully and effectively protected. And judicial site-blocking is narrowly targeted at websites and online services that have no legitimate noninfringing uses.

In its recent *Sony v. Cox* decision,⁵ the U.S. Supreme Court held that a service provider cannot be held liable for infringing acts even if it is aware that those acts are infringing; it has to engage actively in encouraging or promoting the infringement. This standard makes it challenging for copyright owners to successfully pursue intermediaries that exist to foster infringing activities; and the challenge may be compounded by extraterritoriality concerns and jurisdictional constraints. Judicial site blocking offers a reasonable way to balance the interests of copyright owners, service providers, and other stakeholders. It gives copyright holders a swift, effective, and judicious avenue for going after bad actors and shutting down their illicit activities.

³ Michael D. Smith, *What the Online Piracy Data Tells Us About Copyright Policymaking*, Hudson Institute (April 12, 2023), <https://www.hudson.org/intellectual-property/what-online-piracy-data-tells-us-about-copyrightpolicymaking>.

⁴ Letter from Register of Copyrights to the Senate Subcommittee on Intellectual Property (Oct. 28, 2023).

⁵ *Cox Communications, Inc. v. Sony Music Entertainment*, No. 24-171 (U.S. Mar. 25, 2026).

2. Treatment of Ingestion of Copyrighted Materials for “Training” Large-Language Models

Artificial intelligence large-language models (LLMs) ingest vast amounts of copyright-protected works, most often obtained by trawling the Internet. The works are used to build the models’ capacity for complex feedback to users. While “training” is the analogy that’s typically used to describe the process, it is more accurately reproduction, disambiguation of data, and building pattern recognition that occur. Unlike human training, it is not really “education” – i.e., learning with the purpose of become knowledgeable and developing critical skill – rather, the LLMs’ end goal is the accumulation of information and the ability to offer users certain cognitive tools.

Moreover, unlike human training, the technology companies building LLMs do not access copyrighted materials by buying, borrowing, licensing, or otherwise licitly obtaining them. Rather, they simply take the works by scraping them off the Internet. No purchase prices, licensing fees, or royalties exchange hands. No copyright creators are compensated. Not even permission is sought or obtained.

For copyright owners, this is catastrophic: it means that they don’t get paid for their hard work and for the risk they took in undertaking the work in the first place. For creative ecosystems, it is likewise a disaster: it completely undermines the business model on which creative industries are predicated. For the copyright system as a whole, it entirely subverts the incentive to create that is the heart of the Intellectual Property Clause in the U.S. Constitution.⁶

AI companies argue that this is “fair use,” meaning that while they are engaged in wholesale infringement, the purpose of their use is so transformative and so socially beneficial, that the end justifies the means. They also argue that their practices do not undermine the “actual or potential” markets for copyright owners. Both elements must be true for a fair use defense to stand; but neither are established in practice or at law. The purpose may be “transformative” – they change the works they use into data in their models – but it is not clearly a transformation in the legal sense as intended by the Copyright Act – a “change of expressive use for a new and different meaning.”⁷ Further, the practice *does* undermine copyright owners’ actual and/or potential markets in licensing their works for training use.⁸ Copyright owners are usually eager to license their works, but they are precluded from doing so when their works have been appropriated and they are left without a choice.

Technology companies and their advocates argue that it is too costly to license materials for training, due to the sheer volume of works required for ingestion. Yet creative content companies that engage in large, complex media productions regularly engage in cross-licensing works, irrespective of expense: the production of movies, for instance, often entails clearing rights and paying royalties for embedding songs, clips, quotes, and other works. The fact that the scale is

⁶ See U.S. Constitution, Art. 1, Section 8, clause 8.

⁷ See, for e.g., *Andy Warhol Foundation for the Visual Arts, Inc. v. Goldsmith*, 598 U.S. 508, 528-30 (2023).

⁸ In fact, several copyright industry companies have begun to enter licensing agreements for training – which shows that there are markets to be had.

different does not mean that the process should be put aside. It means that licensing arrangements will have to be made more creatively and equitably. Moreover, “it’s too expensive” is not a defense that works when regular people want to access or use a copyrighted work. We all pay to consume content, and we understand that paying the toll is necessary to make sure that the people who create the works we use will continue to do so as professional creators. The AI industry should not be an exception to the rule.

AI companies claim that the market will create rights-clearing processes. Thus far, the market has not acted, and copyright industries continue to lose value daily. Absent action or regulation, multiple court cases brought by copyright owners and intermediaries who are seeing their businesses eviscerated by AI proliferate. Legislation by litigation is expensive and cumbersome, and often results in a patchwork of results that are themselves suboptimal. A preferable solution would be a light hand of regulation: incentivizing licensing, and ensuring that markets in copyrighted material can continue to operate effectively and to optimize value.

Copyright industries have been a robust and reliable engine of economic growth. Do we want to see them undermined to the point of no return? That is the threat that AI poses. The ideal solution is private solutions: reform driven by AI companies and content owners coming together at the negotiating table and devising large-scale licensing arrangements. We see glimpses of that already: in the music industry, licensing deals are being struck,⁹ and in the entertainment industry, stakeholders are striking new arrangements for AI use and compensation.¹⁰ We need to spur such arrangements across all sectors so that the rising AI tide will lift *all* boats.

3. Regulation of Digital Replicas

Digital replicas are real, they are proliferating, and they are becoming increasingly sophisticated, to the point of being indistinguishable from real images and real people. Legislation of digital replicas would serve an important and pressing purpose: it would preserve a longstanding right in one’s identity against a radically new technological threat. It is analogous to a right of publicity property right – the major difference is that rights of publicity have typically been protected at the state level, whereas federal protection would be helpful both in standardizing protection and in ensuring that such protection is robust and enduring. Some critics have raised First Amendment concerns regarding potential hampering of free speech on the Internet. Those concerns, however, would be allayed by prohibiting only realistic digital substitution. Legitimate uses of digital replicas would not be affected.

One concern is ensuring that the transferability of the right is narrowly tailored to protect rights but not hamper licit use. The property right in one’s own images, after all, inheres in personal autonomy. It rightfully belongs to the person being replicated digitally. But should that right be

⁹ See, for e.g., <https://www.theverge.com/news/829189/warner-music-group-suno-ai-licensing-deal>.

¹⁰ See, for e.g., <https://www.hollywoodreporter.com/business/business-news/sag-aftra-four-year-deal-studios-new-ai-protections-1236590891/>.

transferable? Why can, or should, it be assigned, licensed, inherited, and/or controlled by one's estate? This question needs to be considered and dealt with thoughtfully.

There are arguments on both sides of the debate. On the one hand, digital replicas can outlast the span of human lives; and one would not want to see a replica used posthumously in ways that do not respect the subject of the image. On the other hand, an endlessly long span of protection seems to risk overpropertization and to incentivize perennial rent-seeking by third-party actors. Just as copyright, patent rights, and rights of publicity have limited terms of duration; so perhaps should digital replica rights be limited in term. Moreover, such rights should be tightly tied to actual consent of the holder. These are important considerations, but they can and will be worked out by well-crafted litigation that both protects personal rights and encourages the licit use of digital replicas.

Mr. ISSA. Thank you, Doctor. We will now proceed under the five-minute rule for questions. By mutual agreement, we will go to the gentleman from Virginia, Mr. Cline, first.

Mr. CLINE. Thank you, Mr. Chair. Thank you for your leadership on this issue. You have given us a historical perspective that dates back many decades. I know many here and watching have been a large part of that history.

As you said in your opening remarks, it is important to remember that history, but also to be cautious in any movement that we take moving forward. Recognizing that the DMCA, notice and takedown, all these things that were put in place 20 years ago, may need updating, but don't need wholesale replacement. We are not going to throw out the baby with the bath water, or the goose that laid the golden eggs, whatever metaphor we want to use.

Mr. Mohr, in *Cox v. Sony*, this spring the Supreme Court held 9-0 that an internet service provider is not contributorily liable for its user's piracy unless it induced the infringement or tailored its service to it, which retired the older knowledge plus material contribution theory.

With that route against intermediates now narrowed, does a no-fault judicial remedy to restrict access to foreign piracy sites become both the cleaner legal tool and the more realistic one, since it turns on blocking rather than on anyone's fault?

Mr. MOHR. Certainly, from the rights' holder side of our constituency that this is exactly how they view the significance of the *Cox* decision.

I will say that for the platforms that we represent, that there the problem, however, of these offshore sites existed well before the *Cox* decision was decided. The folks that are, the folks like *Sci-Hub* or that I mentioned in my testimony, and the other sites that are ripping off the other folks on this panel don't care about *Cox*.

That is really the reason for the, from the copyright owner's side, the push for site blocking orders, because they need a way to get at websites that U.S. courts can't reach. Because if these websites existed in the United States, they would not last long.

Mr. CLINE. You are absolutely right. The Chair led a delegation of Members on a visit to the U.K. and other countries more than year ago and to see firsthand how their site blocking regimes are working. What we saw very clearly was that these remedies can work to reduce traffic on pirate sites and to increase traffic to legitimate sites, while safeguarding speech, due process, and legitimate internet activities, all without imposing undue burden and liability risks on the ISPs that are directed to implement the court orders.

My understanding is that liability concerns on the part of domestic ISPs has been the most significant impediment to advancing legislation in the U.S. I am also told that the proposals offered to date in the House and Senate all include provisions to address that concern. My questions are these:

First, do we now know enough from the experience with the many foreign jurisdictions that have implemented this remedy successfully over the last 15 years that we can confidently move forward with the U.S. legislation and avoid any unintended consequences?

Second, in light of the *Cox* decision is the concern about ISP liability now a moot issue?

Mr. MOHR. I am not sure I understand the second part of that question.

With respect to the first part, as my testimony makes clear, I am not in a position where I can say a bill is good or a bill is bad. What I can say is that a bill that contains the guardrails is one that I believe Congress can advance. Those guardrails I mentioned in the opening by adversarial testing, the targeting is the biggest concern.

Because of the internet architecture, again, from the kind of infrastructure/internet side of our membership, right, the architecture of the internet is designed to efficiently distribute, not necessarily it is not designed to throttle. The risk, then, of over-blocking because of that architecture and liability for over-blocking from the standpoint of those providers, is real.

With respect to the guardrails, if the safe harbor isn't there, if there is no tech mandate, and if the targeting is precise and the process is fair, that is a roadmap for a successful site blocking bill.

Again, the devil's in the details. I am not in a position where I can give you those.

Mr. CLINE. Thank you. I yield back.

Mr. ISSA. The gentleman yields back. We now go to the Ranking Member of the Subcommittee, Mr. Johnson for his five minutes.

Mr. JOHNSON. Thank you, Mr. Chair. Professor Viswanathan, AI systems require massive amounts of data for their training and development. The AI companies are continuing to train on copyrighted material to release better and better models.

Should AI developers be required to disclose the dataset used to train their models?

Ms. VISWANATHAN. Thank you so much for asking me that question, Mr. Johnson.

I want to start by saying we use the word "training," but I am not sure that this is always the right word. They do ingest enormous amounts of material to generate what they generate. When we train, when you and I train, when we learn, when we go use things, we pay for those materials. We license them or we buy them.

I buy a book in the bookstore, I use it in the library which has already paid a licensing fee, I am training in respect, but that is not the same thing that the AI companies are doing. What they are doing is: They are gobbling up huge amounts of material.

Do they need to disclose their datasets? That is one part of it. That in the various cases I have been talking about that Mr. Raskin was just referring to the one where his books were ingested. Right? What happens there? I don't think they ever paid you for those books. You will be paid, you will find that postcard in the settlement, because it is the point is, right, it is not just disclosing what they trained on.

By the way, in *Bartz*, in the *Bartz* case we found they were, in fact, training on pirate sites as well; right? We are learning what they are training on, and it is not good.

They should also be made to realize that you can't just take it. It is not a get-out-of-jail-free card to say, "oh, it is expensive to li-

cense.” They need to license the materials that they are using, as one does.

It needs market-based solutions are the preferred solutions because parties come to them. We can’t—we need to monitor what, in fact, they are doing. I think disclosure is a part of that but not the entire story. It is an important part of it.

Most of all, I think we need to recognize that harm is being done to the markets, the actual and potential markets of copyright holders. That is not what fair use in the copyright fair use term was ever legally or in the spirit meant to have happen; right?

It was not meant to be a, oh, it is beneficial and so you get to use it for free. It is beneficial, but it is also valuable. The value needs to be paid.

Mr. JOHNSON. Thank you. Mr. Floyd, how has the proliferation of internet piracy changed the way that movies are made?

Mr. FLOYD. It has had a direct impact on the number of movies that we make and which movies we make. When we are making a decision as to go forward with a film, we do a profit and loss analysis. We look at the history of the movies in the last few years, and we look and see what kind of revenues have been generated.

As piracy cuts down on the revenues, the legitimate revenues that we are getting, we determine that our next movie is going to make fewer dollars and that impacts maybe our ability to spend a certain amount of money on a movie or make that movie at all.

What you end up with are fewer movies being made, fewer people being employed along the way, and more risk being taken by the studios on the movies that they do go forward on.

Mr. JOHNSON. Thank you. Mr. Astin, you have made a career off your name, image, likeness, and voice, everything we talk about when we examine digital replica legislation.

What about individuals whose names or likenesses are not a commercial business, do you think those individuals need to be protected as well?

Mr. ASTIN. Absolutely. They need it as much, if not more.

There, yes, if you are—I mentioned in my testimony that if you are a teenager somewhere, in your district for example, and for whatever reason, with very little difficulty someone is able to depict you, as you—not you, this imagined teenager—saying they are doing something—

Mr. JOHNSON. I get it.

Mr. ASTIN. You, too. We all, everyone in here.

Mr. JOHNSON. Yes.

Mr. ASTIN. We traffic in our identity and our reputations all the time. Well, so does a 14-year-old kid. Yet, these big platforms benefit financially from when some horrible depiction is done of them. They have no ability to do anything about it.

Yes, they should have their identity protected as a right. Thanks.

Mr. ISSA. Thank you. I yield back.

Mr. ISSA. The gentleman yields back. We now go to the gentleman from Wisconsin, Mr. Fitzgerald.

Mr. FITZGERALD. Thank you, Chair. I just want to go back to February 2024 for a moment because that is when our Committee first began discussing the issue of AI and digital replicas. I see a

lot of familiar faces on the witness stand as well, and in the audience where were also in Los Angeles for that field hearing.

Mr. Mohr, in fact, you testified at that hearing, if I remember correctly. It was also the first time Mr. Astin was there as well, that first time we met.

Mr. Mohr, let me start with you. When you testified in 2024 at that field hearing, you mentioned that there are already a number of State and Federal laws that address many of the concerns with digital replicas. If Congress were to act, and it should act in areas where AI poses a particular risk of harm left unaddressed by current Federal and State laws, so is that still kind of your testimony today, or has anything changed in the past two years since we last debated kind of the issue of AI?

Mr. MOHR. What I would say is that it is true that a number of the harms that occur from the unauthorized use of digital replicas are covered by, in many instances, will be covered by existing State laws and remedies. There is no Federal remedy.

That presents an opportunity for Congress to present a uniform rule and uniform protection which will benefit both the folks who are injured and the businesses that actually have to implement this by a uniform set of rules and a clear standard of what is allowed and what is not allowed.

To do that, there are a number of equities that this body will have to balance.

Our members view the current State of digital replica law as an opportunity to legislate constructively.

Mr. FITZGERALD. Mr. Astin, let me come to you. I remember that we were able to visit in L.A. I know this is kind of general and wide open, but why is the Federal digital replica right, why is it important to you and those that are in the entertainment industry right now? What is prompting people to kind of move in one direction or another?

Mr. ASTIN. Well, every day we have our images, our voices, our faces, and we created fictitiously in ways that people don't, can't tell the difference. It looks like I am saying or doing things. It is happening all the time.

I had one friend, a colleague, I saw a video image of him. He is really upset in this image. He was talking in great detail about some problem that happened.

I called him up and I said, "Hey, man, are you OK?" He goes, "Yes. What are you talking about?" I said, "Well, I saw you were so upset about this thing." He said, "No, I wasn't." I said, "You were sitting in this room and there was a thing behind you." He said, "No, I wasn't." His wife walks in and says, "I can't believe you would fall for that fake."

I am thinking. I went back and looked at it. I opened it up and I couldn't tell the difference between him and this creation.

You know what? It is, "could you please take this down, YouTube? Could you please pull this off your site?"

They need this law to have the instruction that it is OK to take it down.

Mr. FITZGERALD. The process to do that is tedious.

Mr. ASTIN. No. They just have to know it is OK. Let them work out the tech. These guys back here have it worked out pretty good. Right? They have got a system for how to take it down; right? Yes.

Mr. FITZGERALD. Good.

Mr. ASTIN. It is working. They have to know that it is OK, that we have got our First Amendment that we love and we have to protect. The First Amendment is implicated in this NO FAKES Act in both directions.

You have to be able to do satire, tell the news. You have to be able to tell historical things. You have to be able to do all these things.

You also can't rob someone else of their First Amendment right by having it misrepresented as them. It needs to be clarified for these companies where this country stands in Federal law on the nature of intellectual property, individual intellectual property.

Mr. FITZGERALD. Very well said.

Mr. ASTIN. Thank you for asking.

Mr. FITZGERALD. Very well said. I will yield back.

Mr. ISSA. Would the gentleman yield?

Mr. FITZGERALD. I do yield.

Mr. ISSA. I just want to cover one thing. Doctor, you said you are not going to do Constitution. Since you are here, I am going to pinch you a little bit.

Is it true that States under the Constitution don't have international reach? In other words, they, by definition, might be able to pass a law, but to enforce against countries outside the U.S. is completely limited in the Constitution to the Federal Government?

Ms. VISWANATHAN. I invite you to my Con Law class next year and we will talk.

It is still to a certain extent an open question. Yes, what you are saying is essentially true. There is a case called *Vetter* right now that is pending that is asking about international reach of certain copyrights that we have. That case is in the Fifth Circuit. It is—and going up, hopefully.

It is unclear. That one thing that Federalizing laws like the digital replicas law does is it gives us a level of security that we are playing at a national level and that we are not getting into the morass of States' rights versus international rights.

Site blocking, too, this is something that is so agreed on so many countries in the developed world, it is relatively uncontroversial at this point. It is fair to say that. Digital replicas are going to be a problem worldwide.

We can get not just bipartisan support, but international support behind this, which it is a rare opportunity. We should grab it.

Mr. ISSA. Thank you, Doctor. I would tease it up for our constitutional scholar here on the dais, the gentleman, the Ranking Member Mr. Raskin.

Mr. RASKIN. Well, thank you for that, Mr. Chair. I have to get you a copy of some of my books.

Mr. ISSA. I downloaded them already. What are you talking about?

Ms. VISWANATHAN. Not piratable.

Mr. RASKIN. Professor Viswanathan, the Northern District Court in California held in *Bartz v. Anthropic* that the use of copyrighted

works for AI training constitutes fair use. You just voiced your skepticism about thinking that it is training. According to the court, *Anthropic* is permitted to purchase a copy of a book and then use that work to train the model on language, writing, and story.

Do you agree with the court's conclusion? Is that the right analysis?

Ms. VISWANATHAN. That is not constitutional, that is a leading question.

Mr. RASKIN. Yes.

Ms. VISWANATHAN. That the court is, that courts are struggling. They are struggling for the same reason we are. The court said, to be accurate, that it was transformative.

It is still a question about fair use. Well, for those of you who are not copyright people, I am sorry for you but there is still time and I will help you through this. Right?

I say to you, you infringed. You say, well, you are right, I did, but I did it for good reason. It is an affirmative defense. It has four prongs to it. The biggest ones are, did you do something really important, transformative? Did you change it in some meaningful way that makes it important that we preserve that?

The fourth factor is, does it affect the market? I want to point this out: Actual or potential market, right, for the work, for the original work?

The courts are confused and they are concerned, because they see the effect on potential markets. At least the *Bartz* court does; right?

Mr. RASKIN. Right.

Ms. VISWANATHAN. What is the potential market? You could license that work otherwise. Right?

Mr. RASKIN. All right, are there licensing regimes in copyright law that can serve as a model?

Ms. VISWANATHAN. Absolutely there are. There are licensing regimes that exist right now.

You just asked someone a couple of months ago, how are movies made? They license and cross-license all the time. That is how movies get made. When you embed a piece of song into a movie, you license it. You cross-license it. There are regimes that exist. Fair use is not an open and shut case. There are over 100 cases that are pending right now.

Mr. RASKIN. All right. Let me just ask you, are we going to be able to get to the solution within the existing contours of copyright law, or do we need to legislate to address the brave new world we are in?

Ms. VISWANATHAN. It is hard because we are at a moment right now where we want to go with a light hand because we don't want to hamper innovation. We would like to encourage licensing regimes.

The thing I am concerned about, Mr. Raskin, is the small creator who can't go up against the big tech company and say, "Help me here."

There are also, by the way, schemes to help pay small creators. We have BMI and ASCAP standing as examples of collective rights, collective rights organizations that clear rights for people so that

they can get their royalties. What exists right now? There is a lot that exist right now that we need to tap into.

Mr. RASKIN. OK. Thank you. Mr. Astin, I know that digital replicas are a big issue for SAG-AFTRA. You negotiated hundreds of pages of a four-year deal with the Motion Picture Association that would prevent studios from creating fake actors, as I understand it, absent some compelling reason for doing so, or replicating real ones. That seems to be more categorical; you can't do that. To get out of using living, breathing individuals on screen. Could you explain why collective bargaining agreements with provisions like those are necessary?

Then, answer whether they are sufficient to protect creators from individuals using AI to replicate name, image, likeness, voice, intonation, and so on?

Mr. ASTIN. Yes, absolutely. They are absolutely necessary because the relationship between workers and their bosses is often fraught with being taken advantage of. We are very grateful that the companies in the previous cycle when we had our big strike, but in this cycle were willing to work with us to try and figure out how to manage the fairness when it comes to digital replication and what you were talking about with synthetics.

When it comes to digital replication, we are able in bargaining to achieve an understanding about how much we should be compensated.

Mr. RASKIN. Is that sufficient in your field? Does it cover all the people in the workforce?

Mr. ASTIN. Well, our collective bargaining agreement is our labor.

Mr. RASKIN. Yes.

Mr. ASTIN. So, no. Each different union, the writers, the directors, and the IATSE, everybody has to make their own deal.

Mr. RASKIN. Is everybody represented such that they could come up with a similar agreement?

Mr. ASTIN. Everybody has to try to accomplish what we did first, which is to get meaningful artificial intelligence protections language in our bargaining. We are respected.

SAG-AFTRA and our policy writers, our contract negotiating team have really been in the vanguard on this.

To me, for this moment, the important thing is that it is only good for contracts that we are working with people who are signatory to our union. This NO FAKES Act and the digital replication we are talking about exists everywhere else.

That is where nobody other than this body can offer the protections that we required, which is why we really appreciate you all working so hard on the piracy but on this NO FAKES Act.

Mr. RASKIN. Thank you. Mr. Chair, I yield back.

Mr. ISSA. I thank the gentleman. We now go to the gentleman from Texas, Mr. Gooden, for five minutes.

Mr. GOODEN. Thank you. I am impressed with the Ranking Member who can turn a Republican witness into a collective bargaining chat. Not surprised, but impressed. I actually have a question—

Mr. ISSA. You do know that Ronald Reagan once sat in a similar position. It can happen.

Mr. GOODEN. It can happen, yes. No, we are not surprised.

Professor, I was so fascinated with some of the things I have heard. These long, these LLMs, how do they ingest all this material, like these, the books we are talking about, the things you are talking about they should have paid in, so to speak, for? How do they, how do they consume all this information?

Ms. VISWANATHAN. Think of them as the giant Hoover. They suck them up. Where do they get them? They get them, they troll the internet. They get them from various websites. As I said, it has come out in some discovery in some of the cases that they get them from pirate websites as well.

In the *Anthropic* case, interestingly, they bought tons of books and ripped the covers off of them and copied them. It is essentially disambiguating and copying.

Mr. GOODEN. What are you saying—and I am not trying to be combative, I am genuinely into this—what do you say when someone, because you said you and I have to pay for these books before we read them, what would you say if I said, “well, yes, but what if I pay for the book and give it to you?” You are not going to then go write a check to the author, you are just going to read the book I gave you. How is that any different than me just giving a book to an LLM?

Ms. VISWANATHAN. It is not. Who is giving it to them? I don’t give them my book. I wrote a book called “Cultivating Copyright,” and it was uploaded to *ResearchGate*, a pirate website in about three minutes. I know I don’t get a lot of royalties on my book, OK, but that is 200 buck—

Mr. GOODEN. I am sure it was interesting, too.

Ms. VISWANATHAN. Two hundred bucks. No, it wasn’t, but it was 200 bucks. That could have been a couple Starbucks, you know.

That it is a little false to say that they are—it is just like receiving a book. Sure, the first sale doctrine would say that you could receive a book. They are not receiving it. They are trawling the internet, they are finding it, and they are taking it.

They are actually claiming fair use. Again I will just say, fair use means you are saying I infringed. You are not saying, I have the right to this. You are saying, I infringed but I did this for a good reason.

There is an admission there that they are in fact taking stuff that is under copyright.

The whole point of copyright law, y’all, is to make sure that creators get incentivized, but also that they get paid so that they keep doing what they do. Right? We all work because we love what we do, but we also need to put food on the table.

Mr. GOODEN. Do you think there is a solution that they would go for? Do you believe, is it your impression that they are just against any and all, no matter what?

Ms. VISWANATHAN. No, that there have been some licensing agreements, especially in music lessons, things, for example, that have been emerging. I just think they think it is very expensive. They think that in terms of the arms race against China it might grind, put grind, put salt in the gears, and that it might slow things down.

Again, I want to just emphasize that it is two industries here. We can't just talk about the cost to the tech industry; we should talk about the cost to the copyright industries.

Mr. GOODEN. Thank you. I enjoy hearing you. I would love to take one of your classes someday. I yield back.

Mr. ISSA. Would the gentleman yield?

Ms. VISWANATHAN. Always welcome.

Mr. GOODEN. Take my time, sir, please.

Mr. ISSA. I thank you. I want to follow on the question of fair use and so on.

As you see it, Doctor, clearly the right to input, in other words the right to read a book, isn't in controversy. The right to read or to learn from what is on the internet is not in controversy.

The part that I want to ask all our panelists for a moment is, as we look at the absolute right to read, it would seem that we have two questions:

Do you pay for which is copyrighted, similar to the way you would buy a book? That is a fairly straightforward. The cost of your books is on the cover of it, so to speak.

The question, though, that I have for all of you is, once somebody has learned from, should this Committee look to the nature of the output? Because I want to go back to fair use that you cited very accurately—Shaquille O'Neal took my very words and put it in one of his rap songs, literally my voice, not my likeness but my voice.

When I asked him about it one day, he looked down at me and said, "fair use." I have never forgotten that I never followed up after he said it.

The question, though, is should we be looking at output more than input? Meaning, some input is the result of education, meaning it doesn't look like the original input in any way, shape, or form. It is a result of learning. Some have a similarity, and some, as Rudy would say, if you will, is him, his likeness.

Should that be a standard that is not in any of the current legislation, per se, relative to the injurers? I will let you quickly answer.

Ms. VISWANATHAN. Quickly. It is tough.

Mr. ISSA. Each of you.

Ms. VISWANATHAN. It is quickly, it is tough. It is complicated. Law professors' favorite answer: It is complicated. This is why I take exception to the word "training"—when I, as the creator artist, train, I train so that I can learn things, so that I can make something new.

Mr. ISSA. Right.

Ms. VISWANATHAN. Some people use AI, right, and these large language files to create new things. We should encourage that.

I also think we should be restrained in saying you took something in my style. We don't want to start copyrighting style, because style is something that we want to see developed and grow. It is not something that is copyrightable, in fact. I don't think it should be.

Your exact words? Boy. Maybe a short phrase was not copyrightable. If he took a paragraph from your book, that would be less likely to be fair use.

Mr. ISSA. It wasn't my book.

Ms. VISWANATHAN. I know. It was you saying something.

Mr. ISSA. It was me saying, "Protected by Viper. Stand back."

Ms. VISWANATHAN. OK. Well, that is a tough one; right? It was a short phrase.

The point stands, right, we should be able to use short phrases from each other, unless it is a trademark violation, which is another question altogether.

The question about outputs is tough; right? When they are exact copies, we already have copyright to protect against that kind of infringement. It gets squishier and more difficult.

The other question is, as those outputs get more and more created by prompts and less and less created by humans, do we want to copyright that stuff at all?

Well, if there is some human authorship, the Copyright Office has drawn a hard line and said there needs to be an author behind that. That is the right line to draw.

Mr. ISSA. OK. On that note, one answer is going to have to be sufficient. We now go to the gentlelady, my friend, and indulgent to my question, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chair. Mr. Mohr, in your testimony you note that copyright holders currently lack a targeted judicial remedy against foreign pirate sites operating beyond the reach of U.S. courts. The current law isn't effectively reaching many of the worst foreign piracy sites.

That is exactly the gap that the Foreign Anti-Digital Piracy Act is intended to address. The bill is bipartisan and bicameral, and it was crafted really very carefully for more than two years, actually. I engaged with copyright holders, technology experts, service providers, and public interest advocates. After two years of sorting through various issues, it resulted in that bill, commonly known by the unlovely sounding FADPA.

It is grounded in simple principle that Congress can fight online piracy without sacrificing due process, re-expression, privacy, or the open internet.

Now, I have continued working with colleagues, both in the Senate and here, on discussion graphs. We are working and dialoging, trying to find a viable path forward.

I would just like to mention, people have understandably raised the role that I played in SOPA so many years ago. As many of you know, I played a central role in stopping that adoption. That is not because I support piracy. I don't. It was because those proposals raised real risks to the open internet, free expression, and due process.

I am hopeful that we will be able to make progress even in this Congress or, if necessary, in the next in getting something like FADPA adopted.

Professor, your testimony describes judicial site blocking as kind of a no-fault process, no damages, no blame assigned, and no effort to hold providers liable for infringement. Given that, is it fair to say that Congress can provide strong liability protections for service providers that comply with the court order without also codifying broader, secondary liability rules from *Cox*? What do you think of that?

Ms. VISWANATHAN. Yes, if you are asking me whether there are sufficient protections built into judicial site blocking, absolutely there are.

We have been talking about it for a while now and we have seen it implemented in various countries. Yes, I think legitimate, non-infringing uses will still flourish. The question is really the bad actors, the pirate sites that we can't go after. It's whack-a-mole.

Ms. LOFGREN. Yes.

Ms. VISWANATHAN. That is what we are trying to solve.

Ms. LOFGREN. I am interested as we noted, Congress is not usually quick to act. We have discussed the ruling in California, fair use, essentially finding that data for training models is transformative, nonexpressive and, therefore, protected. Reasonable argument can be made on the other side. Meanwhile, we are not doing much here.

Now, I am wondering if anybody can address the technological protections that could be available to individuals? There can be digital watermarking. It is possible to make sites unavailable to, to AI scoping up.

The question is, would Congress by rule or could the Executive by rule, or do we need to by rule enhance that opportunity for people to take technological steps to protect themselves from the Hoovering up of data? Anybody got an idea?

Ms. VISWANATHAN. So far, it has been sort of leaky. There are watermarks and there is encryption and there are, there are ways. There are so many end runs, and that is part of the problem.

One of the things Ms. Lofgren, that we could do is perhaps incentivize companies that are creating technology, possibly by subsidizing them somewhat.

The caution is fair and reasonable. We can't progress quickly. Again, we are concerned about stifling innovation. It is a very reasonable concern. The technological solutions have been—there is a will and, hopefully, where there is a will there is a way. So far, they haven't been perfect. Meanwhile, technology is moving so rapidly.

Ms. LOFGREN. The Copyright Office was working on what is copyrightable. Their ultimate conclusion was you have to have a human author—

Ms. VISWANATHAN. Right.

Ms. LOFGREN. —to have the protection. I agree with that. Here is the rub. If a human author is using AI to create, then they should have protection. Where do you draw the line between it is AI-generated and it is a human using AI as a tool?

Unfortunately, before they reached the end of that process, the President illegally fired the Registrar and then fired the Librarian, and they have not been refilled.

Do you think existing copyright law sufficiently addresses AI's role in creating? Do we need some more revision and guidance from experts in the Copyright Office, Professor?

Mr. ISSA. You can briefly answer that, though, but we are out of time.

Ms. VISWANATHAN. Yes. At the moment, the Copyright Office is holding a fair line. It is basically saying to show us the human back here.

If you can show us what you did, how your project—I tell my students this: Show me your prompts and I better be able to do it by doing those prompts as well. That is copyrightable.

I think that is fair. It shows that the human, in fact, guided the AI. That is going to happen, like with any tool. Whether we can continue to do that or not remains to be seen.

Mr. ISSA. I thank the gentleladies. We go to the gentlelady from Florida, Ms. Lee.

Ms. LEE. Thank you, Mr. Chair. As we hear today, the internet has created extraordinary opportunities for innovation. It has also made it easier to steal intellectual property and exploit identity through AI-generated content. As Congress considers whether our laws have kept pace, we have a responsibility to protect creators, innovators, and everyday Americans while preserving free expression and ensuring that the United States remains the global leader in AI innovation.

All of you for being here today to share your insights and your expertise in helping us strike that balance.

Mr. Floyd, I would like to start with you. You made the point that America should win the AI race, but not at the expense of lowering our intellectual property standards to match those of countries like China. That is exactly the right approach, that we shouldn't have to choose between innovation and protecting American creativity.

As counsel to Amblin Entertainment, you have seen firsthand how much investment, planning, and talent go into bringing a project from script to screen. It is important that we recognize that uncertainty surrounding AI-generated digital replicas affects not just actors but studios, production companies, and the thousands of people whose jobs depend on the success of the creative industries.

How would a clear Federal framework, like the NO FAKES Act, provide the certainty needed to continue investing in American storytelling while preserving our leadership in AI innovation?

Mr. FLOYD. Thank you for that question. It is a good balance. We, as other witnesses have talked about, do need to balance the interests of AI and the interests of our creative industry. The rules do that.

Something like NO FAKES they carve out exceptions for bio pics, news, and documentaries, so we have a legal standard and balance so we know going in what can be used and what can't be used. We spend, a motion picture company will spend anywhere from \$10–\$200 million on a project. That is a huge investment. There are thousands of people who are working on it. On Disclosure they have 4,000 employees.

To spend that kind of money and to hire that amount of people we need to have ground rules to know that our investment is going to be protected along the way. Balancing those with a Federal law would help that.

Ms. LEE. Mr. Astin, you spoke about the impact that AI-generated digital replicas can have on performers, but also that these same technologies are increasingly being used to target everyday Americans as well.

Whether it is an actor whose performance is replicated without consent, or a teacher, a veteran, a small business owner, a teenager

whose voice and likeness is cloned to commit fraud or damage their reputation, the underlying harm is the same: Someone is exploiting another person's identity without permission.

Would you speak to how protecting an individual's voice and likeness should be a right for all those people, but also, what you are hoping to see Congress do to make that a reality?

Mr. ASTIN. Absolutely. Thank you so much for that. It is easy and obvious when you look at performers, if something happens with their reputation, their identity, their likeness, and their voice, the impact of their, to our business is immediate.

Really what is at stake is you want to have some mechanism to stop someone from doing something harmful to you. The way you do that is Congress tells these companies you are not allowed to use a deep fake of some—to me, I don't know if it is because I have three daughters, I picture their—I guess they are getting older now. Sorry, guys. They are 29, 23, and 20. If somebody deep fakes them and there is nothing I can do about it feels so, it is so horrible.

The idea that you guys could pass a law that says I can go to YouTube and say, please take this down. My daughters on their own behalf can say, please take this down. They have a law that says, well, yes, that has been established in the deep fake. That is not your identity. They can take it down.

I just want to live in a world where they just can't abuse people like this. They just can't make you.

It should be an outlier that someone steals your identity, your credit card identity, whatever it should be an outlier that somebody bad, there is a bad actor out there, bad behavior; right?

This is so massively available to everybody to do without, just it is so simple. You just prompt a little bit. Make Sean look like he is doing this, or whatever, and it looks so realistic. Their creativity, their nefariousness can have me doing something, and we are just sitting here, that should not be allowed.

It is just as plain as the nose on your face. It should not be allowed to make somebody do something or say something they didn't do or they didn't say. That goes for every American. It goes for everybody around the world. I would appreciate it if you guys would fix that for us.

Ms. LEE. Mr. Astin, as a policymaker and as a parent, I agree wholeheartedly with that assessment. Thank you for your input. Mr. Chair, I yield back.

Mr. ISSA. I thank the gentlelady. I might have noted that a generation ago, somebody once said, "Where do I go to get my reputation back?" Perhaps that is a lot of what we are talking about with deep fakes.

Mr. ASTIN. You want to hear a Shakespeare one, or it is sort of a paraphrase?

Mr. ISSA. If the gentlelady from North Carolina will indulge.

Mr. ASTIN. I am sorry.

Ms. ROSS. I will indulge if I don't use my time.

Mr. ISSA. Exactly.

Mr. ASTIN. All right.

Mr. ISSA. Please, sir.

Mr. ASTIN. This is a good one. You take away my life, you take that which is bestial, you take away my reputation, and you take the immortal part of my soul. That is a paraphrase, but it sounds good.

Mr. ISSA. OK. You went back further than I could. With that, we go to the gentlelady from North Carolina.

Ms. ROSS. We have gone from the constitutional to the biblical.

Mr. Francis, you haven't got much action. Many of my questions about AI have been taken. I am going to ask you the next question which, by the way, my secretary of State is very interested in because she ends up having to enforce counterfeit laws in North Carolina because there are not enough Federal resources to do it.

By the way, she used to get grants to do that from the Federal Government. About 20 years ago that dried up.

I want to ask you a few questions and then also ask you about who our partners should be in enforcing some of these trademark and copyright counterfeit laws.

You testified that counterfeits in our supply chain pose significant risk to Americans' health and safety. They range from unsafe counterfeit auto parts, dangerous technology knockoffs, poisonous prescription drugs, and toxic personal care products.

What happens when counterfeits steal the goodwill that legitimate companies have spent decades building, and use it to sell products that put customers' health and safety at risk? How would the SHOP Act help with that?

Mr. FRANCIS. Well, I will start with the partnerships. The secretary of State in North Carolina, there are so many task forces at the State and local levels that do tremendous amount of work.

Yes, ma'am, you are right, the Bureau of Justice Assistance grants that were available for almost 25 years have essentially been stopped funding these task forces which have a significant impact on enforcing intellectual property. We would love to see the support of that, bringing these grants back, because we know the consequences without the Bureau of Justice Assistance grants.

Yes, these counterfeit goods remain to be an extreme problem, especially with the health and safety risks to the American consumers. It is very difficult to assess the entirety of the issue.

When we are looking at these marketplaces that have these anonymous foreign sellers that are just selling goods online, there's very few effective ways to take them down from State and local law enforcement.

Something we have seen as a very useful tool, our Schedule A litigation. This allows a rights holder to file a lawsuit and join all these anonymous foreign sellers online in an effort to recover some of the losses to them.

As it relates to the SHOP SAFE act, from a consumer's perspective I can answer it that way. I would, as a consumer, expect to understand where the origin of these products came from. Most consumers believe that there is a continuous monitoring of these sellers online. We would love to have and see continuous vetting of these sellers and where the products came from.

Ms. ROSS. Right. Basically, there has not been effective enforcement, either at the Federal level or now it is pretty much unfunded at the State level. We are leaving it up to State legislatures to de-

cide whether or not they are going to give State law enforcement the tools they need. Is that correct?

Mr. FRANCIS. That is correct.

Ms. ROSS. That is unfortunate. That is something Congress could do; right?

Mr. FRANCIS. Yes. I will speak for the entire IP industry. The grants that are provided to State and locals are incredibly valuable. Today with the priorities of the Federal Government there is no one more important than State level law enforcement that are actually doing the work on the ground each and every day.

Ms. ROSS. Great. Thank you so much. I do want to pick up on something that the Chair asked about the output. Because we have been focusing a lot on the input, and we have had this *Anthropic* lawsuit. I took copyright law when I was in—and I had David Lange at Duke University who taught me copyright law. It was so much fun. We started with Ansel Adams.

I want to talk about the output because I know that the Copyright Office is coming up with rules for what is produced and whether or not there is human content.

Professor, could you tell us a little bit about how we could apply copyright law from derivative works to this? Because it seems to me that if you are actually using something that somebody else had, you should have gotten the license in the first place. It wasn't fair use.

Then, it is considered a derivative work. A derivative work has to have the attribution and all those other things. I am going to ask for indulgence for the answer to that question.

Ms. VISWANATHAN. Great question. Definitely a product of Professor Lange's excellent instruction. It is a good question. Derivative works are works that come from other works; right? As a copyright holder you have rights in your own derivative works. For example, the translation of your book, right, you have that right.

If AI is being used to create a work that is clearly a derivative work, we have the copyright law now. We keep talking about how we want to amend the Copyright Act, now 50 years old. That is fair. There are new things that need to come into play. Let's use the tools we have now. The derivative rights—right is an important part of it. It is an important part of it. It is not the only part of it.

The tough question becomes what if somebody creates something that is close but not the same? We want to encourage that, but we also want to say you can't come too close; right? You can't take where the authorship is. What did I put into that thing that made me the author? Author, by the way, can talk about a musician or anybody else creative.

Copyright law exists and has been enforced for 50 years successfully. We can apply it to this space and the question of derivative works.

Ms. ROSS. Thank you very much. I yield back.

Mr. ISSA. I thank the gentlelady. I now ask for unanimous consent that a letter statement from the Entertainment Software Association be placed in the record.

Additionally, we will be placing in the record the Fifth Circuit decision in *Vetter v. Resnik*, since it has been included so much as a part of this hearing.

Without objection, so ordered. We now go to the gentleman from South Carolina for five minutes.

Mr. FRY. Thank you, Mr. Chair, for having this hearing. Thank you, guys, for being here today. I appreciate your testimony.

Mr. ASTIN, the actors that you represent are generally not the copyright owners in the films and television shows in which they appear. Can you explain how piracy, however, impacts you or the members that you represent? Is the adoption of site blocking in the U.S. important to those members, and why?

Mr. ASTIN. We see our work exhibited in places like on *YouTube* and around the world where they have not made an agreement with the people who hold the copyrights. We are powerless in two directions.

We are powerless to go to those big companies and get them to compensate us according to our contracts. The people we have the contracts with, don't seem to be doing anything about it. That is actually true. Yesterday, a lawsuit was filed and so we are very—we are looking forward to it.

We are on the business end of a lot of this stuff, and we don't have a lot of control. We do the best we can to negotiate the best deals that we can. Then, we hope that the companies we are in business with advocate for the protection of their IP. We really want them to be good at that.

Mr. FRY. Would site blocking be something that you and your members would like to see and appreciate? Would that have an impact for your members?

Mr. ASTIN. Well, just as I said, the ability for our employers who we have our collective bargaining with to successfully impose the law or that copyright, to protect their copyright, if that mechanism, or that tool is going to help them, then we are all for it, absolutely.

Mr. FRY. From a global perspective, It has been testified today that we were a leader, and maybe still are in some aspects, but were a leader in establishing standards for strong IP. We have got some catching up to do. That if we were to do something, create a more robust system to target these offshore criminal actors, could you explain what this would mean for the U.S. generally, and our ability to maintain the status as that global leader in creativity and innovation?

Mr. ASTIN. My colleagues would probably speak to it better than I would. I was pretty moved by what I heard here today about the other 60 countries that are collaborators in other areas and are accomplishing in this space. I would rather hear their experts in that.

Mr. FRY. Mr. Francis, IP House and Digital Citizens Alliance issued a report in April exploring the growing connection between global organized crime and online piracy. What are some of your top line observations of that, to the U.S. economy and also to our citizens?

Mr. FRANCIS. Yes, the joint publication, "Organized Piracy and Crime" just reiterated that. We are seeing a shift toward criminal organization syndicates.

When the profits are very high and the risks are very low we are seeing a significant amount of bad actors organized in many ways. We showed that these are criminal organizations because they have a structure, they have operators, they have supply chains,

they have ways to finance the funds, and they have IT technology significantly impacting the way that these networks need to be looked at. Right?

The United Nations, INTERPOL, Europol all said that these types of behaviors are more toward indicators of organized crime syndicates.

Mr. FRY. How does it affect our citizens, though? How does that translates to the average person in South Carolina, or New York, or California that are not directly involved with these criminal syndicates, or in the film industries, T.V., or whatever? How does it affect normal Americans and citizens?

Mr. FRANCIS. The effect is the malware that they are watching these unpaid or paid subscriptions that are illicit and piracy, that the malware that they are downloading impacts them because there is a significant amount of data that shows that they are also victims of identity theft.

It could also show that there is probably not enough education and awareness around this issue. This report with the Digital Citizens Alliance really highlights the importance of education around this area of digital piracy which has a significant economic impact really across all sectors and around the world.

Mr. FRY. Thank you for that. Mr. Floyd, really quick as we wrap up. What are the online effects or the effects of online piracy on the economics of film and television productions from the industry itself, to the workers, to the legitimate streaming sites, and even our citizens? What are the effects?

Mr. FLOYD. The impact will hit both the company in deciding what movies to make and how often to make them. It will impacts their workers and how many people get hired and paid. It also impacts people like Mr. Astin's group who have already made a movie.

What happens is when someone streams it online and pays for it legitimately, we automatically share a portion of those revenues with the Screen Actors Guild, with the directors, and with all those people who worked on the movie. That gives them a buffer for when they are not working. It is sort of like a mini retirement plan.

If we are not receiving that money, we don't have the money to share. They end up making less money along the way for the work they have already done.

It impacts us and our ability to hire new people. It impacts them and their ability to make a living off the work they have already done.

Mr. FRY. In effect, a lot of starving actors in L.A., but the stereotype is that they are baristas first or bartenders. You are saying that we might actually see a scenario where they are making less as an actor than a barista or a bartender?

Mr. FLOYD. Absolutely. When there are millions of dollars gone and then we are unable to share, they are losing a lot of money.

Mr. FRY. Thank you for that. Mr. Chair, I see my time has expired. I yield back.

Mr. ISSA. I thank the gentleman. We now go to the gentelady from California for five minutes.

Ms. KAMLAGER-DOVE. Thank you, Mr. Chair. I want to start by saying that I am glad that we are finally having a hearing on the issue of IP. From my district's perspective, today is the day when we are actually talking about issues that the American people care about.

We have had 12 hearings in this Subcommittee, and this is the first one on this issue. The videos that were played at the beginning are a testament to the critical nature of this topic. I actually hope we have more hearings, because each of these topics deserve their own hearing.

This is personal to me. My district includes Los Angeles and Culver City. It is home to actors, and musicians, writers, journalists, content creators, video game developers, and everyday Americans. For these and more of my constituents their voice, their image, their likeness, and their performance, that is their livelihood.

AI we know can create opportunities, but it can also be used to profit off humans' identities, their voices, and their likeness.

I am also reminded of a theme in "Anaconda" between these two, Paul Rudd's character and Jack Black's character. Paul Rudd's character says, "Who cares about IP?"

Black's response is, "Literally everyone. That is what big movies are about. That is why we are here."

I am also going to make a plug for my Republican colleagues to join on as a cosponsor to the NO FAKES Act.

The NO FAKES Act includes exclusions for documentaries, news, commentary, satire, parody, and fleeting uses as well as safe harbors for multipurpose creative tools, unless they are primarily designed to produce unauthorized digital replicas.

The video game industry has raised some good faith concerns that because games rely on fictional characters, background characters, and user-created avatars, that the bill could unintentionally capture lawful content or expose developers to claims based on incidental resemblance.

Mr. Floyd, how can Congress make sure that the bill doesn't sweep in fictional characters, incidental likenesses, or legitimate tools that are used in these interactive games?

Mr. FLOYD. Well, as long as there are guidelines in the legislation to help guide where everyone moves forward on it, it would be helpful.

There are under the copyright laws now you could have incidental uses or uses that are similar. It is the substantiality of what goes on. The legislation talks about that, it will help give guidance to everybody as to know.

If there is one background actor that looks similar, maybe that is not enough. If it is an exact, one exact replica wouldn't be too much, but many that are similar might be too much. You have that balancing act with those guidelines.

Ms. KAMLAGER-DOVE. Thank you for that.

This has come up about counterfeiters. Mr. Francis, I know you don't know this about me, but I support the resale marketplace in a very real way. Trusted resale marketplaces are incredibly important.

One problem is that bad actors use online spaces to traffic counterfeit goods. We talked about pharmaceuticals. It really harms

consumers and legitimate businesses. We do need policies to crack down on counterfeiters while clearly distinguishing organized counterfeit trafficking from lawful resale.

Mr. Francis, how do counterfeiters exploit the ambiguity between legitimate resale and sale of infringing goods online? Why is consumer confusion so important to mitigate in this context?

Mr. FRANCIS. Yes, thank you, Congresswoman, it is just deliberate deception. That confusion really is the goal of these counterfeiters. It is very challenging when you are a consumer and trying to distinguish between what is real, what is fake, the listings, the reviews. These are very extremely deliberate. Of course, extremely challenging for a consumer.

Ms. KAMLAGER-DOVE. Uh-huh.

Mr. FRANCIS. Yes, we are very much in favor of the recommerce platforms. It is a growing market. It is one that really needs to pay particular attention what other marketplaces have been dealing with in the sense of they have also been deceived, these marketplaces by this resale market.

Ms. KAMLAGER-DOVE. Uh-huh.

Mr. FRANCIS. Yes, it is very, especially with antiques and luxury brands and other products that I think are growing in this space.

Ms. KAMLAGER-DOVE. Right. Right. Mr. Floyd, in the remaining time I have left, about piracy. How much traffic do pirated websites receive?

Outside of copyrighted content being stolen, what are the harms that consumers face when they enter these sites and are asked to enter personal information to access the content?

Mr. FLOYD. I don't have the exact numbers on the traffic. If I could get it, I will get back to you. It is massive though.

Because when you get on one of these sites you type in watch disclosure there, you think you are going to a regular site and then you end up on one of these pirate sites that has thousands of movies that are available.

What happens, then, is the consumer thinks it is a legitimate site. It looks like *Netflix*. It has thumbnail photographs of everything. It has the list of people who worked on the movie. You think you are on a legitimate site, and you type in your credit card. When you type in your credit card that money is now used for all kinds of nefarious purposes.

Also, there is malware that is on the ads. If you click on one of those you are now impacted that way.

Then, they steal your credit card information. You, as a regular, innocent consumer have now been detrimentally harmed for trying to watch one movie online.

Ms. KAMLAGER-DOVE. Thank you for that. Mr. Chair, I would like to enter it. I ask unanimous consent to enter into the record a statement from the Motion Picture Association before this Subcommittee on this particular hearing topic.

Mr. ISSA. Without objection, so ordered.

Ms. KAMLAGER-DOVE. Thank you so much.

Mr. ISSA. I want to thank the gentlelady for her comments. The 12 hearings we have done, some have been clearly, many have been on IP, but the fact that this one focuses on piracy specifically, I

take note that I, if I had it to do over again, would have done more and I would have done it sooner.

With that, I will recognize myself for my five minutes. Five minutes isn't enough to deal with all the issues we are dealing with. I think that is clear.

I am going to ask all of you to please revise, extend, give us your thoughts. Doctor, we will take it all, even though we couldn't have it all here. I want to focus on a couple of things.

First, it is clear that we have some laws that the courts have found they are unable to use effectively. Mr. Mohr, I am going to ask you a tough one, one that you may not have actually come prepared for.

In the *ClearCorrect* case, the Fed Circuit limited the ITC from enforcing essentially what we have been talking about here. They can't enforce that which comes in from outside the country which is intangible.

I am going to ask you and then the others, as we look to do site blocking and the other enforcements, including and notwithstanding States that try to enforce Federal law or contracts, should we be looking to empower organizations like the ITC, and any other existing body to, in fact, have the ability to deal in this growing thing of intangible or nonphysical property in a way that would allow for a broader enforcement of our laws?

I use that example because it is frustrating. Most of us didn't know until that case that the ITC can tell Customs to seize the fake DVD, but they can't seize the incoming, if you will, fake product. When we talk about site blocking, if the ITC had that authority perhaps they would have already done it.

I will start with you, Mr. Mohr.

Mr. MOHR. You weren't kidding about that being a tough question. What I would say is this: I think when you look at site, I think a couple of things.

First, putting aside the merits of the decision itself, right, if you are looking, my mind would go to what the remedy is. In that sense what would the ITC have to do to stop this? They couldn't issue an order in the abstract. They would have to find someone, an entity, and tell it, OK, you might not be doing this conduct, but you must cease enabling it.

That is, essentially, where site—that is site blocking. Right? The question then becomes for us, the questions would become what the guardrails are and whether they are appropriate.

Mr. ISSA. Absolutely. I am not going to claim that Ways and Means and we wouldn't have a lot to do.

Mr. Francis, I am going to stay on this line because it is the one thing we didn't cover.

The ports of entry into America are Baltimore, Los Angeles, Seattle, et cetera. The port of entry for products that are worth countless billions, literally trillions of dollars, in fact, today is the internet.

Are we to a great extent looking at the customs process coming into the United States of product that has not been paid for, product that is, in fact, counterfeit, are we looking at customs in the broadest sense having to be expanded to include intangible? Should

that be the work of this and the other Committees in the foreseeable future?

Mr. FRANCIS. Yes, Mr. Chair, I do think that nontangible items have been a concern. When I was even the Director of the IPR Center, we didn't really focus our efforts there. I do think that there could be some legislative and enforcement frameworks that could be built around that to ensure that we can do something beyond just the tangible items that we are seizing at the ports of entry.

Mr. ISSA. Quickly, Mr. Floyd, would you say that, in fact, the problem is bigger than today's hearing and bigger than this Committee's jurisdiction if we do that?

Mr. FLOYD. Yes. It is a massive problem. We are very happy that this Committee is working on it, but it will go much beyond this. Yes.

Mr. ISSA. Mr. Astin, you have been a superb witness. I am a fan of your work before you had this job.

You mentioned support for deep fakes. Mr. Mohr and others have shown us some areas where there could be some unintended problems.

Is it your position that if we can find the solutions that meet the goal of deep fakes that, in fact, you would be equally supportive as an organization to that, as long as we can get to it?

Mr. ASTIN. Well, I will do you one better. I have been watching for three years our team and the other incredible coalitions work hard to meet every single one of these potential concerns with openness and creativity. I mentioned *YouTube*. *YouTube* is part of this coalition. OpenAI is part of this coalition.

Is it complex? Yes, it is very, very complex. They know their—as far as I am concerned, the core, the essence of this NO FAKES Act is to protect people's identity. I have actually been reading, learning, and watching some podcasts about all your laws, all these kinds of enterprises. Phew, that is a different lifetime.

This sausage is coming together nice, from my point of view. I feel like the group that is here and the group that you are working with will do it. Of course, SAG-AFTRA stands foursquare behind getting NO FAKES passed into law.

Mr. ISSA. Mr. Mohr, I would like you to be able to close on where you think we can get to the goal of deep fakes and other legislation, and where the challenges remain?

Mr. MOHR. The challenge, when we talk about the challenges, I list four. I am going to focus on two.

The first one is preemption. What we don't want is a situation where the rights are uneven. That leads to uncertainty both for individuals and for the developers of these tools, some of whom are now the subject of State statutes that would purport to create standards for them.

That should be in the domain of digital replicas, a matter of Federal law.

The second thing I would want to mention is that for us the counter-notification piece of this. Which is, I come back to something Mr. Astin said before in that there was a situation where a friend of his had a video and he simply couldn't tell who, whether it was real or not.

There are instances where there will be things that are real and we can't yet tell the difference. In those circumstances, we should take care to ensure that those particular instances of expression remain available as best we can.

Mr. ISSA. Good, succinct. I understand that you have a unanimous consent. The gentleman is recognized.

Mr. JOHNSON. Thank you, Mr. Chair. I ask unanimous consent to enter into the record a letter from the Council for Innovation Promotion supporting the NO FAKES Act, the SHOP SAFE Act, and judicial site blocking legislation.

Mr. ISSA. Without objection, so ordered.

In closing, this is in fact not our last, and not this Committee's last hearing on this subject. Hopefully, though, it will be the last one before some of this legislation begins to move.

I think that, in fact, people you have seen on both sides of this hearing are close. The issues that Mr. Mohr mentioned are of great concern but they do seem to be surmountable. I am going to make one closing statement. Rights of the Chair, if you will.

This legislation is going to, if I have my way, move under my watch. It means that those who have said they are close, they are not opposed to it but they want to, we are going to test that. Which is that enough is known, language is being distributed on what we believe is final compromises to get to legislation.

It is going to be my intention, with the help of my Chair and old friend, Mr. Jordan, that we will move it out of this Committee. I say so today because I think all of you have made the case that allowing this continued damage is simply no longer possible.

I am going to further close by saying just one thing, which is I started in the era of protecting my trademarks. I certainly understood the standard for confusion as to source was all you really had to prove that you had it infringed.

It shocked me many years later—Professor, you know the history of this—but, that we didn't use that standard in the courts. Having said that, if the courts aren't willing to use trademarks for likeness, then we will have to give them authority and the mandate to do so. That will be the goal of this Committee.

The part I have to say at the close is simply that we will have five legislative days, which with our current schedule could give you a lot more than five days, to accept additional statements here, and questions for all of you, and then a reasonable time to respond.

Will all of you agree to take those questions and answer them to the best of your ability.

[Affirmative answers.]

Mr. ISSA. Thank you all. You have been very generous with your time. This Committee, the Subcommittee stands adjourned.

[Whereupon, at 12:35 p.m., the Subcommittee was adjourned.]

All materials submitted for the record by Members of the Subcommittee on Courts, Intellectual Property, and the Internet can be found at: <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=119417>.