



OFFICE *of the* UNITED STATES TRADE REPRESENTATIVE
EXECUTIVE OFFICE OF THE PRESIDENT

2025 Review of Notorious Markets for Counterfeiting and Piracy

Table of Contents

- Overview of the Results of the 2025 Review of Notorious Markets for Counterfeiting and Piracy ... 1
- Issue Focus: The Piracy of Live Sports Broadcasts and Protecting Copyright in the Digital Age 3
- Positive Developments Since the 2024 Notorious Markets List 15
- Results of the 2025 Review of Notorious Markets 20
 - Online Markets..... 21
 - 1337X.....25
 - 1FICHER25
 - AVITO.....26
 - BAIDU WANGPAN26
 - CUEVANA.....26
 - DDOS-GUARD27
 - DHGATE27
 - DOUYIN SHANGCHENG (DOUYIN MALL)28
 - FIRE VIDEO PLAYER29
 - FITGIRL-REPACKS29
 - FLOKINET29
 - GENIPTV30
 - HIANIME30
 - INDIAMART30
 - KRAKENFILES.....31
 - LIBGEN31
 - MAGISTV32
 - MEGACLOUD32
 - MIG FLASH.....33
 - MYFLIXERZ33
 - PINDUODUO.....33
 - PRIVATE LAYER.....34
 - RAPIDGATOR.....34
 - RUTRACKER35

SAVEFROM.....	35
SCI-HUB.....	35
SQUITTER.....	36
STREAMTAPE	37
TAOBAO.....	37
THEPIRATEBAY.....	38
UNKNOWNCHEATS	38
VEGAMOVIES	38
VIRTUAL SYSTEMS, LLC	39
VK	39
WHMCS SMARTERS.....	40
Y2MATE.....	40
YTS.MX.....	40
Physical Markets.....	42
ARGENTINA	43
BRAZIL.....	44
CAMBODIA.....	44
CANADA.....	45
CHINA	45
COLOMBIA.....	48
INDIA	48
INDONESIA	49
KYRGYZ REPUBLIC	50
MALAYSIA	50
MEXICO.....	50
PARAGUAY.....	52
PERU.....	52
PHILIPPINES.....	53
RUSSIA	54
THAILAND.....	55
TÜRKIYE	55
UNITED ARAB EMIRATES.....	56
VIETNAM.....	57
Public Information	58

Overview of the Results of the 2025 Review of Notorious Markets for Counterfeiting and Piracy

Commercial-scale copyright piracy and trademark counterfeiting¹ cause significant financial losses for U.S. right holders and legitimate businesses, undermine critical U.S. comparative advantages in innovation and creativity to the detriment of American workers, and pose significant risks to consumer health and safety. The 2025 Review of Notorious Markets for Counterfeiting and Piracy (Notorious Markets List or NML) highlights prominent and illustrative examples of online and physical markets that reportedly engage in, facilitate, turn a blind eye to, or benefit from substantial piracy or counterfeiting. A goal of the NML is to motivate appropriate action by the private sector and governments to reduce piracy and counterfeiting.

The NML includes an Issue Focus section. For 2025, the Issue Focus examines copyright piracy of sports broadcasts.

The NML also includes Positive Developments, Online Markets, and Physical Markets sections. The Positive Developments section identifies actions that governments and private entities have taken this past year to reduce piracy and counterfeiting. The Online Markets and Physical Markets sections highlight markets that require further actions.

The Office of the United States Trade Representative (USTR) highlights certain online and physical markets because they exemplify global counterfeiting and piracy concerns and because the scale of infringing activity in these markets can cause significant harm to U.S. intellectual property (IP) owners, workers, consumers, and the economy. Some of the identified markets reportedly host a combination of legitimate and unauthorized activities. Others openly or reportedly exist solely to engage in or facilitate unauthorized activity.

This year's NML includes several previously identified markets because owners, operators, and governments failed to address the stated concerns. Other previously identified

¹The terms "copyright piracy" and "trademark counterfeiting" appear below as "piracy" and "counterfeiting," respectively.

markets may not appear in the NML for a variety of reasons, including that the market has closed or its popularity or significance has diminished; enforcement or voluntary action has significantly reduced the prevalence of IP-infringing goods or services; market owners or operators are cooperating with right holders or government authorities to address infringement; or the market is no longer a noteworthy example of its kind. In some cases, physical and online markets in the 2024 NML are not highlighted this year, but improvements are still needed, and the United States may continue to raise concerns related to these markets on a bilateral basis with the relevant countries.

The NML is not an exhaustive account of all physical and online markets worldwide in which IP infringement may take place. The NML does not make findings of legal violations nor does it reflect the U.S. Government's analysis of the general IP protection and enforcement climate in the countries connected with the listed markets. A broader analysis of IP protection and enforcement in particular countries or economies is presented in the annual Special 301 Report published at the end of April each year.

USTR developed the NML under the auspices of the annual Special 301 process² and solicited comments through a Request for Public Comments published in the Federal Register (<https://www.regulations.gov>, Docket Number USTR-2025-0018). The NML is based predominantly on publicly available information. USTR has identified notorious markets in the Special 301 Report since 2006. In 2010, USTR announced that it would begin publishing the NML separately from the annual Special 301 Report, pursuant to an out-of-cycle review. USTR first separately published the NML in February 2011.

²Please refer to the Public Information section for links to information and resources related to Special 301.

Issue Focus: The Piracy of Live Sports Broadcasts and Protecting Copyright in the Digital Age

Each year, the Issue Focus section of the NML highlights an issue related to the facilitation of substantial counterfeiting or piracy. Past issue focus sections highlighted the growing threat of illicit online pharmacies and counterfeit medicines (2024), the potential health and safety risks posed by counterfeit goods to consumers (2023), the adverse impact of online piracy on workers (2022), the adverse impact on workers involved in the manufacture of counterfeit goods (2021), and e-commerce and the role of Internet platforms in facilitating the importation of counterfeit and pirated goods into the United States (2020).

Sports broadcasting represents one of the most economically significant sectors of the global entertainment industry. The worldwide sports broadcast rights market was valued at approximately \$62.6 billion in 2024, continuing a rapid upward trend over the past decade.³ Beyond its economic importance, sports broadcasting serves vital cultural functions, bringing communities together and providing shared experiences that transcend geographic and social boundaries. Major sporting events like the FIFA World Cup, the Olympic Games, and championship finals for professional leagues attract billions of viewers worldwide, generating enormous commercial value for broadcasters, leagues, teams, and sponsors alike.

The entire professional sports broadcast ecosystem depends fundamentally on copyright and related rights, particularly the rights of reproduction, communication to the public, and distribution that underpin the broadcasting, streaming, and other transmission of live sports broadcasts. These intellectual property protections enable right holders to license exclusive

³Hamilton, Gavin, "Global value of sports media rights tops \$60bn," Sport Business, Global Media Report (November 27, 2024), <https://www.sportbusiness.com/news/global-value-of-sports-media-rights-tops-60bn/>

broadcasting privileges, creating the revenue streams that sustain professional leagues, fund athlete compensation, support grassroots development programs, and finance the production of high-quality broadcasts. Broadcasting revenues have become the dominant financial pillar for most major sports properties. For example, the National Football League’s media rights deals are valued at approximately \$110 billion for the time period from 2023 to 2033 due to key deals with major networks and companies like CBS, ESPN, FOX, NBC, and Amazon, with ESPN intending to pay around \$2.7 billion annually starting in 2026 for Monday Night Football and the Super Bowl.⁴ The English Premier League’s domestic and international broadcast rights for 2022 to 2025 exceeded \$13.2 billion.⁵ The digital streaming of live sports broadcasts continues to bolster the numbers for this industry, with some analyses predicting that by the end of 2025, the number of U.S. viewers who stream a sports event at least once a month will have risen to over 90 million, a steep increase from 57 million in 2021.⁶

However, this industry faces a pervasive and growing threat: the widespread piracy of live sports streams. Unauthorized streaming services, illegal retransmission through social media platforms, and sophisticated illicit Internet Protocol Television (IPTV) operations systematically undermine legitimate markets. These piracy operations siphon revenues from right holders, devalue official broadcasting licenses, and weaken the economic incentives for continued investment in sports production and infrastructure. As streaming technology becomes increasingly accessible and piracy operations grow more sophisticated, the challenge intensifies.

Effective copyright protection and robust enforcement mechanisms are therefore essential to preserving the economic value and competitive integrity of sports broadcasts. Without meaningful deterrence against piracy, the fundamental business model supporting professional sports faces existential threats. This Issue Focus examines the nature and scope of

⁴ Johnson, Michael, “Record NFL revenue continues, with a focus on media opt-outs and global growth,” S&P Global (October 30, 2025), <https://www.spglobal.com/market-intelligence/en/news-insights/research/2025/10/record-nfl-revenue-continues-with-a-focus-on-media-opt-outs-and-global-growth>.

⁵ Poindexter, Owen, “U.S. Deal Vaults Premier League Int’l Rights Over Domestic Rights,” Front Office Sports (February 15, 2022), <https://frontofficesports.com/u-s-deal-vaults-premier-league-intl-rights-over-domestic-rights/>

⁶ PwC, <https://www.pwc.com/us/en/industries/tmt/library/sports-streaming-platforms.html>.

sports broadcast piracy, analyzes its economic and cultural impacts, evaluates current legal frameworks and their limitations, and proposes concrete policy solutions to strengthen intellectual property enforcement in this critical domain.

I. The Nature of Sports Broadcast Piracy

Sports broadcast piracy encompasses any unauthorized reproduction, distribution, or public performance of copyrighted sports content. This includes several distinct but often overlapping forms of infringement. The most common manifestation involves unauthorized live streaming, where individuals or organizations capture legitimate broadcasts and retransmit them through websites, applications, or social media platforms without authorization from right holders. Additionally, piracy occurs through illegal showings in commercial establishments that lack proper licensing, unauthorized embedding of legitimate streams on third-party websites, and increasingly sophisticated illicit IPTV services that offer packages of live sports channels at prices far below legitimate subscription costs.⁷

The technological enablers of sports piracy have proliferated rapidly in recent years. The democratization of streaming technology means that relatively affordable equipment and readily available software allow virtually anyone to capture and retransmit high-quality video streams. Modern unauthorized streams often match or nearly match the quality of legitimate broadcasts, eliminating a traditional deterrent to piracy. The decentralized and fragmented nature of the streaming industry creates additional challenges, as pirated content can be distributed across countless websites, social media accounts, and messaging platforms simultaneously. Social media giants have become inadvertent distribution channels, with users frequently sharing unauthorized streams that reach thousands of viewers before detection and removal.

Televised sports programs face unique vulnerabilities that distinguish them from other forms of copyrighted content. Unlike movies or television series, which retain commercial value for extended periods, sports content derives almost all its economic value from real-time or near-

⁷ European Union Intellectual Property Office, “Online Copyright Infringement in the European Union: Music, Films and TV (2017-2018),” EUIPO Report (2019).

real-time viewing. A soccer match generates minimal viewing interest even hours after its conclusion, let alone days or weeks later. This compressed value window means that piracy inflicts maximum damage. By the time enforcement mechanisms identify and remove unauthorized streams, much or all of the commercial harm has already occurred. The live, time-sensitive nature of sports creates an asymmetry that heavily favors pirate operations over right holders and enforcement authorities.

High-profile examples illustrate the pervasiveness of sports piracy across all major sports properties. The FIFA World Cup is a popular target for massive unauthorized streaming. For example, during the 2018 FIFA World Cup, an audience of about 613,700 illegally watched Brazil play Switzerland, which was the largest number of illicit views for any group match that year.⁸ Major European football leagues also face persistent piracy problems, with matches from the Premier League, La Liga, and other top competitions routinely available through unauthorized channels. Boxing matches, particularly high-profile pay-per-view events, also suffer from rampant illegal streaming. The 2017 fight between Floyd Mayweather and Conor McGregor generated an estimated 239 illegal streams totaling nearly 3 million illicit views during the event.⁹

Right holders have launched extensive anti-piracy campaigns in response. The National Football League employs sophisticated monitoring systems and maintains dedicated legal teams to pursue unauthorized streaming operations. The English Premier League has been particularly aggressive, pursuing legal action against commercial-scale operators. The Spanish soccer league La Liga developed a controversial mobile application that used device microphones to detect unauthorized public screenings of matches, though privacy concerns ultimately forced modification of this approach.¹⁰ These campaigns demonstrate both the seriousness with which

⁸ Lemire, Joe, "More Than 5,000 Pirated World Cup Streams Detected by Irdeto," Sports Business Journal (July 4, 2018), <https://www.sportsbusinessjournal.com/Daily/Issues/2018/07/05/Technology/fifa-world-cup-piracy-streams-irdeto-beoutq/>.

⁹ Dawson, Alan, "An estimated 3 million people illegally streamed the Mayweather-McGregor fight," Business Insider (August 29, 2017), <https://www.businessinsider.com/3-million-people-watched-the-mayweather-v-mcgregor-fight-illegal-stream-box-office-ppv-records-2017-8>.

¹⁰ Jones, Sam, "La Liga fined over app that spied on illegal match screenings," The Guardian (June 12, 2019), <https://www.theguardian.com/football/2019/jun/12/la-liga-fined-over-app-that-spied-on-illegal-bar-screenings-of-matches>.

right holders treat piracy and the difficulty of achieving lasting solutions through enforcement alone.

III. Economic and Cultural Impact

The economic damage inflicted by sports broadcast piracy is substantial and multifaceted. Precise quantification proves challenging due to the clandestine nature of piracy operations and debate over how many pirate viewers would have paid for legitimate access. Nevertheless, industry estimates suggest massive revenue losses. In 2023, the NFL, NBA, and UFC claimed in a joint statement that live piracy causes the global sports industry to lose up to “\$28 billion in additional potential annual revenue.”¹¹ These figures reflect direct losses in the form of reduced subscription revenues, diminished pay-per-view purchases, and devalued advertising inventory. When legitimate viewing audiences shrink due to piracy, the commercial value of advertising during broadcasts correspondingly decreases.

Beyond direct revenue losses, piracy creates ripple effects throughout the sports ecosystem. Leagues and teams depend on broadcasting revenues to fund operations, pay athletes, and invest in facilities and youth development. When transmission rights decline in value due to piracy’s erosion of the viewer base, these downstream funding sources are diminished accordingly. Sponsors face reduced exposure and engagement when viewers shift to pirate streams that often strip out advertising content or provide inferior viewing experiences that diminish brand impact. The compounding effects mean that every dollar lost to piracy potentially reduces spending on event production quality, fan engagement initiatives, grassroots sports development, and player compensation.¹²

The broader market dynamics also suffer harm. Piracy fundamentally undermines fair competition by allowing unauthorized distributors to offer sports content without bearing the costs of acquiring legitimate rights. This creates an impossible competitive situation for legal

¹¹ Comment from UFC, NBA & NFL, U.S. Patent and Trademark Office request for comments in the Federal Register (August 24, 2023), <https://www.regulations.gov/comment/PTO-C-2023-0006-0041>.

¹² Stephen F. Ross and Stefan Szymanski, “Antitrust and Inefficient Joint Ventures: Why Sports Leagues Should Look More Like McDonald’s and Less Like the United Nations,” *Marquette Sports Law Review*, vol. 16, no. 2 (2006): 214-259, <https://scholarship.law.marquette.edu/sportslaw/vol16/iss2/4/>.

broadcasters who have spent billions of dollars in licensing fees for broadcasting rights and high-quality broadcast features such as commentators, analysts, camera technology, and production expertise. When piracy reduces available resources, broadcast quality may suffer, diminishing the viewer experience. Broadcasters considering investments in enhanced production techniques, new viewing technologies like virtual reality or augmented reality experiences, or improved streaming infrastructure face reduced returns on those investments when piracy siphons away potential customers. This stagnation ultimately harms sports fans, who would benefit from continued innovation in how sporting events are produced and delivered.

IV. Legal Framework and Enforcement Challenges

International and domestic legal frameworks in some countries provide some protections against sports broadcast piracy, though enforcement remains deeply challenging. At the international level, the World Intellectual Property Organization (WIPO) has established key treaties protecting the rights of communication to the public (i.e., broadcasting) and making available to the public (i.e., streaming). More broadly, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by the World Trade Organization, requires member states to provide protection for broadcasts and establishes minimum enforcement standards.

National copyright laws typically protect sports broadcasts through multiple overlapping rights. In the United States, copyright law protects the audiovisual work embodied in a sports broadcast, even though the underlying sporting event itself is not copyrightable. The Copyright Act and related laws provides civil remedies and criminal penalties for unauthorized reproduction, public performance, and distribution of protected works, including criminal penalties for piracy-focused streaming services.¹³ The Digital Millennium Copyright Act (DMCA) established notice-and-takedown procedures requiring online service providers to expeditiously remove infringing content upon notification by right holders.¹⁴ Similarly, the European Union's

¹³ 17 U.S.C. § 101 et seq. (Copyright Act of 1976); 18 U.S.C. § 2319C (Protecting Lawful Streaming Act of 2020).

¹⁴ 17 U.S.C. § 512 (Digital Millennium Copyright Act, 1998).

Copyright Directive and individual member state laws protect broadcasting organizations and provide enforcement mechanisms including injunctions and monetary damages.¹⁵

Despite these legal protections, enforcement faces formidable practical challenges. The most fundamental problem stems from the real-time nature of sports broadcasts combined with the speed of digital dissemination. Live pirated streams can reach thousands or millions of viewers within minutes of a match beginning. Even when right holders or enforcement authorities detect unauthorized streams quickly, the notice-and-takedown process typically takes longer than the duration of the sporting event. By the time a pirated stream is removed, the commercial damage has occurred. The match is over, and the time-sensitive value of the content has evaporated. This temporal asymmetry creates a nearly insurmountable structural advantage for pirates over enforcement systems designed for content with longer commercial lifespans.

Cross-border jurisdictional limitations compound these timing challenges. Pirate streaming operations frequently operate from jurisdictions with weak intellectual property enforcement, limited enforcement resources, or lack of political will to pursue copyright violations. A pirate streaming service may be operated from one country, host its servers in another, target viewers in multiple additional countries, and process payments through yet another jurisdiction. Coordinating enforcement across multiple legal systems with varying laws, procedures, and priorities proves extremely difficult and time-consuming. Even successful enforcement actions in one jurisdiction often merely cause operations to relocate to more permissive environments rather than cease entirely.

The technical sophistication of piracy operations themselves creates additional enforcement difficulties. Commercial-scale pirate services increasingly employ encryption, virtual private networks, and routing through anonymous networks to obscure their operations and operators. Tracing the ultimate controllers of large piracy operations can require extensive technical resources and international cooperation. Moreover, piracy-enabling platforms

¹⁵ Directive 2001/29/EC of the European Parliament and of the Council on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society (May 22, 2001).

demonstrate remarkable resilience through rapid adaptation. When authorities shut down a pirate streaming website, operators can simply register new domain names, rebrand under different names, or migrate to alternative hosting providers. This whack-a-mole dynamic frustrates enforcement efforts and requires sustained, resource-intensive campaigns that often exceed the capabilities of right holders and enforcement agencies.

V. Strengthening Intellectual Property Enforcement

Addressing sports broadcast piracy effectively requires a multifaceted approach combining legal remedies, technological innovation, and international cooperation. Enhanced enforcement mechanisms must account for the unique characteristics of live sports content and the sophisticated, adaptive nature of modern piracy operations.

Foreign governments should undertake policy reforms to strengthen protection for sports broadcasts and enable more effective enforcement against piracy operations. The global nature of both sports broadcasting and piracy operations necessitates strengthened international cooperation. WIPO, the World Trade Organization, and regional trade frameworks provide existing foundations for cooperation, but these mechanisms require enhancement. Countries should be encouraged to join and fully implement international intellectual property treaties, particularly those specifically addressing copyright and related rights in the digital environment. For example, the WIPO Copyright Treaty requires signatory countries to provide legal protection against circumventing technological protection measures (TPMs), which are valuable tools for detecting and preventing piracy. TPMs include measures that control access to and use of copyrighted digital content in order to prevent unauthorized copying and sharing, with examples including encryption, password protection, and device limits.

Beyond treaty obligations, practical operational cooperation among enforcement agencies yields concrete results. Cross-border investigations of large-scale piracy operations benefit enormously from coordination, information sharing, and mutual legal assistance among law enforcement agencies in different jurisdictions. Regular multilateral meetings, joint training programs, and established communication channels enable more effective pursuit of piracy operations that span multiple countries. More countries can partner with both government and

private organizations like the U.S. Department of Justice (DOJ) International Computer Hacking and Intellectual Property (ICHIP) program and the Alliance for Creativity and Entertainment (ACE) to shut down piracy sites, as these organizations can provide crucial coordination and resources for international investigations.

International trade agreements increasingly incorporate intellectual property provisions and enforcement commitments. These bilateral and multilateral agreements offer opportunities to secure commitments from trading partners to enhance copyright protection and enforcement, including for broadcast signals. For example, USTR has sought commitments from trading partners to ratify or accede to and to fully implement the World Intellectual Property Organization (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty (collectively known as the WIPO Internet Treaties).

Many jurisdictions require legislative updates to address the specific challenges of live broadcast piracy. Governments should enact or strengthen “live signal protection” provisions that recognize the unique nature and value of real-time sports broadcasts. The traditional notice-and-takedown framework, while valuable for addressing static copyrighted content, often proves inadequate for live sports broadcasts. Expedited injunction procedures specifically designed for live events should be incorporated into national legal frameworks. For example, the United States has expedited provisions for copyright protection, primarily through temporary restraining orders (TROs) and preliminary injunctions, which a court can grant to immediately stop infringing activity.

Additionally, current penalty structures in many jurisdictions fail to provide meaningful deterrence, particularly for sophisticated operations generating substantial revenues. Criminal penalties should include meaningful imprisonment terms and fines proportional to the economic harm inflicted or the revenues generated by piracy operations. Civil penalties should similarly be enhanced, with statutory damages provisions that account for the massive scale on which modern streaming piracy occurs. Asset forfeiture provisions allow authorities to seize the profits of piracy operations and the infrastructure used to conduct them, providing both punishment and disruption of illicit enterprises.

Governments must also dedicate adequate resources and develop specialized expertise for intellectual property enforcement. Many countries have established dedicated police units or prosecutorial teams with specific responsibility for IP crimes, including sports broadcast piracy. These specialized units receive training in digital forensics, streaming technologies, international investigations, and the business models of both legitimate broadcasting and piracy operations. Adequate funding for investigations, including resources for technical tools, international coordination, and sustained operations against sophisticated criminal networks, is essential.

Customs and border protection agencies also play an important role, particularly in addressing the importation of devices designed or marketed primarily for accessing pirated streams. Enhanced cooperation between IP enforcement teams and customs authorities can disrupt supply chains for piracy-enabling hardware and identify individuals or organizations involved in commercial piracy operations.

Platforms hosting user-generated content should continually work towards implementing more effective enforcement mechanisms to address piracy occurring through their services. For example, social media platforms and video-sharing websites can proactively deploy automated tools to detect pirated content rather than relying solely on right holder notifications. Moreover, repeat infringer policies should be rigorously enforced, with accounts that repeatedly stream pirated sports content subject to permanent suspension.

Effective implementation of available technologies requires active collaboration between broadcasters and technology firms. Right holders can partner with platforms, Internet service providers, and specialized anti-piracy technology companies to develop integrated systems for real-time detection and removal of infringing streams. Some sports leagues have developed their own monitoring operations, employing teams that actively search for unauthorized streams during events and immediately pursue takedowns. Expanding these capabilities through cooperation with technology companies possessing sophisticated monitoring tools and closer relationships with platforms can enhance effectiveness.

Consumer education about the harms of piracy and the importance of using legitimate services is also critical to solving this problem. Public awareness campaigns, particularly those

highlighting the impact on sports and athletes that audiences care about, can shift cultural norms around piracy and build long-term respect for intellectual property rights. Furthermore, one consumer piracy survey involving 25,000 adults across 30 countries found that despite the high number of consumers around the globe watching pirated video content, almost 50% of them would either fully stop or watch less illegal content after learning the damage that piracy causes the media industry.¹⁶ The fact that nearly half of consumers are willing to change their viewing habits suggests that education and increased public awareness could significantly reduce video piracy.

VII. Conclusion

Sports broadcast piracy represents a significant and growing threat to the economic foundations of professional sports worldwide. The combination of massive economic importance, technological vulnerability, and enforcement challenges creates a complex problem requiring coordinated responses from right holders, technology platforms, and governments. The billions of dollars in revenues that sustain professional leagues, support athlete compensation, and fund sports development depend fundamentally on effective protection of intellectual property rights in broadcasts.

Current legal frameworks, while providing important protections, have not kept pace with the technological realities of modern piracy operations. The live, time-sensitive nature of sports content demands enforcement mechanisms that can operate in real-time and the global nature of piracy operations requires international cooperation for effective enforcement action. Effectively addressing these challenges requires a comprehensive, multifaceted approach. Enhanced legal remedies specifically designed for live content, technological innovations in detection and protection, strengthened international coordination, modernized national legislation, specialized enforcement capacity, and improved consumer education all play

¹⁶ Sports Video Group staff, "Irdeto Releases Results of Largest Consumer Piracy Survey Ever Conducted," Sports Video Group (March 10, 2017), <https://www.sportsvideo.org/2017/03/10/irdeto-releases-results-of-largest-consumer-piracy-survey-ever-conducted/>.

essential roles. No single intervention will suffice; sustained commitment across multiple domains is necessary.

Sports broadcasting serves important cultural and social functions, bringing communities together and providing shared experiences. High-quality sports coverage depends on continued investment, which in turn depends on viable business models protected by effective intellectual property rights. As technology continues to evolve and piracy operations grow more sophisticated, the challenge will intensify without proactive policy responses.

Positive Developments

Since the 2024 Notorious Markets List

Since the release of the 2024 Notorious Markets List, there have been notable efforts to address the widespread availability of counterfeit and pirated goods in some online and physical markets. The United States commends these efforts and encourages governments, right holders, service providers, and the owners and operators of these and other markets, including those newly identified in the 2025 NML, to engage in sustained and meaningful efforts to combat piracy and counterfeiting.¹⁷

Enforcement Activities: Pirated Content

During the past year, several enforcement authorities conducted successful actions against online piracy markets. In July 2025, the U.S. Federal Bureau of Investigation, with assistance from the Dutch Fiscal Information and Investigation Service, seized the domains of multiple online criminal marketplaces, including nsw2u.com, nswdl.com, game-2u.com, bigngame.com, ps4pkg.com, ps4pkg.net, and mgnetu.com. NSW2U, a major global site distributing infringing copies of Nintendo Switch games, was listed in the 2023 and 2024 NML. For more than four years, these websites provided pirated versions of popular video games. Between February 2025 and May 2025, a total of 3.2 million downloads occurred on these sites, resulting in an estimated loss of \$170 million.

In July 2025, Argentine authorities dismantled a network facilitating illegal subscriptions to Magis TV Pro (in part rebranded as Flujo TV), a service providing unauthorized audiovisual content access that received over 10 million annual visits. MagisTV was listed in the 2024 NML. The operation, coordinated by the Cybercrime Unit of the Buenos Aires Provincial Prosecutor's

¹⁷ References to foreign governments' judicial and law enforcement actions to address piracy and counterfeiting provide helpful factual context to the listings in this year's NML but should not necessarily be interpreted as the U.S. government's endorsement of the particular means used therein.

Office, and supported by football division La Liga and the Alliance Against Audiovisual Piracy, involved raids, arrests, and critical evidence seizure across multiple locations.

In Brazil, authorities continued to carry out the anti-piracy Operation 404, conceived in 2019 with support from U.S. government law enforcement to identify and shut down illegal pirate websites. In 2025, the eighth phase of the operation resulted in the suspension of 525 websites and one illegal streaming application and the execution of a total of 44 search and seizure warrants.¹⁸

In February 2025, Torrent Galaxy, one of the most popular BitTorrent streaming sites at the beginning of the year, welcoming millions of users every day, went offline.¹⁹ The shutdown of Torrent Galaxy appears to be related in part to a November 2024 order by a Dutch court blocking the site in the Netherlands, which also led to bans in other countries.

In September 2025, Greek authorities carried out targeted actions to shut down an operation reselling IPTVs, resulting in the arrest of one individual and the referral of 68 end-users for prosecution. This action marks a positive shift in law enforcement's approach to IPTV piracy in Greece and reflects the importance of a new Greek law that provides for thousands of euros in fines for both sellers and users of the piracy-enabling devices.²⁰

Another positive development was the shutdown of the illegal South Korean piracy site TVWiki (formerly known as NoonooTV), believed to be the most popular illegal streaming site in Korea. The operator of the pirate website was arrested by Korean authorities, sentenced to three years in prison, and ordered to forfeit approximately \$510,000 for violating the Korean Copyright Act.

¹⁸ Maxwell, Andy, "Operation 404: 3,000+ Pirate Domains Blocked, USDOJ & USDOC Get to Watch," TorrentFreak (December 2, 2025), <https://torrentfreak.com/operation-404-3000-pirate-domains-blocked-usdoj-usdoc-get-to-watch-251202/>.

¹⁹ Okunyte, Paulina, "TorrentGalaxy's mysterious downtime sparks speculation," Cybernews (February 18, 2025), <https://cybernews.com/news/torrent-galaxy-down/>.

²⁰ Maxwell, Andy, "Greek Cybercrime Unit Shuts Down IPTV Pirates, 68 End Users Face Fines," TorrentFreak (November 26, 2025), <https://torrentfreak.com/cybercrime-unit-shuts-down-iptv-pirates-68-end-users-face-fines-251126/>.

The Motion Picture Association's Alliance for Creativity and Entertainment (ACE) continued its efforts to work with local law enforcement to shut down pirate websites around the world. In one significant development, ACE worked with Egyptian law enforcement to identify and dismantle a network of more than 80 domain names associated with Streameast, one the world's largest unlicensed sports streaming platforms. The service received over 1.6 billion visits in the last year.

Enforcement Activities: Counterfeit Goods

Several countries have increased enforcement efforts in physical marketplaces and coordination with right holders to effectively reduce counterfeit activity. In May 2025, the Argentine Federal Police led 60 simultaneous raids in the La Salada market in Buenos Aires, a popular market and well-known counterfeit distribution center that has been featured in the NML for many years. These operations, part of a multi-year investigation against the owners of La Salada, resulted in 20 arrests and the temporary closure of the market. Inspections of the seized merchandise showed that 70 percent of the goods included counterfeit branding. Argentine officials have also led multiple raids and inspections throughout 2025 in the Barrio Once and Avellaneda Avenue markets, resulting in a number of shop closures and a significant decrease in the number of illegal street vendors.

In Colombia, despite limited enforcement resources, Tax and Customs Police officials conducted raids targeting markets and offsite warehouses. Authorities seized merchandise valued at \$114 million in the first nine months of 2025. This shows a successful trend upwards from 2024, in which enforcement operations led to the seizure of counterfeit merchandise worth \$153 million.

In July 2025, Honduran customs authorities seized over 14,000 pairs of counterfeit sports shoes of well-known brands. The counterfeit footwear that originated in China and was destined for Nicaragua was valued at approximately \$1.8 million.

In 2024, French Customs seized a record-breaking 21.47 million counterfeit articles, valued at \$751.8 million, marking a 5 percent increase from the previous year and continuing a five-year upward trend. The counterfeit items spanned a broad range of categories, with

perfumes and cosmetics accounting for 34.35 percent of the total value, followed by toys, packaging, and clothing. French authorities also reported efforts to increase consumer awareness and disrupt local sales of counterfeit goods, including an operation in March 2025 that resulted in the seizure of approximately 3.5 tons of counterfeit goods and five arrests at the Marche aux Puces de Saint-Ouen in Paris.

The Intellectual Property Office of the Philippines, in coordination with other government agencies under the National Committee on Intellectual Property Rights (NCIPR), reported significant seizures of counterfeit goods and continued efforts to limit the sale of these goods. From January to June 2025, the NCIPR confiscated counterfeit goods worth \$291.85 million. In one notable operation, the Bureau of Customs conducted a coordinated raid that resulted in the seizure of \$1.7 million worth of products, including bags, clothing, and accessories with counterfeit trademarks of well-known luxury brand names.

Studies and Reports

Several studies published this year addressed global trade in counterfeit and pirated goods. Most notably, in May 2025, the OECD released a report titled “Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges.”²¹ The report provides an analysis of global trade in counterfeit and pirated goods, and found that in 2021, global trade in counterfeit goods was valued at approximately \$467 billion, or 2.3% of total global imports.

In November 2025, the European Union Intellectual Property Office (EUIPO) published “Online Advertising on IPR-Infringing Websites and Apps 2024,” a report analyzing how internet websites and mobile apps that provide access to content, goods, or services that infringe intellectual property rights on a commercial scale often use the sale of advertising space as a key source of revenue.²² EUIPO also released a report titled “Influencers and IP,” which investigates the growing and powerful role social media influencers play in shaping attitudes, behaviors, and

²¹ OECD/EUIPO, “Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges, Illicit Trade,” OECD Publishing (May 7, 2025), <https://doi.org/10.1787/94d3b29f-en>.

²² European Union Intellectual Property Office (EUIPO), “Online Advertising on IPR-Infringing Websites and Apps 2024,” EUIPO (November 13, 2025), <https://www.euipo.europa.eu/en/publications/online-advertising-on-ipr-infringing-websites-and-apps-2024>.

consumption patterns. This study analyzes how influencers engage with intellectual property and the extent to which they contribute to or help prevent IP infringement.²³

The United States commends these efforts, appreciates studies being done in this area, and encourages its trading partners to continue their individual and collective efforts to combat counterfeiting and piracy.

²³ European Union Intellectual Property Office (EUIPO), “Influencers and IP,” EUIPO (November 10, 2025), <https://www.euipo.europa.eu/en/publications/influencers-and-ip>.

Results of the

2025 Review of Notorious Markets

The Notorious Markets List identifies prominent and illustrative examples of online and physical markets in which pirated or counterfeit goods and services reportedly are available or that facilitate, turn a blind eye to, or benefit from substantial piracy and counterfeiting. It does not constitute a legal finding of a violation or an analysis of the general IP protection and enforcement environment in any country or economy. The NML is not an exhaustive inventory of all notorious markets around the world. Markets on the NML are drawn from the many nominations received as well as other input, such as from U.S. embassies, in order to highlight prominent examples of both online and physical markets where pirated or counterfeit goods and services reportedly are trafficked to the detriment of legitimate trade in IP-intensive goods and services.

Owners and operators of notorious markets that are willing to address counterfeiting and piracy have many options for doing so. Such owners and operators can, for example, adopt business models that rely on the licensed distribution of legitimate content and can negotiate appropriate licenses with right holders. If an otherwise legitimate business has become a platform for piracy or counterfeiting, the owner or operator can work with right holders and law enforcement officials to help discourage and curtail acts of infringement. Industry groups have developed a variety of best practices that can help combat counterfeiting and piracy.²⁴ In the absence of good faith efforts, responsible government authorities should investigate reports of piracy and counterfeiting in these and similar markets and pursue appropriate action against such markets and their owners and operators. Governments should also ensure that appropriate

²⁴ E.g., International Trademark Association, Addressing the Sale of Counterfeits on the Internet (June 2021), https://www.inta.org/wp-content/uploads/public-files/advocacy/committee-reports/Addressing_the_Sale_of_Counterfeits_on_the_Internet_June_2021_edit.pdf; ICC/BASCAP, Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain (Mar. 2015), <https://2go.iccwbo.org/roles-and-responsibilities-of-intermediaries-fighting-counterfeiting-and-piracy-in-the-supply-chain-2015.html>.

enforcement tools are at the disposal of right holders and government authorities, which may require closing loopholes that permit operators to evade enforcement actions.

Online Markets

The 2025 Notorious Markets List identifies examples of various technologies,²⁵ obfuscation methods, revenue models, and consumer harms associated with infringing activity. USTR bases its selections not on specific types of technologies, but on whether the owners, operators, or users of a nominated market or affiliated network of markets reportedly engage in or facilitate substantial piracy or counterfeiting to the detriment of U.S. creators and companies.

Many of those who submitted public comments this year highlighted the complex ecosystem—including domain name registries and registrars, reverse proxy and other anonymization services, hosting providers, caching services, advertisers and advertisement placement networks, payment processors, social media platforms, search engines, and network management infrastructure—which providers of pirated content abuse. Each component in this ecosystem can play a role in facilitating or reducing piracy, which in 2019 cost the U.S. economy an estimated \$29.2 billion in lost revenue.²⁶

This year, the NML continues to reflect right holders' concerns with the prevalence of cyberlocker sites to facilitate the storage and distribution of pirated content. Cyberlockers act as the hosting and content storage sites for the world's most popular piracy streaming and linking websites. The streaming sites highlighted in this year's NML depend on the storage capabilities of the cyberlockers also listed here. Right holders emphasized that cyberlocker sites typically depend on advertising for revenue and are thus incentivized to drive more traffic to their sites by offering popular copyright-protected content for free. Many sites also offer a tiered revenue

²⁵ For simplicity, the NML uses terminology that links alleged copyright and trademark infringement to specific technologies (e.g., websites). However, the focus of the NML is on the actions of owners, operators, or users that engage in or facilitate infringement using the technologies, not on the underlying technologies themselves.

²⁶ Global Intellectual Property Center, Impacts of Digital Piracy on the U.S. Economy (June 2019), <https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf>.

sharing system to reward the uploaders of their most popular content, further incentivizing content contributors to continue uploading protected works, including pre-release material. Some cyberlocker sites do offer a takedown reporting system but typically do no proactive monitoring to stop the uploading, sharing, and re-sharing of pirated and infringing content. Content reporting often requires right holders to monitor the thousands of streaming and sharing sites that link back to the cyberlocker, with no restrictions to stop content from being re-uploaded after its removal.

This NML also continues to highlight right holders' concerns with "bulletproof" Internet service providers (ISPs) that facilitate piracy. Bulletproof ISPs are characterized by terms of service that often explicitly advertise leniency in allowing their customers to upload and distribute infringing content. Right holders have for several years expressed concerns with bulletproof ISPs, and in 2025, as with previous years, several submissions noted that the reliance of pirate sites on these ISPs made it increasingly difficult for right holders to remove infringing content. This is especially true where ISPs disguise their ownership and locations, and refuse to respond to right holders' communications and takedown requests.

Additionally, the NML this year continues to highlight ongoing concern from right holders about the proliferation of counterfeit sales facilitated by the confluence of e-commerce platforms and social media sites. This trend is now well-established as the popularity of e-commerce has led many sellers to maintain both a physical and online presence, or to shift to online platforms entirely. Right holders state that while certain e-commerce and social commerce (social media sites with integrated e-commerce ecosystems) platforms have taken positive steps to implement anti-counterfeiting policies, many others still lack adequate anti-counterfeiting policies, processes, and tools such as identity verification, effective notice-and-takedown procedures, proactive anti-counterfeiting filters and tools, and strong policies against repeat infringers.

Right holders continued to express concern about fraudulent advertisements and links to fake websites misleading users into unknowingly purchasing counterfeit products through both e-commerce and social commerce platforms. In 2025, as with in previous years, several

submissions highlighted trends that spread through social commerce sites encouraging consumers to seek out counterfeit goods. Right holders noted the increasing popularity of social media influencers who review, promote, and share links to counterfeit luxury products, intentionally driving their viewers to purchase counterfeit goods through pages linked in their social media profiles. Stakeholders have expressed similar concerns about markets such as TikTok Shop and Meta platforms Facebook and Instagram. As with other markets listed in this NML, stakeholders raise concerns with the high volume of counterfeit products available in these marketplaces, fraudulent advertisements and popular influencers promoting counterfeit goods, and ineffective enforcement measures to limit counterfeit sales and deter repeat offenders. USTR is concerned that foreign actors can utilize these popular platforms to cause harm to U.S. right holders and consumers. USTR will continue to monitor and engage with such platforms. E-commerce and social commerce platforms can continue to address these types of concerns by adopting strong and effective IP enforcement policies, increasing transparency and collaboration with right holders to quickly address complaints, and working more closely with law enforcement to identify IP infringement.

However, many e-commerce and social commerce platforms have taken solid steps toward initiating additional anti-counterfeiting practices and adapting to new circumvention techniques used by counterfeiters. Several platforms filed public submissions this year outlining their implementation of new or enhanced anti-counterfeiting tools, including educational campaigns, increased identity verification requirements, and faster and more transparent notice-and-takedown processes. Additionally, several platforms continue to invest in artificial intelligence (AI) and machine learning technologies as a way to scale up and quickly adapt traditional anti-counterfeiting measures such as text and image screening. As e-commerce platforms and industry associations continue to become more transparent and forward-leaning with their anti-counterfeiting practices, an opportunity exists to collaboratively establish industry best practices, create standard counterfeit-related measurements, and find ways to counteract the ever-changing methods of those that manufacture, distribute, and sell counterfeit

goods. Reducing the availability of counterfeit goods online should be viewed as an industry-wide goal.

1337X

Nominated as 1337x.to. Related sites include 1337x.tw. Utilizes reverse proxy services to mask the location of its hosting servers.

The torrent website 1337x provides links to torrent files, which are small files that contain the information necessary to download unlicensed movies, television shows, music, videogames, software, and other copyright-protected files through the BitTorrent protocol. It is reportedly one of the most popular pirate sites in Europe, and had over 40 million visits in August 2025. The site is reportedly hosted in Bulgaria by a provider known to ignore notices of copyright infringement. Variants of the site have been subject to blocking orders in Australia, Austria, Belgium, Denmark, India, Indonesia, Ireland, Italy, Malaysia, Portugal, Singapore, Spain, Sweden, and the United Kingdom.

1FICHIER

Nominated as 1fichier.com. Hosted in France.

This cyberlocker²⁷ is popular in France and reportedly makes premium pirated content, such as unlicensed movies and video games, available to the public. Despite a criminal conviction against the site's publisher and owner and related civil court judgments in French courts, right holders state that the site has failed to come into compliance. The site was also found liable in French civil court for failing to remove or block access to infringing content. Right holders continue to raise concerns about 1fichier's low response rate to notice-and-takedown requests, and one right holder has reported a response rate of 0.38%. The low response rate reportedly not only attracts more unauthorized uploaders but also benefits third-party linking websites that index links to content hosted on 1fichier, since the infringing content typically remains active on the platform for long periods of time.

²⁷The cyberlockers identified in the NML reportedly operate primarily to provide users with access to unauthorized copyright-protected content.

AVITO

Nominated as avito.ru.

Avito is a Russia-based online marketplace reportedly offering a wide variety of counterfeit goods. Right holders note that, despite the platform's general responsiveness in removing listings, there are no effective proactive measures in place. The volume of counterfeits remains high, and repeat infringers can reportedly continue operating easily. Right holders also report an overly burdensome notice-and-takedown process, with the site requiring detailed evidence of infringement to obtain removal.

BAIDU WANGPAN

Nominated as pan.baidu.com. Headquartered in China.

This cloud storage service is operated by Baidu, the largest search-engine provider in China. Users of the service are able to share links to files stored on their accounts with other users, and infringing content is reportedly disseminated widely through social media and other piracy linking sites. Baidu has been the subject of several copyright infringement cases in China brought by other content distributors, but right holders report little change in the site's enforcement measures. Although Baidu has several tools to take down unauthorized content, according to right holders, it reportedly applies procedures for filing complaints unevenly and with insufficient transparency. Additionally, takedown times are reportedly lengthy and, despite continuous filing of complaints by right holders, repeat infringements still occur.

CUEVANA

Nominated as cuevana.biz. Related sites include cuevana3.eu, cuevana3.ch, cuevana.pro, cuevana.si, cuevana4.me, and cuevana3cc.me. Utilizes reverse proxy services to mask the location of its hosting servers.

Cuevana is the most popular unlicensed streaming site group in Spanish-speaking Latin America and one of the most popular worldwide. SimilarWeb recorded over 41 million visits to Cuevana and related sites in August 2025. Cuevana offers Spanish-language content, including more than 19,000 unlicensed television and movie titles. Cuevana websites have been active since at least 2020 and rely on cyberlockers for the underlying content. Cuevana monetizes its

infringing content through advertising services. Cuevana's use of multiple domains has allowed variants of the site to remain operational. Despite successful enforcement efforts in 2023 that enabled right holders to shut down 22 domains linked to Cuevana, mirror sites were able to quickly re-emerge under new domains.

DDOS-GUARD

Nominated as ddos-guard.net.

DDoS-Guard is an entity reportedly based out of Russia that offers various services including "bulletproof" hosting. According to right holders, it does not respond to takedown requests. DDoS-Guard hosts a number of the most notorious cyberlockers and streaming and downloading sites offering pirated content in the world, including several piracy streaming sites named on this list.

DHGATE

Nominated as dhgate.com. Also available as a mobile app. Headquartered in China.

DHgate is a leading business-to-business, cross-border e-commerce platform in China that primarily serves purchasers outside of the country. Some stakeholders have reported a good relationship with the platform and acknowledged DHgate's significant investment in making its pilot IP enforcement program permanent and available for right holders. DHgate described its improvements in its IP protection program, including its ongoing application of AI-based proactive screening tools, its vendor verification process, and its efforts to cooperate with law enforcement authorities, including publishing a law enforcement guide. DHgate has also taken on leadership roles in industry initiatives to combat challenges in anti-counterfeiting efforts, such as hidden links. However, some stakeholders continue to observe that DHgate remains a significant source of counterfeits that remain easily accessible through search results, a lack of transparency about penalties for infringers, and ineffective deterrence against repeat infringers. As DHgate has increased its popularity with consumers, resellers continue to use the platform to purchase counterfeit goods wholesale from China. There have been reports of law

enforcement cases in the United States involving purchases from the platform. Sellers of counterfeit goods reportedly continue to evade detection by using misspelled variations of brand names and digitally blurred logos. Although many stakeholders welcomed DHgate's recent improvements, DHgate should address these concerns on the continued visibility of counterfeits on the platform, methods by which counterfeit sellers have worked around DHgate's proactive detection procedures, seller vetting process, and penalties for repeat infringers.

DOUYIN SHANGCHENG (DOUYIN MALL)

Douyin Shangcheng (Douyin Mall) is a shopping platform under Douyin, the Chinese online platform offering short-form video, live stream, and e-commerce functionalities owned by ByteDance, also the parent company of TikTok's operations outside of the U.S. Stakeholders report that Douyin Mall has featured live-streaming e-commerce content, allowing users on the Douyin Mall interface to view short videos or livestream videos about products, resulting in Douyin Mall becoming an important channel for counterfeit sales. Stakeholders also report that proactive filtering mechanisms are inconsistently applied. In response to these concerns, Douyin emphasized that it maintains multiple reporting portals for right holders to submit complaints, as well as a one-stop "IPPRO" platform for right holders to submit and manage IP infringement reports. Douyin also described how tens of thousands of right holders have registered their information through the IPPRO platform and how it has responded to notice-and-takedown requests with an average processing time of three working days. However, stakeholders have reported that the platform has often failed to act quickly, imposed stringent evidentiary requirements, and delayed store closures, with little practical cooperation from Douyin against the sales of counterfeit goods on the platform. Douyin should address concerns about the prevalence of counterfeits on its platform, including questions about the effectiveness of its proactive screening mechanisms, evidentiary requirements, and its system for processing IP infringement complaints.

FIRE VIDEO PLAYER

Reportedly operated from Türkiye.

Fire Video Player operates as a type of “piracy-as-a-service” site. The site provides software that allows purchasers to source content hosted on local storage or widely available cloud or video sharing services, enabling individuals to set up and manage their own video piracy streaming sites. Right holders report that a number of popular sites for streaming copyright-infringing content use the Fire Video Player service and that the site does nothing to limit its use by illegitimate actors.

FITGIRL-REPACKS

Nominated as fitgirl-repacks.site.

FitGirl-Repacks, often abbreviated to “fitgirl,” is a well-known “repacking” site that provides access to compressed versions of unauthorized and pirated versions of video games. The site is popular because repacking allows users to download the pirated content using minimal bandwidth through file hosting services and BitTorrent. The site reportedly fails to comply with takedown notices for infringing content and has been the subject of blocking orders in Germany, Italy, and Spain.

FLOKINET

“Bulletproof” hosting providers like FlokiNET support infringing websites by refusing to respond to notices of infringing activity and by failing to cooperate with right holders and law enforcement. FlokiNET’s website explicitly allows anonymous hosting of content, stating, “We do not require any personal details or identification. Any valid email address is enough information to be a customer,” and the site is rarely responsive to law enforcement or right holder requests. In fact, FlokiNET hosts many websites associated with copyright infringing activity. According to FlokiNET’s website, it has servers in Romania, Iceland, the Netherlands, and Finland. The site has registered companies in Romania and Iceland, and is reportedly operated from Romania.

GENIPTV

Nominated as geniptv.com and geniptv.net.

GenIPTV is one of the largest IPTV providers in the world, reportedly operating through multiple affiliates to sell subscriptions for access to over 16,000 broadcast and streaming channels as well as a video library of over 100,000 copyright-protected video titles. According to its website, GenIPTV offers not only the “Latest Movies & Series” on multiple supported devices but also live sports and 24/7 online support.

HIANIME

Nominated as hianime.to. Related sites include hianime.nz; hianime.sx; hianime.tv; hianimez.to; and hianimez.is.

HiAnime is reportedly a successor site to the previously popular site Aniwatch, which was listed on the 2023 NML. The Aniwatch site was itself a rebrand of the well-known zoro.to site. In July 2023, right holders and anti-piracy trade associations shut down zoro.to, which was run from Vietnam, and thereafter the site apparently was rebranded as Aniwatch. The site was again rebranded to HiAnime in March 2024. Stakeholders report that the HiAnime site provides pirated versions of popular movies and television, particularly anime. According to SimilarWeb, the site received over 244 million visits in August 2025.

INDIAMART

IndiaMART, a high-volume e-commerce website and mobile app that connects buyers with suppliers, describes itself as the largest online business-to-business (B2B) marketplace in India. Right holders reported that it continues to sell a large volume of counterfeit goods, estimated to make up more than 50% of all products sold, including pharmaceuticals, electronics, and apparel. Right holders have reported no measurable progress over the past year in addressing these concerns. IndiaMART still has no dedicated IP reporting tool for brand owners, is slow to respond to requests for information, and does not facilitate right holders' attempts to remove listings. Right holders remain concerned about the lack of proactive

monitoring for infringing goods and seller vetting. While sellers must accept the market's terms of use, IndiaMART does not certify that sellers have a right to sell what they are selling either by license or by law. IndiaMART continues to disclaim all liability, claiming that it bears no responsibility for the products sold on its site and merely serves as a passive intermediary between buyers and sellers.

KRAKENFILES

Nominated as Krakenfiles.com.

This cyberlocker is a major source of infringing content, particularly pre-release music. Additionally, the site operator reportedly runs an associated forum site with links to KrakenFiles content where users can download pirated music tracks and albums. KrakenFiles' website states that over 19.4 million files have been uploaded. According to SimilarWeb, the site has received over 67 million visits in the past year.

LIBGEN

Nominated as libgen.rs. Related sites include libgen.is, libgen.li, libgen.st, library.lol, libgen.rocks, libgen.gs, annas-archive.org, annas-archive.gs, and other mirror sites. Reportedly operated from Russia.

Libgen, also known as the "Library Genesis Project," hosts a large number of digital copies of books, manuals, journals, and other works, many of which are unauthorized copies of copyright-protected content. According to Libgen, the site hosts 2.4 million non-fiction books, 80 million science magazine articles, 2.2 million fiction books, and 2 million comic strips. Libgen sites are subject to court orders in Belgium, Denmark, France, Germany, Italy, Portugal, Russia, Spain, Sweden, the United Kingdom, and the United States. In 2022, U.S. law enforcement seized hundreds of mirror site domains associated with Libgen. In 2023, a group of major U.S. publishers were granted a default judgement in a copyright infringement suit against the site. Despite these enforcement actions, Libgen and its network of mirror sites remain active.

MAGISTV

Nominated as magistv.net. Related sites include oficialmagistv.com, magistv.digital, magistv.la, magisla.com, magistvoficial.com, and magistv-venezuela.com.

MagisTV is one of the world's most popular IPTV services and operates primarily in Latin America. The service provides unauthorized access to live sports streams, television channels, and on-demand movies and television shows to its customers for a monthly subscription. The service's devices, subscriptions, and applications are distributed through a broad array of resellers and websites. Stakeholders report that, despite its use of infringing content, MagisTV has attempted to establish a legitimate business presence by filing for trademark registration for the company's wordmark in a number of Latin American countries, including Argentina, Ecuador, Mexico, and Uruguay, as well as in the United States under a parent company based in Shenzhen, China. Despite successful enforcement actions against MagisTV in Argentina, Colombia, Ecuador, and Venezuela, the service remains active through new domains, social media advertising, and local device resellers. MagisTV has also re-branded some of its services and applications FlujoTV.

MEGACLOUD

Also known as VidCloud or RapidCloud. Reportedly operated from Vietnam.

The hosting platform MegaCloud, together with VidCloud and RapidCloud, formerly operated under the pirate service 2embed, which was taken down in July 2023 through the coordinated efforts of right holders and anti-piracy trade associations. The MegaCloud network is a pirate content management system that allegedly provides a large library of infringing content obtained by crawling many infringing websites and search engines and scraping infringing content. The network reportedly acts as a backend hosting system delivering infringing video files—including more than 46,000 movies and 16,000 TV series—directly to more than 260 pirate streaming sites around the world, including listed on the NML. According to SimilarWeb, the sites using the MegaCloud network reportedly received over 600 million monthly visitors in July 2025. The network is an example of a “piracy-as-a-service” provider that significantly contributes to the global trade in pirated content by offering services that make it easy for other bad actors to create, operate, and monetize fully functioning piracy operations.

MIG FLASH

Nominated as Migflash.com.

Migflash.com is the official website for a line of piracy-enabling third-party accessories for the Nintendo Switch and Nintendo Switch 2 videogame consoles. These devices, the “MIG Flash Dumper” and “MIG Flash Card,” provide users with unauthorized access to a game’s files by circumventing the technological protection measures which normally limit such access. The MIG Flash Dumper enables the user to extract (or “dump”), copy, and distribute a game’s files, while the MIG Flash Card enables the user to load and play game files which have been dumped and distributed by other users. Unlike much home console-based piracy, these products do not require hardware or software modifications to the game console itself and thus enable extensive piracy of valuable properties, including new releases, with very few barriers to entry.

MYFLIXERZ

Also known as Sflix. Related sites include myflixerz.to, sflix.to, sflix2.to, moviesjoytv.to, and hdtodayz.to. Reportedly operated from Vietnam.

MyFlixerz and its network of related streaming sites are one of the most popular pirate streaming networks in the world. According to SimilarWeb, these sites received more than 622 million visits in August 2025. These sites are hosted through the MegaCloud/VidCloud/RapidCloud network, which is also listed on this year’s NML, and provide direct access to a wide variety of copyrighted movies and television shows. Right holders report that the streaming sites make money through banner and pop-up advertisements as well as redirects to other sites.

PINDUODUO

Nominated as pinduoduo.com. Also available as a mobile app. Headquartered in China.

Pinduoduo, a social commerce app, is one of the largest e-commerce platforms in China. Right holders report that high volumes of counterfeits persist on the platform, with one stakeholder observing that a large majority of products in certain fashion and sport categories

are counterfeits. This year, stakeholders emphasized the inefficient and unwieldy nature of Pinduoduo's IPR Protection Platform. They reported on the onerous process for submitting complaints, including the inability to allow multiple members from brands' enforcement teams to log into the system concurrently, how right holders are limited to submitting only one hyperlink as supporting evidence per copyright infringement complaint, and how complaints are rejected if submitted images do not exactly match infringing listings. As in previous years, stakeholders continue to highlight concerns about Pinduoduo's unwillingness to engage with brand owners to resolve issues or develop improved processes. Right holders continue to convey that excessive delays in takedowns remain a problem, with processing times up to five working days. Other longstanding issues remain unresolved, including ineffective measures to screen sellers and listings, as well as a lack of transparency with enforcement processes, such as penalty mechanisms and decisions rejecting takedown requests.

PRIVATE LAYER

Related companies include Swiss Global and Netulu.

Private Layer, reportedly operated from Panama with data center and hosting operations in Switzerland, is a "bulletproof" hosting provider that supports a number of infringing sites, many listed here in the NML report, by refusing to respond to right holders and take down infringing content.

RAPIDGATOR

Nominated as rapidgator.net. Related sites include rg.to. Reportedly operated from Russia.

Right holders report that Rapidgator, one of the largest file sharing websites in the world, hosts unlicensed high-quality, recent, and pre-release content. Other notorious markets use Rapidgator to host their pirated content. Rapidgator collects revenue through its premium membership and subscription plans and employs rewards and affiliate schemes to compensate users based on downloads and sales of new accounts. Rapidgator reportedly takes down some infringing content, but there are no proactive measures in place to prevent the upload of

infringing content, and content is frequently reuploaded and disseminated. According to SimilarWeb, the site received over 28 million visits in August 2025. Trade associations from the music, television, and book publishing industries all nominated Rapidgator for continued inclusion on the 2025 NML.

RUTRACKER

Nominated as rutracker.org. Hosted in Russia.

Rutracker remains one of the most popular torrent sites in the world, even though it does not provide access to the public and requires users to register an account with a username and password. According to SimilarWeb, Rutracker received 439 million visits in the past year. The site provides access to pirated movies, television shows, software, electronic games, video games, and other copyright-protected works. It has been reportedly subject to blocking orders in Australia, Brazil, Denmark, Indonesia, Italy, Malaysia, Russia, and Singapore.

SAVEFROM

Nominated as savefrom.net. Related sites include savef.net, savefrom.live, savefrom.app, save-from.net, savefrom.best, and save-from.biz.

SaveFrom is a popular stream-ripping site that circumvents the content-protection measures for videos on sites such as YouTube and allows users to download videos or convert them to digital audio files on their devices. In April 2020, SaveFrom stated that, due to “attacks by certain U.S. copyright holders,” it was terminating its services in the United States. It has also reportedly terminated services in the United Kingdom and Spain. However, it continues to operate in other countries and reportedly received nearly 2 billion visits in the past year.

SCI-HUB

Nominated as sci-hub.se. Related sites include sci-hub.ru, sci-hub.st, annas-archive.org, and annas-archive.gs. Reportedly hosted and operated from Russia.

Right holders continue to report that Sci-Hub and its mirror sites facilitate unauthorized access to over 88 million journal articles and academic papers, which comprise at least 90% of all

toll-access published journal articles, a proportion greater than what is available legally to major institutional subscribers. Right holders state that Sci-Hub obtains these articles by using hijacked proxy credentials to allow remote users to illegally access various university intranet systems and university databases. The copyright-protected material obtained by Sci-Hub is reportedly stored on Sci-Hub servers as well as cross-posted to other well-known infringing sites such as Libgen, Z-Library, and Anna's Archive. Right holders state that the site appears to be funded through both donations as well as cryptocurrency. Sci-Hub is reportedly subject to blocking orders in Belgium, Denmark, France, Germany, Italy, Portugal, Russia, Spain, and Sweden and is the subject of similar enforcement activity in India. U.S. right holders secured several court judgments against Sci-Hub in 2015 and 2017, resulting in the suspension of its U.S.-administered domains.

SQUITTER

Nominated as squitter.eu.

Right holders report that Squitter Networks or ABC Consultancy, another “bulletproof hosting provider,” hosts a number of online piracy services, including several sites highlighted in this list. Squitter’s domain registration suggests it may be in the Netherlands, but physical addresses associated with Squitter point to various other countries. Despite stakeholder investigations, the true locations of the site and associated companies are unknown. The site appears to control Internet Protocol (IP) addresses assigned to several different countries and right holders report that the service changes names frequently, making it more difficult to track and identify. Right holders state that Squitter has ignored thousands of takedown notices and does not respond to any communications. An associated domain reportedly advertised “[Digital Millennium Copyright Act] ignored” hosting as a service. Squitter appears to be a “stealth bulletproof” provider attempting to operate as anonymously as possible.

STREAMTAPE

Nominated as streamtape.com. Reportedly hosted in France.

Streamtape is a popular video hosting service that offers unlimited storage and bandwidth. According to its website, Streamtape offers a partner program that allows content uploaders to earn money for every 10,000 downloads or streams of their content. As a result, Streamtape has become a popular platform for sharing infringing content. In August 2025 alone, SimilarWeb reported that Streamtape had 13.6 million visits from 6.02 million unique visitors.

TAOBAO

Nominated as taobao.com. Headquartered in China.

Taobao, one of the largest e-commerce platforms in the world, is Alibaba's platform for Chinese consumers. A number of stakeholders have recognized Alibaba for its proactive engagement and cooperation with right holders and the U.S. Government, as well as for its investment in anti-counterfeiting processes and tools across its platforms, including Taobao. Alibaba emphasizes that, since its 2023 structural reorganization, Taobao is devoting more resources to IP enforcement, applying effective and efficient AI tools to take down large numbers of listings for counterfeit goods, and that its international and China-facing teams are working to increase support for law enforcement investigations of counterfeit sellers. At the same time, some stakeholders have mixed experiences with Taobao's ability to remove listings of counterfeits, the level of transparency about Taobao's notice-and-takedown and repeat infringer policies, and the amount of information Taobao requires to support a takedown request, especially for copyright holders. Even right holders that express appreciation for Alibaba's outreach continue to report high volumes of counterfeit products and pirated goods, as well as challenging requirements to identify specific piracy indicators to support requests for the takedown of listings for pirated goods. Taobao reports that it continues to provide leads for offline investigations, including a recent large-scale enforcement operation in China. Yet, some right holders report that investigations have limited resources except where more influential brands are involved. USTR will continue to monitor the transparency and effectiveness of

Taobao's anti-counterfeiting efforts, including the evidentiary requirements for takedown requests.

THEPIRATEBAY

Nominated as thepiratebay.org. Utilizes reverse proxy services to mask the location of its hosting servers.

As one of the first BitTorrent indexing websites and one of the most vocal in openly promoting piracy, ThePirateBay reportedly remains one of the most frequently visited BitTorrent websites in the world. In 2009, a Swedish court convicted the founders of ThePirateBay of large-scale copyright infringement and sentenced them to prison as well as large fines. However, ThePirateBay is available in 35 languages and serves a global market, using multiple alternative domains hosted globally. Authorities in more than twenty countries have issued orders blocking access to this site. Right holders report that this site does not respond to takedown requests.

UNKNOWNCHEATS

Nominated as unknowncheats.me.

This site is an example of a popular "cheat" site that allows users to submit, develop, and download video game cheat codes for players. These codes can infringe on right holders' copyrights when the cheat code copies the underlying code of the game software. The unknowncheats site reportedly offers cheat code software for over 100 different copyright-protected titles and relies on advertising to generate revenue.

VEGAMOVIES

Nominated as vegamovies.in. Related sites include vegamovies.hot, vglist.nl, vegamovies.gmbh, vegamovies.house, and vegamovies.pics.

Vegamovies is one of the most popular piracy streaming sites in India. The site is in English and is known for providing unauthorized access to a wide range of international movie and television content, as well as India-based content. Right holders report that the site frequently changes its domain name to evade enforcement efforts, and has multiple sources of

revenue including advertising. The site reportedly has more than 40 known associated domains, so total traffic is widely dispersed and difficult to estimate.

VIRTUAL SYSTEMS, LLC

Nominated as vsys.host. Reportedly based in Ukraine.

Right holders report that Virtual Systems is another popular bulletproof hosting provider that provides services to upwards of five thousand infringing websites and IPTV services, including many sites highlighted in this NML. The Virtual Systems website reportedly advertises “DCMA Ignored” hosting services, and right holders state that the site continues to ignore thousands of takedown notices, does not respond to any communications, and frequently changes domain names to avoid enforcement actions.

VK

Nominated as vk.com. Headquartered in and operated from Russia.

Vkontakte (VK) is one of the most popular sites in the world and among the top sites visited in Russia and other Russian-speaking regions. According to SimilarWeb, vk.com received almost a billion visits in August 2025. VK continues to operate as an extremely popular social networking site but also reportedly facilitates the distribution of copyright-infringing files, with thousands of infringing films and television programs identified by the U.S. motion picture industry each month. The site allows users to easily upload video files, including pirated content, and to stream this content through an embedded video player. Despite previous actions to improve copyright protection, right holders report that since 2022 VK’s responsiveness to takedown notices has been inconsistent despite ongoing regular notification filings from right holders. Moreover, right holders continue to note that VK lacks an effective repeat-infringer policy and other processes to effectively reduce the volume of infringing content posted by its users.

WHMCS SMARTERS

Sites include whmcsmarters.com and iptvsmartersplus.com. Also doing business as New Spark Technology, Mohali, India.

WHMCS Smarters is a company in India that sets customers up in the illegal IPTV business by building them a customized “over the top” (OTT) IPTV platform and providing end-to-end support. According to the WHMCS Smarters website, services include website design and development, customized apps on several different platforms, design, graphics, branding, payment processing, and billing. WHMCS Smarters also provides Smarters Pro, a media player configured for different types of platforms that allows users to watch live television, movies and TV series on demand, and TV catch-up on their devices. While WHMCS Smarters states that it does not sell infringing streams, channels, or other content or subscriptions, it does sell the software, tools, and services an individual would need to establish and operate his or her own “off the shelf” illegal IPTV business.

Y2MATE

Nominated as y2mate.nu.

Y2Mate is reportedly an extremely popular YouTube stream-ripping site. Despite a slight decline in popularity, the site still reportedly received over 650 million visits in the last 12 months. Y2Mate allows users to easily download music videos and tracks from YouTube and similar sites, convert them to video or audio files, and download them to their devices. Stream ripping is a popular method for obtaining unauthorized copyright-protected music.

YTS.MX

Nominated as yts.mx. Related sites include yts.lt, yts-official.to, and yts-official.org. Reportedly hosted in Bulgaria.

YTS (also known as YIFY), is reportedly the most popular peer-to-peer torrent site dedicated to movies in the world, with over 62,000 high-quality films available including high definition, 4K, and even 3D. The site facilitates global consumption of its library of pirated content through an accompanying subtitle site, yifysubtitles.ch, which provides subtitles in numerous different languages synchronized to each individual torrent. The site is reportedly

subject to blocking orders in Australia, Denmark, France, India, Indonesia, Italy, Ireland, Malaysia, Norway, Portugal, Spain, and the United Kingdom, but frequently changes domain names to avoid enforcement.

Physical Markets

While the sale and distribution of counterfeit and pirated goods online continue to be a growing concern, physical markets continue to enable substantial trade in counterfeit and pirated goods.

In a global environment, basic enforcement measures against unscrupulous retailers and wholesalers will not be sufficient to reduce the flow of counterfeit and pirated products. To address current and ongoing challenges, governments need targeted, modernized enforcement tools, including:

- effective border enforcement measures to prevent the exportation of counterfeit and pirated goods manufactured in their countries, the importation of such goods into their countries, and the transiting or transshipment of such goods through their countries on the way to destination countries;
- the ability for customs and criminal authorities to detain, seize, and destroy counterfeit and pirated goods entering into and exiting from free trade zones;
- robust data sharing and border enforcement authority to interdict small consignment shipments, such as those sent through postal or express-courier services;
- asset forfeiture, which is a tool that can be used to reach owners of the markets or facilities where infringing products are manufactured, assembled, processed, sold, and stored;
- criminal procedures and penalties for trafficking in counterfeit labels and packaging; and
- enhanced criminal penalties for particularly serious cases, such as large-scale commercial trafficking in counterfeit products, and trafficking in counterfeit products that threaten security, health, and safety.

This year, stakeholders continue to report that many physical markets also offer online sales, a trend that grew out of the COVID-19 pandemic and which market vendors continue to maintain and profit from today. Some sellers have permanently shifted to focus more on online

trafficking, using their physical space to store goods that are subsequently sent or delivered to online purchasers, while others have adopted a hybrid approach, conducting both in-person and online sales. USTR will continue to monitor and evaluate the infringing activities in these markets.

ARGENTINA

Barrio Once, Buenos Aires

Barrio Once is a large neighborhood with a high concentration of indoor and outdoor street vendors of counterfeit products. Right holders report that vendors offer large quantities of easily visible counterfeit apparel, cosmetics, handbags, wallets, accessories, and shoes. A September 2025 report on illegal sales from the Argentine Chamber of Trade and Services (CAC) reported that Barrio Once represents 24% of total illegal street vendors in the City of Buenos Aires. In 2025, the Prosecutor's Office of the City of Buenos Aires led multiple raids and inspections in Barrio Once, closing several stores and a clandestine workshop producing counterfeit soccer jerseys. Authorities seized counterfeit merchandise valued at approximately \$175,000. These enforcement actions have reduced the number of illegal vendors in Barrio Once, but also prompted their relocation to other illegal markets.

La Salada, Buenos Aires

La Salada is an area covering about 50 acres that incorporates three markets primarily for low-cost clothing and apparel. La Salada reportedly hosts 30,000 workers across 8,000 vendors and supports the sale and international distribution of counterfeit goods manufactured in the outskirts of the City of Buenos Aires. The market has been operating for over 30 years, and now also advertises on social media and hosts its own website. In 2025, a judge ordered the closure of the market after a federal prosecutor led multiple raids in La Salada and other markets. The raids led to multiple arrests, including of one of the principal owners of the market. Operations in La Salada ultimately resumed but under enhanced oversight, including required registration of vendors, financial monitoring by national and provincial fiscal agencies, and a ban on counterfeit

goods and on cash sales. Although key arrests marked progress, sustained long-term oversight and legal accountability remain critical to maintaining these reforms. Argentina's currency depreciation has increased the attractiveness of the market for shoppers not only from Argentina but from neighboring countries. In 2025, La Salada continued to attract shopping tours from neighboring countries such as Brazil and Uruguay and tourists from across South America.

BRAZIL

Rua 25 de Março, São Paulo

The Rua 25 de Março area includes seven markets spanning São Paulo's Centro Histórico, Santa Ifigênia, and Bras neighborhoods, including Shopping 25 de Março, Galeria Page Centro, Santa Ifigênia, Shopping Tupan, Shopping Korai, Feira da Madrugada, and Nova Feira da Madrugada. The Rua 25 de Março markets remain well known for selling counterfeit and pirated goods as well as for containing warehouses that store these goods. Right holders note that this area is one of the largest wholesale and retail counterfeit markets in Brazil and all of Latin America, with over a thousand shops selling an extremely high volume of counterfeit goods of all kinds. Consumer electronics and apparel are reportedly the most visible goods in the market, but right holders have raised concerns about counterfeit printing supplies, agricultural chemicals, and pharmaceuticals, as well as pirated works. Right holders also state that the Rua 25 de Março markets contain facilities to distribute counterfeit and pirated goods throughout the São Paulo region and other parts of Brazil. There were no reports of enforcement actions in 2025, and past enforcement has not led to significant criminal prosecutions or meaningful penalties against counterfeit sellers.

CAMBODIA

Central Market, Phnom Penh

Central Market, a sprawling market and historic landmark in Phnom Penh, is known for the sale of counterfeit goods, including apparel, shoes, handbags, watches, sunglasses, and other items. Many of the goods appear to be imported from China or Vietnam, with some

vendors claiming to sell “top grade” counterfeit goods imported from South Korea. Although local authorities have conducted raids to seize counterfeit products, the Central Market remains a popular destination for consumers seeking counterfeits, and Cambodia continues to be a growing hub for the distribution of counterfeit goods.

CANADA

Pacific Mall, Toronto

Right holders continue to report the widespread availability of counterfeit goods for sale at Pacific Mall, with Pacific Mall management not taking the necessary measures against sellers and law enforcement not prioritizing actions against counterfeit trade. Noticeably counterfeit luxury goods, apparel, electronics, and automobile parts are reportedly on display or hidden under tables or in back rooms but are available upon request. Some higher-end counterfeit products are being sold as authentic, with packaging and tags resembling the authentic brands but at a reduced price. Stakeholders report that in 2025, the Pacific Mall’s management continues to remain largely disinterested in engaging with intellectual property owners to address well-known issues with counterfeit goods, while engagement by local law enforcement remains sporadic.

CHINA

China continues to be the number one source of counterfeit products in the world. IP-infringing goods from China, including Hong Kong, seized by U.S. Customs and Border Protection in Fiscal Year 2024 accounted for almost 93% of the value of all IP-infringing goods seized from all countries, as measured by manufacturers’ suggested retail price.²⁸ Counterfeiting activities have increased as economic conditions have declined within China. Although foot traffic to some physical markets has declined, sellers of counterfeit merchandise continue to use their brick-and-mortar storefronts as points of contact for customers, sites for “sample/product testing,”

²⁸U.S. Customs and Border Protection, Intellectual Property Rights (IPR) Seizures Dashboard (Apr. 1, 2025), <https://www.cbp.gov/newsroom/stats/intellectual-property-rights-ipr-seizures>.

and centers for fulfillment of online sales. Enforcement authorities targeting counterfeit goods online often uncover links to vendors with a presence in physical markets. However, in many cases, enforcement at physical markets remains weak and easily circumvented by vendors. Even when there is a police presence near such markets, there is little deterrent effect against counterfeit sellers. USTR encourages China to modify and expand the scope of robust enforcement actions to respond to the changing nature of counterfeit sales at physical markets, with a special focus on the following key markets.

Baiyun Leather Trading Center, Guangzhou, Guangdong Province

Right holders reported that storefronts at this location sell many types of counterfeit goods, including leather bags, garments, wallets, and other accessories. Many shopkeepers openly offer counterfeit goods, but even those that do not will, upon request, redirect customers to secret showrooms or a second shop upstairs. Sellers even indicated that they could ship counterfeit items internationally, including to the United States. While there have been some reports of regular raids conducted by law enforcement and administrative penalty decisions against some sellers, it is reportedly difficult to address the counterfeiting issue as such products remain widespread.

Huaqiangbei Electronics Malls, including the Yuan Wang Digital Mall, Long Sheng Communications Market, Tongtiandi Communication Market Feiyang Yang Times, SEG Communication Market, and Taixing Communications Market, Shenzhen, Guangdong Province

This market offers widespread and high-volume retail and bulk sales of counterfeit electronics, as well as counterfeit accessories such as watches and handbags. The location continues to supply electronic devices and components from manufacturers in Shenzhen and surrounding cities to the world. At one of the malls, Yuan Wan Digital Mall, nearly all storefronts sold counterfeit products, with vendors offering “high quality copies” to a steady stream of customer foot traffic. Many counterfeit sellers continue to shift their sales online. If a counterfeit product is not in stock, sellers often propose following up with buyers in order to set up and

complete the transaction online. At another location in the area, SEG Communication Market, while a large sign warns against intellectual property rights violations and outlines potential punishments, there has been no visible enforcement by authorities as shopkeepers openly offered counterfeit goods to passersby.

Kinsun Market near Zhanxi Road, Guangzhou

This market in Southeastern China consists of five floors of vendors that sell almost exclusively counterfeit goods. The first two floors openly sell counterfeits of well-known clothing brands, as well as bags, watches and jewelry. The upper three floors also contain counterfeits, but appear to be abandoned and are listed as “office space” on signage to disguise them. Shopkeepers will reportedly escort customers up to these upper floors past highly secured doorways to reach well-kept shops full of counterfeit items.

Luohu Commercial City, Shenzhen, Guangdong Province

This is a well-known mall located next to the Luohu border crossing between Shenzhen and Hong Kong, China. Right holders report that counterfeit products, in particular clothes and fashion accessories like bags, continue to be available at this market. In addition, while large banners in the market encourage respect for intellectual property rights, there appears to be no visible enforcement, as many sellers openly sell so-called “high quality” counterfeits to customers.

Wu'ai Market, Shenyang, Liaoning Province

This large wholesale and retail market in Northeastern China, which has a state-owned management company, remains a regional hub for the distribution of counterfeit shoes, jewelry, toys, handbags, backpacks, luggage, and apparel. Vendors continue to openly advertise such counterfeit products for retail and wholesale purchase. Right holders continue to report that although inspections and raids have been conducted from time to time, the impact has been minimal. Additionally, local authorities are reportedly concerned about how actions against

infringing vendors could harm employment in the region, which has discouraged them from addressing counterfeiting.

COLOMBIA

San Andresitos Market, Bogotá

The “San Andresitos” markets are a collection of over 600 shopping centers across Colombia selling counterfeit goods, such as clothing, shoes, handbags, perfumes, and cell phone accessories. While San Andresitos markets exist in most large Colombian cities, the majority are located in Bogotá. The largest San Andresitos in Bogotá are “San Andresito de la 38” and “San Andresito de San José.” Right holders estimate that 80% of the foreign-branded products sold at San Andresitos are counterfeit. Although Colombia’s Tax and Customs Police have seized counterfeit goods at market stalls, most of the inventory is located in off-site warehouses. As a result, enforcement efforts are also focused on warehouses where counterfeit goods are stockpiled and distributed to San Andresitos markets across the country. San Andresitos markets continue to draw large numbers of customers, with the local media reporting that the markets generate over one million jobs nationwide. There is little evidence of a substantive reduction in the counterfeit products sold in San Andresitos markets in the past year. The individual shopping centers also maintain professionally branded websites and social media accounts to advertise counterfeit merchandise found in physical stores.

INDIA

Musafir Khana Market, Mumbai

This market, one of the oldest and most popular in Mumbai, has been implicated in selling counterfeit products, especially cosmetics, electronics, watches, and accessories. Musafir Khana plays a significant role in supplying counterfeit inventory to other markets in the region. Although some targeted enforcement actions were taken by police in recent years, including 2025, right holders report that law enforcement has struggled to control illicit sales.

Sadar Patrappa Road Market, Bengaluru

Sadar Patrappa (SP) Road Market is a very popular market well known for a wide variety of counterfeit electronic products, sold at a fraction of the cost of legitimate products. This market also sells counterfeit ink cartridges, mobile accessories, and chargers, as well as pirated software. Despite occasional raids in this market, enforcement efforts by local authorities have been insufficient to significantly reduce sales of counterfeit and pirated products in this Bengaluru market.

Tank Road, Delhi

Right holders report that this central New Delhi market continues to sell a significant number of counterfeit products, including apparel, footwear, watches, and beauty products. Tank Road Market—as well as other nearby markets in the Karol Bagh neighborhood, including the Karol Bagh Market and Gaffar Market—supply wholesale counterfeit goods to be resold throughout the region, as well as to various online markets based in India, and small-scale manufacturing occurs in the area as well. Right holders raise concerns that counterfeits sold at the markets in the Karol Bagh neighborhood pose a risk to public health and safety. They also report that support from local police has been inconsistent and enforcement efforts have been insufficient to significantly reduce sales of counterfeits in the market.

INDONESIA

Mangga Dua Market, Jakarta

Mangga Dua, particularly the market known as ITC Mangga Dua, remains a popular market for a variety of counterfeit goods, including handbags, wallets, toys, leather goods, accessories, and apparel. There has been little or no enforcement actions against counterfeit sellers. Stakeholders continue to report that warning letters issued to sellers have been largely ineffective, and they raise concerns that counterfeit sales typically resume after such warnings. Indonesia should take robust and expanded enforcement actions in this and other markets, including through actions by the IP Enforcement Task Force.

KYRGYZ REPUBLIC

Dordoi/Dordoy Bazaar, Bishkek

Known locally as “Container City,” this market stretches for more than a kilometer on the northeastern outskirts of Bishkek and is one of the largest markets in Central Asia. Stakeholders reported no substantive improvements in the situation at Dordoi Bazaar this past year. Large volumes of various types of counterfeit goods, including footwear, clothing and luxury items, are reportedly easy to find. This market reportedly also supplies other markets including Jayma Bazaar in Osh, which further supplies markets and consumers in the region. Dordoi Bazaar has traditionally been the center of the Kyrgyz Republic’s re-export activity, and thus a transit hub for China-made goods, including counterfeits, en route to Europe, Russia, and other countries in the region. Laws prohibiting counterfeit goods are rarely enforced in the market and past efforts by the Kyrgyz government to mandate electronic cash registers to track sales have failed.

MALAYSIA

Petaling Street Market, Kuala Lumpur

Petaling Street Market is a well-known market that is popular with tourists and sells counterfeit goods, including luxury handbags, apparel, shoes, accessories, and electronics. Stakeholders report that the Ministry of Domestic Trade and Cost of Living have increased enforcement activity by conducting large-scale raids and seizing significant quantities of counterfeit goods. Nonetheless, counterfeit goods continue to be widespread, and stakeholders express the hope that enforcement authorities can consistently follow through on the raids with investigations and penalties.

MEXICO

El Santuario, Guadalajara

El Santuario is one of the oldest neighborhoods in Guadalajara and is a well-known location for the sale and distribution of illicit drugs, including counterfeit, stolen, and expired

medicine. Vendors in this neighborhood are engaged in retail-level sales, wholesaling, warehousing, and distribution of counterfeit pharmaceuticals throughout the region, which stakeholders report have resulted in a billion dollars in annual losses to legitimate companies. The illegal activity in this neighborhood is conducted in the open with no apparent enforcement actions by authorities to seize the counterfeit pharmaceuticals or bring criminal actions against those responsible for the illicit activity.

Mercado San Juan de Dios, Guadalajara

Mercado San Juan de Dios, also known as Mercado Libertad and located in Guadalajara, is the largest indoor market in Latin America, spanning over 430,000 square feet and hosting approximately 3,000 stalls. Right holders report that the majority of vendors in this market sell counterfeit apparel, footwear, home goods, pharmaceuticals, and accessories, as well as pirated software, movies, electronic games, and electronic-game circumvention devices. Stakeholders from the video game industry recently observed that vendors offer a variety of services to support circumvention of technological protection measures, including selling, repairing, and the installation of modchips on consoles. Despite the reported scale of counterfeiting, no major IP enforcement raids were conducted in 2025. Right holders report that the government of Guadalajara is the owner of the market and that the illegal activity is conducted openly, in full view of the authorities.

Tepito, Mexico City

Tepito, a massive open-air market in the middle of Mexico City, is a major distribution hub for counterfeit and pirated goods in local markets across Mexico and Central America. Right holders report that Tepito remains dangerous due to criminal activity, making it nearly impossible for right holders to enforce their rights themselves. Infringing items sold at Tepito include counterfeit apparel, accessories, beauty products, luxury goods, and electronics, as well as video games, modified game consoles, and circumvention devices designed to enable video

game piracy. However, unlike previous years, in 2025 Mexican authorities apparently conducted no raids against counterfeit and pirated products at the market.

PARAGUAY

Ciudad del Este

The markets at Ciudad del Este remain a regional hub for the sale of counterfeit goods, as well as the manufacture, assembly, and distribution of counterfeit and pirated products in the Brazil-Argentina-Paraguay tri-border area and beyond. Although high-end department stores offer legitimate goods, many tourists are drawn to nearby storefronts that offer counterfeit goods products, including apparel, footwear, luxury goods, electronics, and cosmetics. Some right holders have described the Municipal Market as a particular area of concern, noting an estimate that over 75% of vendors offer counterfeit goods, affected brands cover numerous product sectors, and the overall volume of illegal sales has increased since the previous year. Organized criminal groups are also reportedly involved in the trafficking of counterfeit goods, and right holders and law enforcement have sometimes faced a violent response to enforcement actions. Although officials at the National Directorate of Intellectual Property (DINAPI), customs officials, and local prosecutors have reported efforts to improve coordination and organize raids, the scope of the counterfeit distribution and manufacturing operations in Ciudad del Este requires a whole-of-government approach and stronger efforts to address illicit activities in the markets.

PERU

Gamarra District, Lima

The Gamarra District is Peru's primary textile market and garment district which includes more than twenty blocks of large, multistory complexes with thousands of shops where vendors sell fabric in bulk, curtains, bed linens, and all categories of clothing, the vast majority being off-brand as well as counterfeit apparel. In addition to the indoor stores, dozens of makeshift vendors fill the streets with racks and tables full of clothing bearing a variety of recognizable

brands, sports teams, and cartoon characters. Reviews on travel websites note its wide selection of counterfeit products. In 2025, Peru's National Police conducted 51 operations in Gamarra, reportedly seizing counterfeit items with a total street value of \$90 million. Although police raids have been reported in 2025, these enforcement actions have not resulted in a noticeable decrease in the number of illicit products available in the market.

Polvos Azules, Lima

Polvos Azules is an indoor shopping center located in the La Victoria district of Lima with a capacity of approximately 2,000 stalls selling a wide range of counterfeit apparel, fashion accessories, footwear, perfumes, handbags and luggage, videogames and consoles, cell phones, and other electronics. Polvos Azules has an active e-commerce site as well as various social media accounts for advertising purposes. The social media pages also include photos and contact information for customers interested in purchasing items from individual vendors. While some stakeholders reported positive engagement with law enforcement in 2025, the frequency with which raids have been conducted was generally viewed as insufficient to bring about significant or sustained improvements in the market, particularly when the penalties lacked any meaningful deterrence.

PHILIPPINES

Greenhills Shopping Center, San Juan, Metro Manila

Greenhills Shopping Center is a large mall in Manila with many storefronts selling counterfeit electronics, perfumes, watches, shoes, accessories, and fashion items. Law enforcement authorities, in collaboration with right holders, have conducted raids at the mall, and the management at Greenhills Shopping Center has applied a three-strikes rule to take action against counterfeit sellers. The management reports that almost 300 vendor stalls have been removed over the past year for selling counterfeit goods. The government, through the National Committee on Intellectual Property Rights (NCIPR), is working with right holders and shopping center management on implementing a transition program to transform Greenhills

Shopping Center into a high-end mall with legitimate sellers. NCIPR is also working to establish a pilot location for the NCIPR Help Desk at Greenhills Shopping Center, in coordination with management and the city government. Although right holders have welcomed these developments, they also continue to observe a significant number of counterfeit goods and continue to wait and see if the transition program will resolve their concerns about the volume of counterfeit goods.

RUSSIA

Gorbushkin Dvor Trade Center, Moscow

Gorbushkin Dvor Trade Center is reportedly known primarily for its high volume of counterfeit electronics and high-end home appliances, such as refrigerators, washing machines, and flat screen televisions. Counterfeit luxury watches and pirated movies, videogame systems, and software are also available at a fraction of normal retail prices. There are reportedly more than 1,000 vendors in this market with no visible police presence. This market has been a long-standing feature of the NML, and right holders report no improvements in IP protection efforts. The Moscow City government had previously announced plans to close the Gorbushkin Dvor market and build an apartment building on the site by 2025, but there is reportedly no decrease in market activity and no signs that this plan is moving forward.

Sadovod Market, Moscow

Sadovod Market is the largest trading center for consumer goods in Russia, spanning nearly 100 acres with over 9,500 stores serving more than 90 million customers per year. Businesses from across Russia and Central Asia, as well as China, Vietnam, Türkiye, and Belarus openly trade in counterfeit clothing, accessories, and cosmetics of well-known name brands. In particular, counterfeit cosmetics and perfume are reportedly popular items, due to high-quality packaging that makes the fake products nearly indistinguishable from the legitimate ones as well as to social media advertising by well-known influencers. The market also advertises the availability of bulk purchases of beauty products both in the market and via social media. Right

holders note that there is no visible police presence in the market and vendors openly display counterfeit products.

THAILAND

MBK Center, Bangkok

MBK Center in Bangkok is a large eight-floor shopping mall catering to tourists and others. Stakeholders have welcomed significant efforts by the Department of Intellectual Property (DIP) and the Economic Crime Suppression Division of the Royal Thai Police to increase the frequency and scale of raids at MBK Center, with one operation involving over a hundred police officers and 30 officials from DIP. Other high-profile raids have led to the seizure of thousands of items. DIP, partner agencies, and the MBK Center have also conducted high-profile public education campaigns to raise awareness of the negative impacts of counterfeits among consumers and retailers. MBK Center has reportedly terminated rental agreements with tenants who have been arrested on charges of IP violations. Stakeholders welcomed the visible reduction of openly displayed counterfeit products, with many stores reportedly shut down in recent months. However, they also report that counterfeit goods have reemerged in temporary stalls on the higher-level floors, including counterfeits of luxury handbags, clothing, watches, and shoes. It remains important for MBK's owners and operators to continue its sustained enforcement actions, including raids and lease terminations, to address the high volume of counterfeits and discourage the further sale of counterfeit goods.

TÜRKIYE

Aksaray, Istanbul

Türkiye's geographic location makes it a major transit hub for counterfeit goods coming from China into European and Middle Eastern markets. The markets of the Aksaray district are a top destination in Istanbul for counterfeit goods. Both local shoppers and tourists visit Aksaray specifically to buy these counterfeits, as the area has a reputation for selling affordable but relatively high-quality fakes. Shops and stalls in places like the Aksaray Yeralti Carsisi frequently

openly display and sell imitation products of major luxury brands, including apparel, shoes, handbags, watches, and accessories.

Tahtakale, Istanbul

The Tahtakale district of Istanbul adjoins the walled Grand Bazaar, but is commercially separate. The shops in the Tahtakale district sell a wide variety of inexpensive goods, many of which are counterfeit clothing, shoes, and consumer electronics. Right holders report that the Turkish Police have conducted multiple raids in the markets in recent years and there have even been a number of prosecutions. As a result, vendors have worked to develop more sophisticated strategies to hide counterfeit goods and avoid detection and counterfeit products remain widely available in the market. Right holders continue to encourage more vigorous and proactive enforcement actions.

UNITED ARAB EMIRATES

Markets in Deira District, Dubai

The Deira District is home to several markets, including the Dubai Souk, Deira Old Souk, Dubai Gold Souk, Dubai Spice Souk, and Perfume Souk. Right holders report these markets are well-known among tourists and locals for selling IP-infringing goods ranging from luxury items to industrial products. Vendors sometimes sell counterfeit goods openly but more commonly make them available in back rooms or nearby buildings. Despite regular official enforcement efforts, the Deira District remains a major center for counterfeit trade in the region. Right holders report that, despite frequent raids and large-scale seizures by authorities, counterfeit products remain widely available. Right holders continue to report the need to issue deterrent-level penalties to discourage repeat violators and increased border enforcement measures to interdict counterfeit goods before they reach the local market.

VIETNAM

Gia Lam, Hanoi

Gia Lam market in Hanoi, also known as Ninh Hiep market, is well known among locals for both retail sales and wholesale distribution of counterfeit goods, including luxury handbags, clothing, and footwear. Sellers reportedly source their counterfeit goods from China. Although enforcement authorities raided the main market structure and closed many shops in May 2025, counterfeit products remain widespread in adjacent streets.

Saigon Square Shopping Mall, Ho Chi Minh City

Saigon Square Shopping Mall, located just across the street from one of the largest shopping malls in Ho Chi Minh City, remains a popular market for the sale of counterfeit luxury products, including handbags, wallets, jewelry, watches, and electronics. As counterfeit sales to locals have shifted online, the market now mainly attracts tourists and domestic travelers. Although government authorities have increased administrative enforcement efforts in recent months, which temporarily reduce the availability of counterfeits, right holders note that low penalties have had little deterrent effect, and counterfeit products remain rampant

Public Information

The 2025 Notorious Markets List is the result of the fifteenth out-of-cycle review of notorious markets, which USTR initiated on August 18, 2025, through a Federal Register Request for Public Comments. The 77 public submissions this year are available at <https://www.regulations.gov>, Docket Number USTR-2025-0018. USTR developed the 2025 NML in coordination with the federal agencies represented on the Special 301 Subcommittee of the Trade Policy Staff Committee (TPSC). Information about Special 301 and other intellectual property-related processes and issues is available at <https://ustr.gov/issue-areas/intellectualproperty>.

To assist U.S. right holders and consumers who confront IP infringement online, the U.S. Government continues to expand the tools available on <https://www.stopfakes.gov>, including by providing links to infringement reporting mechanisms at a number of popular online retailers and markets. Victims and interested parties may report IP theft and import violations to U.S. law enforcement agencies through <https://www.stopfakes.gov>, <https://eallegations.cbp.gov>, or <https://www.iprcenter.gov/referral/report-ip-theft-form>.