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 cliche. 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/bill/119th-congress/senate-bill/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-deterring. 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 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 networks[45] 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 intedned 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.