Questions for the Record
House Judiciary Subcommittee on Courts, IP, AI & the Internet
Hearing: A Midlife Crisis? IP and the Internet After 40 (June 30, 2026)
QFRs from Rep. Darrell Issa (R-CA)

Response of
Steve K. Francis
Executive Chairman
IP House

Q1. Counterfeiting and piracy have been the most persistent global IP challenges of the last three decades or more. What will it take to finally bring the problem under control?

Counterfeiting and piracy persist because the economics reward the infringer: consumer demand, minimal marginal cost, anonymity, and a low risk of real consequence. Bringing the problem under control means changing that risk-reward calculation, and no single tool does that alone. In IP House's experience, three goals can help move the needle.

First is reaching the money rather than just the listing. Financial disruption produces durable deterrence by removing the incentive to infringe and provides an opportunity to trace the proceeds to help identify the infringer. Consolidated federal actions against foreign online anonymous infringers accomplish both in one proceeding. Unfortunately, this once streamlined civil action is facing increasing judicial scrutiny as more rightsholders are looking to use it.

Second is disrupting consumer access to fully infringing foreign sites and services through judicial site-blocking, which nearly 60 countries already use in some form today. This places real friction between American consumers and foreign services built for no purpose other than theft, thus redirecting demand to legitimate sites and services.

Third is sustained and well-resourced public-private partnerships. IP crime spans jurisdictions and no single government or law enforcement agency can reach infringers alone. Combining public and private resources to investigate the full supply chain is what makes it possible to cut infringing goods and content off at the source. Control over IP crime comes from layering detection, financial disruption, supply-chain visibility, and cross-border investigation so they all continually reinforce one another.

Q1a. Approximate volume of counterfeit goods and pirated content consumed globally and domestically.

Precise figures are elusive, but the best available estimates indicate that the volume of IP infringing goods and content is large and, in some key sectors, growing. When talking about trade in physical goods, the most recent OECD–EUIPO study estimates trade in counterfeit and pirated goods reached roughly $467 billion in 2021, or up to 2.3% of total global imports.[1]

Domestically, enforcement data indicates the physical scale of what is being aimed at the American market. In fiscal year 2025, U.S. Customs and Border Protection seized nearly 79 million counterfeit items carrying a manufacturer's suggested retail price (MSRP) of $7.4 billion, up from roughly 32 million items and $5.4 billion in fiscal year 2024.[2] Item counts rose far faster than declared value, implying a seizure mix shifting toward lower-value goods, consistent with the end of the de minimis exemption surfacing shipments that previously entered without inspection. Notably, while China and Hong Kong continue to dominate in terms of counterfeit product origin, their combined share of total seizure quantity fell from 88% in fiscal year 2024 to approximately 67% in fiscal year 2025. Whether that reflects genuine supply reduction from those origins or re-routing and transshipment through third countries is an open question, which we address further in response to Question 4.

Pirated content is measured differently, and unfortunately, less completely. While there is no recent U.S.-specific data, we can turn to the EUIPO's most recent assessment of online copyright infringement which finds piracy consumption in EU nations stabilizing at roughly ten accesses per internet user per month across film, television, music, and publishing, while software piracy live-sports piracy, and IPTV piracy are all growing, though actual consumption through those services remains unknown.[3]

Q1b. What practical solutions, if any, could generate strong bicameral, bipartisan, and stakeholder support?

Several measures show bipartisan and cross-industry momentum:

- **Judicial site-blocking:** We are encouraged by the serious attention this remedy has drawn over the past several years across Congress and among stakeholders. Nearly 60 countries now operate site-blocking regimes through courts or administrative agencies, and the independent evidence is measurable. IP House's review of that evidence found that traffic to blocked infringing sites fell 89 percent in the United Kingdom, 70 percent in Portugal, and 69 percent in Australia following judicial site blocking.[4] The more consequential finding is what happened to lawful consumption. For example, the United Kingdom's orders increased use of legal subscription services by an estimated 7 to 12 percent.

  We also see value in the design of the mechanism itself. It is narrow by construction: it requires a court order and is aimed only at services that exist for no purpose other than theft, which is what keeps the necessary safeguards in place for legitimate intermediaries. It also reaches foreign operators in a way no other U.S. civil remedy can. An operator who ignores notices, rotates domains, and has no U.S. presence to serve can still be cut off from the American audience

[1] OECD/EUIPO, Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges (May 2025).
[2] U.S. Customs and Border Protection, Intellectual Property Rights Seizure Statistics: Fiscal Year 2025 (May 2026).
[3] EUIPO, Online Copyright Infringement in the European Union – Films, Music, Publications, Software and TV, 2017-2023 (November 2024).
[4] IP House, Overseas and Out of Reach (September 2024).

whose traffic funds the operation. This would materially change the enforcement picture for the American innovative economy. The Subcommittee has a genuine evidence base to draw on across global jurisdictions that have benefited, and IP House supports continued development of legislation in this effort.

- **The public-private partnership model:** The most durable IP enforcement results come where government authority is combined with private-sector visibility. Domestically, the National Intellectual Property Rights Coordination Center ("National IPR Center") is the clearest example, bringing more than two dozen federal agencies and international and industry partners into a single referral and deconfliction channel. The same pattern holds abroad. Coordinated actions run with Europol, INTERPOL, and national police services have dismantled infringing networks no single jurisdiction could have reached alone, including investigations that began as IP theft and ended in seizures of drugs, weapons, and more. Sustained resource investment in these channels across the Federal government is comparatively inexpensive and consistently productive to the immense benefit of American consumers and innovators.

  While the National IPR Center has a permanent statutory charter at 19 U.S.C. § 4344, that charter carries no authorization of appropriations, no staffing floor, and no dedicated budget line, so its resourcing turns entirely on annual appropriations to Homeland Security Investigations ("HSI"). Pairing the existing charter with an authorization of appropriations or a distinct program-project-activity would give it a durability it does not presently have. Second, the step that converts a domestic evidentiary package into a foreign case runs through HSI's international operations and the Department of Justice's overseas components rather than through the National IPR Center itself, which coordinates and refers into those channels but does not staff them. Capacity in those overseas channels is what determines how many referrals become cases abroad. One concrete step would be to ensure that DOJ's International Computer Hacking and Intellectual Property ("ICHIP") network is funded for both advisors and agents, and that intellectual property remains an express priority.

- **Consolidated actions against foreign anonymous online sellers:** What is commonly known as Schedule A litigation lets a rights holder bring a single action against a group of foreign anonymous online sellers, obtain identifying information from platforms and payment providers, and restrain proceeds before they move beyond reach. These defendants are not small domestic retailers. They are overseas operators selling infringing listings from online storefronts with false registration details and no U.S. presence to serve. Often these bad actors move operations and money within hours of learning they have been named in a lawsuit. Schedule A has proven highly effective for American rights holders. World Trademark Review recently reported that the practice now accounts for 43.4% of U.S. trademark cases filed in the first half of 2026, against 6.3% in 2017.[5] As courts continue to refine questions of joinder, provisional relief, and service of process, we have observed that treatment in the last year has varied considerably from district to district and courtroom to courtroom, and that unevenness makes the remedy less predictable for

[5] Tim Lince, "US trademark litigation heads for another record as Schedule A share breaks 40%," World Trademark Review, (July 24, 2026).

the rights holders who depend on it. We would encourage the Subcommittee to keep close attention on how the practice is working in the field and to encourage consistent application across courts. Where the Subcommittee could helpfully act is in encouraging the Judicial Conference and its Advisory Committee on Civil Rules to take up the joinder and provisional-relief questions through the Rules Enabling Act process, and in commissioning a Federal Judicial Center or Government Accountability Office review to build the empirical record the debate presently lacks. Predictability here is not a procedural nicety. It determines whether dangerous and infringing goods can be taken off the market quickly and at scale, which is what protects American consumers and the businesses whose livelihoods depend on protected IP.

Q2. Does enforcement against copyright piracy websites and enterprises located outside U.S. jurisdiction pose unique challenges for rights holders?

Yes. Foreign-operated infringing sites and services sit largely beyond the practical reach of U.S. civil and criminal process. They operate anonymously behind rotating domains, storefronts, and payment processors; they have no verifiable U.S. presence to serve or seize; and when one operation is disrupted, it often reappears within days under a new domain. Rights holders confront a jurisdictional wall in which they can document the harm but cannot readily reach the operator, its assets, or the infrastructure abroad. That is precisely why remedies that prioritize disrupting network infrastructure and financial flows are most effective against foreign operators rather than solely relying on takedowns directed at individual URLs or files.

Q2a. Do foreign piracy sites typically respond to DMCA takedown requests?

Generally, no, at least not in any way that lasts. The DMCA's notice-and-takedown system was built for cooperative, U.S.-based intermediaries, and with them it works reasonably well. Sites built for theft are a different matter. They ignore notices outright or remove a link and repost the same file or stream within hours at a new address. For those operators, a takedown notice is a routine cost of doing business rather than a deterrent.

The reasons are structural, and it helps to separate the site operator from the businesses whose services it relies on. The operator's revenue depends on the infringing content staying up, so it has every incentive not to comply. It conceals its identity behind privacy services and false registration details, selects hosts that advertise their resistance to copyright notices, and moves between hosts and domains as soon as enforcement lands. Many such operators do not regard themselves as subject to U.S. law at all and often operate from places where local enforcement is impractical.

Compliance is far stronger among the legitimate intermediaries around them: hosting providers, content delivery networks, search engines, and social platforms that maintain U.S. operations, seek safe-harbor protection, or run formal copyright-reporting programs. What does not predict compliance is where a provider is based. Two providers in the same country routinely respond in opposite ways. Business model and exposure to U.S. law matter more than location.

Removing a URL is not the same as disrupting a site, and a site going dark after an escalation is not the same as a site being gone entirely. In both cases the content usually resurfaces at a new address by the same operator within days. Search-engine delisting and demotion makes infringing pages harder to find in the United States, which has value that has been documented, but leaves the site itself untouched. Figures built on URL removals or delisting rates alone therefore measure enforcement activity (i.e., a site's volume of infringing activity and willingness to address that activity), not durable results.

Q2b. What does a typical enforcement action against such a website require?

Enforcement against a foreign infringing site is a layered process rather than a single action that "brings down" a website. It normally proceeds in six stages:

- Detection, validation, and evidence collection: Identify the infringing URLs and the copyrighted works involved; capture supporting evidence including timestamps, screenshots, and details of the material and its URL; and validate that the material is unauthorized and falls within the enforcement authority and instructions the rights holder has provided.

- Notice to the operator or the service directly hosting the material: An appropriate copyright notice to the site operator or to the cyberlocker, user-generated-content platform, or hosting provider holding the content, with delivery, acknowledgement, action, rejection, and any counter-notice tracked.

- Infrastructure analysis following non-compliance: Review of publicly and lawfully available domain-registration, DNS, and infrastructure information to identify the hosting provider, CDN, reverse-proxy provider, and other supporting services.

- Escalation to the relevant intermediaries: Hosting provider, CDN, search engine, advertising provider, payment processor, or other supporting service, according to their respective roles and policies. Each can act only within its own technical or contractual control. A search engine may delist a URL, a hosting provider may disable hosted material or an account, and an advertising or payment provider may restrict the operator's ability to monetize the service.

- Legal or governmental action where notices and escalations are ineffective: Site-wide action generally requires a court order, subpoena, law-enforcement involvement, or proceedings in the jurisdiction connected to the operator or the infrastructure. A private enforcement company cannot independently seize, suspend, or permanently disable a third-party website.

- Post-action verification and continued monitoring: Confirm that the targeted content, URL, account, or service has in fact become unavailable, then monitor for re-uploading, replacement links, infrastructure migration, and successor or mirror domains, escalating again when the infringement reappears.

Because the operator is often unreachable, effective action targets the infrastructure and the money rather than individual listings. The realistic objective is sustained disruption, cutting the service's visibility, traffic, and revenue. Permanent removal is rarely achievable through notices alone, because a determined operator can migrate to replacement infrastructure quickly. That is precisely where court-ordered remedies and law-enforcement partnerships become decisive.

Q3. Has enhanced information sharing under the INFORM Consumers Act improved accountability for illicit sales?

The INFORM Consumers Act was a meaningful step. In principle it raises the cost of the anonymity illicit sellers depend on, and it has changed marketplace onboarding. Whether it has measurably improved accountability, however, is not yet established. In August 2025, the Act's own Senate sponsors publicly called on the FTC to disclose how INFORM had thus far been implemented, noting that at the time no investigations had been carried out.[6] One month later the FTC brought its first case under the Act, a September 2025 settlement with the operator of Temu, the only INFORM-related action taken to date.[7]

Data released in January 2026 by Senator Durbin purports substantial marketplace activity related to the Act: roughly 40,000 high-volume seller accounts suspended, approximately three million other accounts suspended or removed, and some 24 million listings taken down.[8] Those are meaningful numbers and we do not discount them. We would offer one caution in reading them. Account suspension measures platform action, not whether the operator behind the account ceased operating, and in our experience the same operators return under new accounts, on other platforms, or on their own websites. IP House's own vantage point is consistent with that assessment. Notice-and-takedown practice alone does not surface INFORM effects because when a platform confirms a removal, it does not indicate whether the seller or listing came down because of INFORM compliance or on the grounds of IP infringement submitted by a rights holder. We have not observed a significant shift in removal rates or in seller conduct on major marketplaces since the legislation went into effect, and seller accounts have always routinely disappeared and reappeared on platforms, which makes any before-and-after comparison difficult. The framework exists but the enforcement record, and thus the accountability payoff, seems to remain largely unmeasured.

Two developments are worth the Subcommittee's attention, though. We are seeing an increase in sellers registering accounts with false U.S. addresses, including residential properties, an effort to appear compliant rather than to avoid the requirement altogether, which indicates the requirement is being felt by foreign bad actors. We are also seeing a migration toward independent, seller-controlled websites, where there is no platform oversight of the account at all, publication and advertising sit entirely with the seller, and links back to overseas operators are harder to identify. The pattern is displacement rather than reduction: as marketplace onboarding tightens, illicit sellers move venues. That migration also relocates the problem to precisely the environment where marketplace cooperation cannot reach it, and where judicial site-blocking and Schedule A actions are helpful tools. Verification can only work on the

[6] Letters from Sens. Durbin and Cassidy: call on the FTC to disclose how the Act has been implemented (August 20, 2025) and to online marketplaces (August 27, 2025).
[7] FTC Press Release, Online Marketplace Temu to Pay $2 Million Penalty for Alleged INFORM Act Violations (Sept. 5, 2025).
[8] Press Release, U.S. Senate Committee on the Judiciary, "Durbin Releases Data on How His INFORM Consumers Act Has Impacted Online Marketplaces" (January 2026).

information a seller supplies, so when that information is false, or when the seller operates off-platform entirely, identifying who is behind an operation generally requires judicial process, another example of why Schedule A litigation remains a necessary complement to marketplace cooperation.

Q4. Does recent data show the effect of closing the de minimis loophole on the scale of counterfeit and pirated goods sold through e-commerce channels?

The picture is still early but clear. Previously, low-value "de minimis" shipments (duty-free up to $800) were the dominant channel for IP infringing goods into the United States. In fiscal year 2024, 97% of intellectual property seizures within cargo originated as de minimis shipments, amounting to roughly 31 million counterfeit items, and de minimis volume had grown from 134 million shipments in 2015 to more than 1.36 billion in 2024.[9] In 2025 the exemption was suspended: first for China and Hong Kong, then for all countries. Early CBP figures show the reform is surfacing more illicit trade. CBP reported roughly an 82% increase in seizures of unsafe/non-compliant low-value goods (including IP infringing goods) after de minimis ended for China and Hong Kong and has collected over $1 billion in duties on 246 million-plus low-value shipments.[10] One figure within that data deserves the Subcommittee's attention: the combined China and Hong Kong share of total seizure quantity fell from 88% to approximately 67% year over year, even as total volumes rose. We do not yet know whether that reflects genuine supply reduction from those origins or re-routing and transshipment through third countries, and we would treat it as an open question rather than a result. It is, however, precisely the kind of signal that warrants sustained measurement.

Our own monitoring supports that caution. In test purchases and online monitoring of goods offered into the United States, we have not seen the changes one would expect if the suspension had truly squeezed low-value, illicit product flows: item prices have not risen (the average is flat and the median has actually drifted down), delivery reliability has not deteriorated, and listing volumes are essentially unchanged — though those counts measure our own sampling capacity rather than market size and should not be read as the global scale of the trade. The pattern looks more like adaptation of illicit trade under the new rules than contraction in the overall market. However, none of this argues against the reform. A structural change of this kind may take years to show up clearly in the data. What the early evidence suggests is that the market is adapting rather than retreating.

Q5. Any evidence that proceeds from online IP crimes — including by transnational criminal organizations — have funded terror and other adversarial activities?

Yes. The clearest and most current evidence is of convergence with transnational organized crime. Large-scale online IP theft has been shown to take place alongside money laundering, sanctions evasion, drug trafficking, and forced labor, run by networks that are structured and financed like criminal enterprises rather than like single operator infringers of years past. The proceeds do not stay in

[9] The White House, Fact Sheet: Suspending the De Minimis Exemption for Commercial Shipments Globally (July 30, 2025), and Department of Homeland Security, President Trump Ends Unfair "De Minimis" Tariff Exemption (July 31, 2025); House Select Committee on the Chinese Communist Party (March 1, 2024).
[10] U.S. Customs and Border Protection, "CBP collects $1 billion since end of de minimis loophole" (December 2025).

the trade that generated them. They are laundered through shell companies, cryptocurrency, and cash-intensive businesses, and reinvested into other criminal activity.

That is the central finding of our recent joint investigation with the Digital Citizens Alliance, and it is corroborated independently by global law enforcement: Europol and EUIPO have documented that IP crime relies on the same enablers as other serious, organized crime, including money laundering, document fraud, and corruption. Often, the payment channels used to move illicit IP revenue are the same channels used to evade international sanctions, which adds a layer of concern regarding national security in addition to just the economics. According to organizations like INTERPOL, Europol, and UNODC, these larger IP infringing networks meet the criteria for transnational organized crime.[11]

International bodies and published research have documented terrorist organizations drawing revenue from trade in counterfeit and illicit goods.[12] There is also evidence that designated terrorist entities use pirate distribution infrastructure to reach audiences, including audiences in the United States, in circumvention of U.S. restrictions.[13] But that record has limits. Illicit proceeds are often laundered through intermediaries before any destination can be traced, making it difficult to determine the frequency with which IP crime directly funds terror organizations.[14] We would encourage the Subcommittee to press the question with the federal and multilateral agencies equipped to investigate it.

Q6. Should Congress update the laws governing imports, such as Section 337 of the Tariff Act, to include cross-border electronic transmission of IP-infringing content into the United States?

We see considerations for each side. Modern technology and e-commerce have blurred the line between a physical good and a digital transmission. Continuing to omit infringing digital products from Section 337, together with the absence of site-blocking legislation, leaves content innovators without a reliable enforcement remedy. However, extending Section 337 to infringing data raises hard questions of scope, practical enforceability, and overlap with the site-blocking bills now under discussion, which are court-ordered, copyright-specific, and already carry due-process and intermediary safeguards. A digital Section 337 remedy would be an exclusion order enforced at the border, and excluding a data flow means filtering at the network level, essentially the same intermediary and expression questions as site-blocking, but resolved by a trade agency rather than a federal court.

Under the Federal Circuit's 2015 decision *ClearCorrect*, the Commission's authority reaches physical articles but not electronic transmissions, a position that has not since been disturbed by the courts or Congress.[15] Whether to change it is a legislative judgment for the Subcommittee. We defer to

---

[11] Digital Citizens Alliance and IP House, Organized. Piracy. Crime. (April 2026).
[12] UNODC, Education for Justice University Series, Organized Crime, Module 16: Intellectual Property Crime and Terrorism; RAND Corporation, Film Piracy, Organized Crime, and Terrorism (2009).
[13] Digital Citizens Alliance and IP House, Organized. Piracy. Crime. (April 2026), section on terrorist financing and promotion.
[14] Laundering typologies documented in Organized. Piracy. Crime. (April 2026); Europol and EUIPO, Uncovering the Ecosystem of Intellectual Property Crime (October 2024).
[15] ClearCorrect Operating, LLC v. International Trade Commission (Fed. Cir., decided Nov. 10, 2015) (2-1; Newman, J., dissenting)

Congress on the choice of vehicle; our observation is that any update to Section 337 should be considered as complementary to judicial site-blocking rather than an alternative.