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 Co-operation 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

Alarmingly, 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.