



2016 Out-of-Cycle Review of Notorious Markets



OFFICE *of the* UNITED STATES TRADE REPRESENTATIVE

DECEMBER 2016

Contents

1

Overview

3

Positive Developments Since the 2015
Out-of-Cycle Review of Notorious Markets

5

Issue Focus: Stream Ripping

6

Results of the 2016 Out-of-Cycle
Review of Notorious Markets

22

Public Information

Results of the 2016 Out-of-Cycle Review of Notorious Markets

Overview

Commercial-scale trademark counterfeiting and copyright piracy cause significant financial losses for right holders and legitimate businesses, undermine critical U.S. comparative advantages in innovation and creativity to the detriment of American workers, and can pose significant risks to consumer health and safety. The Notorious Markets List (List) highlights prominent online and physical marketplaces that reportedly engage in and facilitate substantial copyright piracy and trademark counterfeiting.^[1] A goal of the List is to motivate appropriate action by owners and operators in the private sector, as well as governments, to reduce piracy and counterfeiting.

The Office of the United States Trade Representative (USTR) has developed the List under the auspices of the annual Special 301 process.^[2] USTR solicited comments regarding potential markets to highlight in this year's List through a Request for Public Comments published in the Federal Register ([WWW.REGULATIONS.GOV](http://www.regulations.gov), Docket Number USTR-2016-0013). The List is based on publicly-available information.

USTR highlights these markets not only because they exemplify global counterfeiting and piracy concerns, but also because the scale of infringing activity in such markets can cause significant economic harm to U.S. intellectual property rights (IPR) holders. Some of the identified markets reportedly host a combination of legitimate and unauthorized activities. Others reportedly exist solely to engage in or facilitate unauthorized activity. The List is not an exhaustive account of all physical and online markets worldwide in which IPR infringement may take place.

USTR has identified notorious markets in the Special 301 Report since 2006. In 2010, USTR announced that it would begin publishing the List separately from the annual Special 301 Report, pursuant to an Out-of-Cycle Review (OCR). USTR first separately published the List in February 2011. The present List is the result of the 2016 OCR of Notorious Markets.

The List does not make findings of legal violations. It also does not reflect the U.S. Government's analysis of the general IPR protection and enforcement climate in the countries connected

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

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

with the listed markets. A broader analysis of IPR protection and enforcement in particular countries or economies is presented in the annual Special 301 Report published on or around April 30th of each year (please refer to the Public Information section at the end of this document).

The List includes several previously-identified markets because our previously-stated concerns with those particular markets have not been addressed. We have examined each market anew and updated each listing. Other previously-identified markets may not appear in the present List for a variety of reasons, including that: the market has closed or its popularity or significance has diminished; enforcement or voluntary action has reduced or eliminated the prevalence of IPR-infringing goods or services; market owners or operators are cooperating with right holders or government authorities to address infringement; the market is no longer a noteworthy example of its kind; or no commenter nominated the market for continued inclusion on the List. ■

Positive Developments Since the 2015 Out-of-Cycle Review of Notorious Markets

Since the release of the 2015 List, some market owners and operators have undertaken notable efforts to address the widespread availability of pirated or counterfeit goods in their markets. The United States commends these efforts, and encourages governments, right holders, and the owners and operators of these and other markets, including those newly identified in the 2016 List, to engage in sustained and meaningful efforts to combat piracy and counterfeiting.

During the past year, some previously-listed online markets have been subject to successful enforcement efforts or are reported to have undertaken various measures that demonstrated a willingness to cooperate in addressing infringement, such as: accelerating responses to infringement complaints; entering into licensing arrangements with right holders; developing technology to identify or prevent infringing uses of platforms; and engaging with right holders to develop cooperative procedures. For example, **KAT** (Kickass Torrents)^[3] was allegedly one of the most popular and lucrative illegal piracy sites in the world until it was taken down by a U.S. law enforcement action in cooperation with foreign law enforcement agencies.^[4] The principal operator was arrested and indicted. Following the enforcement action against KickassTorrents, another popular piracy site, **TORRENTZ.EU**, shut down voluntarily. Other notable successes since the release of the 2015 List include the closing of previously-listed **CUEVANA.TV**, as well as the shutdown of previously-nominated Solarmovie.is and Mp3skull.com after federal litigation in the United States.^[5] Uruguay has continued to increase enforcement activities in Free Trade Zones which were on the List in 2014 and then removed in 2015. From January through September 2016, the Intellectual Property, Drug Trafficking and Asset Laundering Division of Uruguay's National Customs Directorate conducted 36 seizures of infringing goods valued at nearly \$10 million. The United States commends these efforts and encourages its trading partners to continue their individual and cooperative efforts to combat piracy and counterfeiting.

One potentially positive development is the announcement, on November 16, by Ukraine's largest file-hosting website **EX.UA** that it will cease operations. The site has been widely reported to have allowed copyrighted music, video, and software to be illegally downloaded since

[3] Only previously- and presently-listed markets appear in bold text. In contrast, markets that have not appeared on this or prior year's Lists are not in bold text. When a paragraph includes multiple references to a market, only the first instance appears in bold text.

[4] See Press Release, U.S. Department of Justice, "U.S. Authorities Charge Owner of Most-Visited Illegal File-Sharing Website with Copyright Infringement," July 20, 2016, available at <https://www.justice.gov/opa/pr/us-authorities-charge-owner-most-visited-illegal-file-sharing-website-copyright-infringement>

[5] Alternative clone, or "mirror," sites may be connected to sites that have closed as a result of successful enforcement action, such as Emp3world.ch, which has the same registrant as Mp3Skull. Mirror sites of Torrentz.eu and Cuevana.tv have also emerged. The United States will continue to follow these developments and assess whether these mirror sites should be re-listed in future reviews.

2009, and has been responsible for 15 to 25 percent of all Internet traffic in Ukraine. The ex.ua announcement followed a Ukrainian police raid of fs.to, another popular Ukrainian file-hosting site. In conjunction with these recent developments, Ukrainian government officials made encouraging statements acknowledging that these websites earn millions of dollars per year, while copyright holders receive nothing for their content. However, Ukraine has yet to pass anti-piracy legislation that would address online piracy despite repeated legislative proposals. Ex.ua is not highlighted as a Notorious Market this year because it has stated an intention to close, but if it does not follow through or change its practices it could be listed next year.

USTR continues to monitor markets that have been removed from the List. Markets may be relisted if there is a change in circumstances, such as if a website or physical market that ceased to operate as a result of enforcement or other action resumes its unauthorized activities or the corrective actions that merited removal from the List prove inadequate or short-lived. ■

Stream Ripping

Stream ripping is an emerging trend in digital copyright infringement that is increasingly causing substantial economic harm to music creators and undermining legitimate services. Stream ripping is the unauthorized act of converting a file from a licensed streaming site into an unauthorized copy for distribution via download to the requester. Stream ripping often involves violations of terms of use and the circumvention of technological protection measures that legitimate streaming services put in place to protect music content from unauthorized copying and distribution. A study from the International Federation of the Phonographic Industry shows that stream ripping is on the rise in the world's leading music markets. Nearly 30 percent of Internet users obtain unauthorized copies of music from stream ripping services.^[6] This is the first Notorious Markets review in which copyright stakeholders have nominated stream ripping sites for inclusion in the List.

Digital music revenues and streaming revenues in particular represent an increasingly important share of music industry growth. In 2015, digital music revenues surpassed physical sales for the first time, and streaming revenues—which grew more than 45 percent—were a major driver behind overall global growth.^[7] Stream ripping is a direct threat to this digital growth as it eliminates the need for users to return to licensed services, thereby depriving artists and record companies of this important revenue source. Pay-for-download sites and legitimate streaming services are simultaneously undermined, and incentives to create and launch new legitimate streaming services are weakened. In recognition of this growing threat, **YOUTUBE-MP3** is added to the Notorious Market List this year as an example of one of the reportedly more popular stream ripping sites. ■

[6] Ipsos and IFPI, 2016 Music Consumer Insight Report, at 16, available at <http://www.ifpi.org/downloads/Music-Consumer-Insight-Report-2016.pdf> (based on 12,610 respondents from 13 countries surveyed—United States, Canada, Great Britain, France, Germany, Spain, Italy, Sweden, Australia, Japan, South Korea, Brazil, and Mexico).

[7] IFPI, Global Music Report 2016, available at <http://www.ifpi.org/downloads/GMR2016.pdf>

Results of the 2016 Out-of-Cycle Review of Notorious Markets

As noted, the 2016 List identifies prominent online and physical markets in which pirated or counterfeit products and services reportedly are available. It does not constitute a legal finding of a violation or an analysis of the general IPR protection and enforcement environment in any affiliated country or economy. The List is not intended to be an exhaustive listing of all notorious markets around the world. The List is drawn from the many nominations received to highlight prominent examples of both online and physical marketplaces where pirated or counterfeit goods reportedly are trafficked to the detriment of legitimate trade in IP-intensive goods and services.

Owners and operators of the notorious markets included in the 2016 List that are willing to address piracy and counterfeiting have many options for doing so. Such owners and operators can 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 enforcement officials to help discourage and curtail acts of infringement. There are a variety of best practices developed by industry groups that can help combat these problems.^[8] However, in the absence of such 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 enforcement tools are at the disposal of right holders and government authorities, which may require closing the loopholes that permit operators to evade the law.

Online Markets^[9]

The 2016 List of notorious online markets again includes examples of various technologies and business models. USTR based its selections not on specific types of technologies or business models but on whether a nominated site or affiliated network of sites was reported to engage in or facilitate substantial piracy and counterfeiting to the detriment of U.S. creators and brand

[8] See, e.g., International Chamber of Commerce Business Action to Stop Counterfeiting and Piracy, "Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain," Mar. 2015, available at <http://www.iccwbo.org/Data/Documents/Bascap/International-engagement-and-advocacy/2015-Roles-and-Responsibilities-of-Intermediaries/>; International Trademark Association, Sept. 2009, "Addressing the Sale of Counterfeits on the Internet," available at <http://www.inta.org/Advocacy/Documents/INTA%20Best%20Practices%20for%20Addressing%20the%20Sale%20of%20Counterfeits%20on%20the%20Internet.pdf>

[9] In most cases, the List identifies online markets by the domain name provided in the public responses to the Federal Register request. However, it is common for operators of online Notorious Markets to change a site's domain name ("domain name hopping") or to use multiple domain names at once to direct users to the main site. The List reflects each market's most commonly referred to or well-known domain name or names as of December 16, 2016.

owners, as well as legitimate sellers and distributors. In addition to facilitating IPR infringement, these sites may lack safeguards for consumer privacy, security, and safety. Some sites reportedly actively and surreptitiously install malware on users' computers, commit advertisement fraud, and enable phishing scams that steal personal information, all to increase their unlawful profits. A July 2016 study concluded that one in three content theft sites expose consumers to malware and other risks.^[10] In some cases, though online markets in the 2015 List are not highlighted this year, improvements may still be required and the United States may continue to raise concerns related to these markets on a bilateral basis with the countries concerned.

4SHARED.COM

This cyberlocker site^[11] is well-known globally and is particularly popular in Brazil.^[12] While 4Shared provides legitimate file-storage services, the site also facilitates the streaming and downloading of high volumes of allegedly pirated videos, music, books, and video games. 4Shared mobile apps reportedly enable users to stream infringing content to mobile devices, while certain search and music player features may encourage music infringement. Right holders use 4Shared's notice-and-takedown mechanism frequently but with little apparent impact on the overall levels of infringing content stored on and accessed through the site. Looking for other ways to steer Internet traffic away from infringing files, right holders have requested more than 50 million removals of 4Shared URLs from prominent search engine results since June 2011; more than any other domain.^[13] While major U.S. payment providers no longer service 4Shared, site operators continue to collect revenue from premium accounts and advertising by using resellers and offshore payment processors.^[14] 4Shared is registered to an entity in the British Virgin Islands and hosted by a company in Cyprus.

[10] Compared to mainstream legitimate websites, content theft sites are 28 times more likely to present malware and other security risks. Digital Citizens Alliance, "Enabling Malware," July 2016, available at <https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0057c1cf-28f6-406d-9cab-03ad60fb50e4.pdf>

[11] The cyberlockers identified in the List reportedly operate primarily to provide users with access to unauthorized content. Such sites are distinguishable from legitimate cloud storage services that enable consumers to lawfully store, share, backup, and access data.

[12] Unless otherwise noted, the global and country-specific popularity of online markets referenced in this List is determined through Alexa rankings, SimilarWeb data, and public submissions. Alexa.com utilizes a proprietary methodology to analyze global and country-specific user traffic and develop a numerical rank that indicates a website's popularity relative to other sites. Rankings can change dramatically and quickly. SimilarWeb.com uses big data technology to estimate websites' unique visitors and the origin of those visits. For example, according to Alexa, 4Shared.com is the 52nd most popular website in Brazil and has the highest percentage of global visitors (21 percent) and according to SimilarWeb, 4Shared.com is the 44th most popular site in Brazil and has the highest percentage of unique visitors (33 percent). Both the Alexa rankings and SimilarWeb data that appear in this document are current as of November 17, 2016.

[13] See Google Transparency Report, available at <https://www.google.com/transparencyreport/removals/copy-right/searchdata/domains/?id=4shared.com>

[14] 4Shared has been identified as one of the largest and most profitable direct download cyberlockers that facilitate infringement. NetNames & Digital Citizens Alliance, "Behind The Cyberlocker Door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions," Sept. 2014, available at <http://www.digital-citizensalliance.org/cac/alliance/content.aspx?page=cyberlockers>. 4Shared.com disputes the allegations made in the report.

BEEVIDEO.TV

BeeVideo is an application that facilitates the viewing of allegedly infringing movies and television shows on smart TVs through set-top boxes, and on mobile devices. The app is available through the BeeVideo.tv website portal. BeeVideo has been downloaded more than 12 million times and once downloaded allegedly provides unlimited unauthorized access to infringing content. The developer and operator of BeeVideo is allegedly based in China.

BOOKFI & LIBGEN

BOOKFI.NET and **LIBGEN.IO** also operating alleged mirror sites as **LIBGEN.INFO**, **BOOKFI.ORG**, **BOOKZZ.ORG**, **BOOKER.ORG**, **BOOKSC.ORG**, **BOOK4YOU.OR**, and **BOOKOS-Z1.ORG**

Bookfi.net and Libgen.io reportedly make available for download millions of books and other publications, a significant number of which are distributed without the consent of copyright holders. Bookfi is allegedly a mirror site of Libgen.^[15] These sites, and other mirror sites, reportedly make it possible to download—all without permission and without remunerating authors, publishers or researchers—copyrighted books by commercial publishers and university presses; scientific, technical and medical journal articles; and publications of technological standards. Information about the registrants and operators of the Bookfi and Libgen family of sites is obscured but Libgen is allegedly based in Russia. Bookfi.net is hosted in the Netherlands and brings in revenue through gift card donations. Libgen has been the subject of court-ordered enforcement action in the United Kingdom, but continues to operate.

EXTRATORRENT

EXTRATORRENT.CC, formerly **EXTRATORRENT.COM**, also displays through official and unofficial mirror sites such as **ETMIRROR.COM**, **ETPROXY.COM**, **EXTRATORRENTONLINE.COM**, and **EXTRATORRENTLIVE.COM**

ExtraTorrent has appeared on the Notorious Markets List since 2013 and continues to benefit from Ukraine's status as a haven for online piracy. In addition to allegedly infringing content, ExtraTorrent has also been identified as a source of malware. Despite being subject to several enforcement actions, it maintains a global Alexa rank of 207, and rankings in India, Pakistan, and China of 170, 19, and 319, respectively. This illustrates the broad impact that sites facilitating infringement can have on geographically diverse markets. The United States encourages the Government of Ukraine to take lasting action against those who operate Extratorrent and similar sites within Ukraine's jurisdiction.

[15] A "mirror site" is a website that is a proxy or clone of an original pirate site that may offer the same, new, or cached infringing content as the original. Some mirror sites are designed to spread malware or steal personal information. Mirror sites can complicate or delay sustained enforcement against the original pirate site.

GONGCHANG.COM

The business-to-business (B2B) e-commerce platform GongChang is reportedly one of several online markets in China that are well-known for the sale of counterfeits, including counterfeit security tags that retailers affix to products as part of a shoplifting prevention system. The GongChang platform specializes in industrial products and servicing manufacturers and retailers. Counterfeit security tags may help give an appearance of authenticity to counterfeit goods or they may fail to alert retailers who believe their goods are protected, increasing the likelihood that shoplifting will go undetected. The sale of these counterfeits at the B2B level illustrates how significant quantities of counterfeit inputs can enter global supply chains.

MOVSHARE GROUP

Operating as **NOWVIDEO.SX**, **WATCHSERIESFREE.TO**, **VIDEOWEED.ES**, **NOVAMOV.COM**, **NOWDOWNLOAD.CH**, **DIVXSTAGE.TO**, and **MOVSHARE.NET** among others

This group of affiliated and extremely popular sites, with ties to Switzerland, Sweden, France, the Netherlands, Panama, and other countries, reportedly uses multiple technologies to make available countless unauthorized copies of movies, games, music, audiobooks, software, and sporting event broadcasts. These cyberlockers, linking sites, forums, and streaming sites all work together to facilitate global distribution of allegedly infringing content. The sites are said to generate revenues through advertising and premium membership or subscription fees, and to compensate users for uploading popular infringing content. Several sites reportedly engage in domain hopping to evade law enforcement and work around search engine demotions to rise to the top of search engine results. Right holders report that Nowvideo and others in the Movshare group are entirely unresponsive to takedown notices.

MP3VA.COM

This site is one of several based in Russia and Ukraine that allegedly engages in the unauthorized sale of U.S. sound recordings. The site attracts more than 860,000 visits a month, principally from the United States, United Kingdom, and India. It has the look and feel of legal music download sites but sells tracks for pennies. MP3VA's FAQ page misrepresents the legality of its operations and purports to have a license from Avtor, a rogue Ukrainian collecting society. However, the site's music download sales are not authorized and authors are not paid. Major U.S. credit card and payment processors no longer support the site. The hosting provider is located in Russia and the operators appear to be located in Ukraine.

MUABAN.NET

Muaban is one of several Vietnamese e-commerce platforms nominated this year. Although this Vietnam-based online marketplace facilitates sales of legitimate goods, stakeholders have identified this site, which has over 3 million page views each month, as one that also offers counterfeit apparel and footwear. Muaban does not appear to have an effective mechanism to remove counterfeit listings.

MYEGY.TO

Founded in 2005, MyEgy is one of the largest marketplaces for infringing video game and other copyrighted content in the Middle East. Stakeholders report that hundreds of new links to infringing video game files are posted to the site daily and that the operator is unresponsive to takedown requests. This linking site was created by an anonymous web developer in Egypt, where it is regularly among the most popular sites. The MyEgy site is in Arabic and content is available in both Arabic and English. The site is hosted in Russia and, like five other listed sites this year, uses the country code top-level domain of Tonga (.to).

NANJING IMPERIOSUS TECHNOLOGY CO., LTD

Also operating as **DOMAINERSCHOICE.COM**

Nanjing Imperiosus, based in China, is reported to disproportionately provide services to illegal online pharmacies. Counterfeit pharmaceuticals sold through illegal online pharmacies cause damage to the reputation of brands and to legitimate pharmacies, and may put consumers at risk. This year, Nanjing Imperiosus is reportedly selling domain name registration services to more than 2,300 known illegal online pharmacies, far surpassing the previously-listed registrar, Rebel. These known illegal online pharmacies make up almost 10 percent of Nanjing's total domain count, and some are registered directly to the domain name registrar operator, Mr. Stefan Hannsman, a German national.^[16] There are roughly 900 companies with registrar accreditation, but based on stakeholder reports, just seven registrars reportedly provide domain names to 50 percent of illegal online pharmacies. Stakeholders also report that most registrars have policies that prohibit domain names from being used in furtherance of criminal activity, and they act on complaints as appropriate to suspend or lock domain names of illegal online pharmacies. The excessively high number of illegal online pharmacies serviced by Nanjing Imperiosus suggests that it neither has nor follows such a policy. As of December 12, 2016, the Internet Corporation

[16] Nanjing Imperiosus had 24,375 domains as of July 2016. See <https://features.icann.org/compliance/regis-trars-list> for registrar counts. ICANN cites 5mg-cialis20mg.com, acheterdutadalafil.com, viagra-100mgbestprice.net, and 100mgviagralowestprice.net as examples of domains registered to Hansmann and his company. See ICANN, Notice of Breach of Registrar Accreditation Agreement, available at https://www.icann.org/uploads/compliance_notice/attachment/873/serad-to-hansmann-12oct2016-en.pdf

for Assigned Names and Numbers (ICANN) has suspended Nanjing Imperiosus' ability to create or initiate inbound transfers of new Registered Names for 90 days.^[17]

POBIERAMY24.PL, DARKWAREZ.PL, CATSHARE.NET, & FILESHARK.PL

These sites all share connections to Poland and together represent a major hub of allegedly infringing video games. Pobieramy24, Darkwarez, and Fileshare all use the country code top-level domain for Poland. Between the four sites, over a hundred thousand links to allegedly infringing video game files are indexed, directing users to over a hundred thousand files stored in cyberlockers.

PRIVATE LAYER-HOSTED SITES

Including **THE-WATCH-SERIES.TO** and **PROJECTFREE-TV.TO**

This group of websites, all hosted by Switzerland- and Panama-based Private Layer, is an example of the popularity among a wide variety of pirate sites of certain Swiss hosting services. Switzerland has announced plans to close a loophole in its law that restricts enforcement against pirate sites. However, at this time, right holders report that Switzerland is an increasingly popular host country for such sites. Other listed and nominated sites, including Putlocker, 1337x.to, Primewire.ag, and Nowvideo.sx may also be hosted by Private Layer but are using reverse proxy services to obfuscate the true host from the public and from law enforcement.

PUTLOCKER.CH

Formerly **PUTLOCKER.IS**

Putlocker appears again on the List as one of the most-visited video streaming sites in the Asia-Pacific region for allegedly pirated movies and television shows. Streaming sites, such as Putlocker, are overtaking torrent and other piracy sites as the primary mode of movie and television piracy.^[18] The operator of Putlocker is believed to be based in Vietnam and appears to be taking actions to evade enforcement measures. For example, in 2016 Putlocker hopped domains from the country code top-level domain of Iceland (.is) to Switzerland (.ch) and started using reverse proxy services to obscure the location of its hosting provider.

[17] See ICANN, Notice of Suspension of Registrar's Ability to Create New Registered Names or Initiate Inbound Transfers of Registered Names, available at https://www.icann.org/uploads/compliance_notice/attachment/885/serad-to-hansmann-24nov16-en.pdf

[18] One study by content protection company MUSO estimates that three quarters of all pirated movie and TV-show traffic (57 billion of 78 billion site visits across 14,000 of the largest global piracy sites) went to streaming sites. See MUSO, Global Film & TV Piracy Insights Report 2016, available at <https://www.muso.com/magazine/press-release/musos-global-film-tv-piracy-report-2016-released/>

RARBG.TO

This site, located in Bosnia and Herzegovina, was nominated by commenters from the movie, television, and music industries and is quickly gaining popularity as prominent competitor sites like KickassTorrents and Torrentz.eu have closed. Rarbg was started almost a decade ago to target the Bosnian market but now has a global user base. It reportedly has changed hosting services to prevent shutdowns in recent years. Although Rarbg has been the subject of enforcement and voluntary actions in the United Kingdom and Portugal, it still continues to operate.

RUTRACKER.ORG & RAPIDGATOR.ORG

Formerly **TORRENTS.RU**

Commenters from the book publishing, movie, and music industries all nominated Rapidgator for inclusion on this year's List. Rapidgator is hosted in Russia but primarily provides allegedly infringing content to users outside of the country. Rapidgator employs rewards and affiliate schemes to compensate users based on downloads and sales of new accounts. Operators of the site allegedly net an estimated \$2 million annually. Rutracker, hosted in and operated from Russia, is a BitTorrent portal with more than 13 million active accounts. The site is currently one of the most popular in the world and a top site in Russia, with an Alexa ranking of 20.

TAOBAO.COM

The Taobao.com e-commerce platform is an important concern due to the large volume of allegedly counterfeit and pirated goods available and the challenges right holders experience in removing and preventing illicit sales and offers of such goods. Taobao is a consumer-to-consumer marketplace that offers "hundreds of millions of product and service listings." In 2014, Taobao ranked as China's largest online shopping destination by gross merchandise volume and the Mobile Taobao App stood as the top Chinese e-commerce app in March 2015.^[19] According to Alexa rankings, Taobao.com is among the 15 most popular websites globally and among the top 5 websites in China. Right holders in the United States and internationally continue to report serious challenges to reducing high levels of counterfeit and pirated goods on Taobao. Longstanding obstacles to understanding and utilizing basic IP enforcement procedures continue unabated. Right holders report that initial attempts to report IPR infringement are refused inconsistently; denials of takedown requests contain little to no justification or guidance on how the right holder may amend its notification to get results; error messages stall or prevent use of IP complaint systems; pertinent communications to right holders are not translated from Chinese; and

[19] Alibaba Group Corporate Overview available at http://alibabagroup.com/assets2/pdf/Alibaba_Group_Corporate_Overview_Eng.pdf

broken hyperlinks prevent direct communication between right holders and Taobao sellers.

Taobao's parent company, the Alibaba Group (hereinafter Alibaba), reportedly has taken steps to address right holders' concerns on Taobao by, for example, establishing internal offices focused on IPR and appointing experienced officers to guide these efforts, addressing the misuse of brand keywords and blurred trademarks in product images, and developing technology to prevent counterfeit sellers from re-opening. Alibaba claims it has proactively removed more than 380 million product listings and closed approximately 180,000 Taobao stores in the 12 months ending August 2016. Prospectively, Alibaba has announced a shift from a Four Strike to a Three Strike Policy and the launch of a Joint Force System that is intended to expand proactive enforcement efforts. The Good Faith Program reportedly is intended to provide a more effective and efficient avenue for participating right holders to enforce their IPR, and participation has grown with Alibaba's support. Unfortunately, the Good Faith Program reportedly remains out of reach for the vast majority of right holders, particularly SMEs, due to stringent eligibility criteria that must be met and maintained over a period of time. There is a reported significant disparity between the timeliness and effectiveness of Alibaba's responses to complaints submitted by right holders in the Good Faith Program and those outside the program.

While recent steps set positive expectations for the future, current levels of reported counterfeiting and piracy are unacceptably high. Not only do counterfeit and pirated goods pose a grave economic threat to U.S. creative and innovative industries, undermining the Chinese and global market for legitimate U.S. products, substandard counterfeits such as auto parts pose a potential public health threat to unsuspecting consumers. One large motor vehicle manufacturer reported that at least 95 percent of the merchandise bearing its company's brand names and trademarks found on Alibaba platforms is suspected to be counterfeit.

Given the dominance of Chinese sellers on Alibaba's platforms, it is critical that the Chinese Government support these efforts through measurable enforcement efforts across China and stronger domestic IPR reforms identified in previous Special 301 reports such as the development of its E-Commerce law. In 2017, the United States will closely monitor the implementation and effectiveness of the set of prospective actions described in Alibaba's Notorious Markets List submission. As Alibaba moves forward with its plans to further reform and enhance its enforcement tools across platforms, the recommendations highlighted in the 2015 List remain valid, namely: (1) simplifying processes for right holders to register and request enforcement action; (2) making good faith takedown procedures generally available; and (3) reducing Taobao's timelines for takedowns and issuing penalties for counterfeit sellers. In addition, the United States welcomes increased efforts to further refine and identify metrics to assess objectively the scale of infringing products sold over Taobao and other Alibaba platforms, as well as additional attention to the needs of SMEs, such as by devoting resources to provide proactive takedowns tailored to assist SMEs.

Senior corporate representatives at Alibaba have noted that, "[Alibaba has] the responsibility to be the global leader in anti-counterfeiting... the scale, . . . the data and . . . the commitment." The U.S. Government remains committed to working with Alibaba and right holders to find effective solutions to curb infringing activity on Taobao and other Alibaba platforms, and to resolve the concerns raised by right holders.

THE PIRATE BAY

THEPIRATEBAY.ORG most recently operating as **THEPIRATEBAY.SE**, formerly registered at the following domains: .GL, .IS, .SX, .AC, .PE, .GY, .GS, .AM, .LA, .GD, .MN, .VG, .FM, .SH, .MU, .TW, and .MS

The Pirate Bay returns to the list of notorious markets after an unfortunately brief hiatus. Despite enforcement actions around the world and drawn-out legal battles against its operators, The Pirate Bay is of symbolic importance as one of the longest-running and most vocal torrent sites for admittedly illegal downloads of movies, television, music, and other copyrighted content. Internet browsers reportedly regularly detect and warn of malicious content on the site, including malware that installs harmful programs and phishing attempts to reveal personal information. The site launched its own browser in an apparent effort to circumvent court-ordered enforcement in more than ten countries. The Pirate Bay has allegedly had more than a dozen domains hosted in various countries around the world, applies a reverse proxy service, and uses a hosting provider in Vietnam to evade further enforcement action.

UPLOADED.NET

Formerly **UL.TO** and **UPLOADED.TO**

This cyberlocker reportedly provides access to a broad range of unauthorized copies of copyright-protected content such as books, movies, television, and music, including pre-release music. Uploaded uses a combination of multi-tiered subscriptions, a referral program, and a rewards scheme to generate revenue,^[20] to incentivize unauthorized sharing of popular copyrighted content, and to expand its user base. For example, the site pays rewards to users based on large file sizes, such as those for movies and television, and based on the number of times a file is downloaded, paying more when the downloads come from “Top-Countries.” The operator allegedly employs multiple IP addresses, domain names, and server locations to evade law enforcement. In 2016 a German court found an Uploaded operator liable for infringing content shared by its users because it failed to take proactive measure to prevent the same infringing works from being re-uploaded and made available for download again.^[21] Uploaded is owned by a Swiss company and is hosted in the Netherlands.

[20] In 2014, one report estimated that Uploaded generated approximately \$6.6 million in annual revenue through premium accounts and advertising. See <https://www.netnames.com/assets/shared/whitepaper/pdf/dca-netnames-cyber-profitability-1.compressed.pdf>

[21] LG München I, Az. 21 O 6197/14

VIBBO.COM

Formerly **SEGUNDAMANO.ES**

Vibbo is one of the most popular e-commerce platforms in Spain, connecting many users to a wide variety of products and services. While the terms of use expressly prohibit activity that violates IPR, some sellers reportedly use the platform to sell and distribute counterfeit security tags and circumvention devices and services. Circumvention devices and services break the technological protection measures in game consoles and handheld devices to enable unauthorized uses or the copying of game software. In many countries, including Spain, this is in direct violation of the law. Some sellers also openly advertise that their games and services are pirated. Right holders report that Vibbo is largely non-responsive to notices of infringing activity.

VK.COM

Also known as **VKONTAKTE.COM**

Nominated again this year, VK is one of the most popular sites in the world and continues to operate as an extremely popular social networking site in Russia and neighboring countries. VK reportedly facilitates the distribution of copyright-infringing files. Social networking sites can serve as a uniquely valuable communication platform, enabling beneficial commercial, cultural, and social exchanges. Most successful social networking sites do so in ways that do not involve the active facilitation of copyright infringement. Reports that VK is taking steps to address piracy are encouraging. In particular, VK has reached licensing agreements with major record companies, has taken steps to limit third party applications dedicated to downloading infringing content from the site, and has experimented with content recognition technologies. Despite these positive signals, VK reportedly continues to be a hub of infringing activity and continues to be listed pending the institutionalization of appropriate measures to promote respect on its platform for IPR of all right holders, not just those with whom it has contracts, that are comparable to those measures used by other social media sites.

YOUTUBE-MP3.ORG

As detailed in the issue focus above, stream ripping is a growing threat to musicians, record labels, and digital music delivery models. Youtube-mp3 is one of the most popular stream ripping sites with 4.8 billion visits in the past year, a high global Alexa rating of 332, and high country-specific Alexa ratings in Mexico (77) and Turkey (111). Youtube-mp3 allegedly accounts for about 40 percent of the world's stream ripping activity, and the music industry estimates that it generates hundreds of thousands of dollars a month in revenue through advertising. The operator is located in Germany and legal action in multiple jurisdictions is ongoing.

Physical Markets

The Internet has brought about a global revolution in the authorized and unauthorized distribution of films, music, software, video games, and books. The Internet also makes available innumerable sites that facilitate the distribution of legitimate and counterfeit products to consumers worldwide. In some countries, infringing physical media (including CDs, DVDs, video game cartridges, pre-loaded computer hard drives, and other storage devices) continues to be prevalent. In most countries, online distribution of, or access to, unauthorized copyright-protected content has largely replaced physical distribution of media. Physical markets, however, remain a primary distribution channel for counterfeits in much of the world.

As in past years, copyright-intensive industries nominated online markets more than physical markets. Several commenters focused exclusively on notorious online markets due to the rise of digital distribution and online infringement. In contrast, trademark-based industries continued to nominate both online and physical marketplaces.

In a global environment, basic enforcement against unscrupulous retailers will not be sufficient to reduce the flow of counterfeit products. To address 21st century challenges, governments need targeted, modernized enforcement tools including:

- enhanced criminal penalties for particularly serious cases, such as trafficking in counterfeit trademark products that threaten health and safety;
- robust border enforcement authority to interdict small consignment shipments, such as those sent through postal or express courier services;
- asset forfeiture, a tool which can be used to reach the custodians of locations where infringing products are sold and stored;
- 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;
- criminal procedures and penalties for trafficking in counterfeit labels and packaging; and
- customs and criminal authorities to detain and seize counterfeit and pirated goods entering into and exiting from Free Trade Zones.

Another key to reducing piracy and counterfeiting lies in the ability to influence demand and redirect the consumers who knowingly participate in illicit trade to legitimate alternatives.

As in past years, several commenters continue to identify China as the primary source of counterfeit products. Some Chinese markets, particularly in larger cities, have adopted policies and procedures intended to limit the availability of counterfeit merchandise, but these policies are not widely adopted, and enforcement remains inconsistent. At the same time, some online markets are cooperating with law enforcement on counterfeiting and piracy operations offline. It is reported that in many instances, Chinese authorities engage in routine enforcement actions in physical markets. The United States welcomes these efforts and recommends their expansion to combat more effectively the scale of the reported problem in China, with a special focus on the following key markets:

Baiyun Leather Goods Market Guangzhou, China
Jin Long Pan Foreign Trade Garment Market Guangzhou, China
Chenghai District Shantou, China
Wu Ai Market Shenyang, China

China is reportedly the global hub for manufacturing counterfeits, with Guangdong Province at its epicenter. At the multi-story Baiyun Leather Goods Market in Guangzhou, vendors reportedly sell a wide range of counterfeit leather goods and other articles, including to a cross section of foreign buyers. Also in Guangzhou, shops in the Jin Long Pan Foreign Trade Garment Market allegedly sell low-quality, relatively inexpensive counterfeit versions of U.S. and other branded apparel and footwear on a wholesale scale for export to Africa and the Middle East, in particular. Chenghai District, also in Guangdong Province, is reportedly an egregious counterfeiting zone where factories manufacture counterfeit toys and consumer goods for wholesalers. Wu Ai Market, located in Shenyang, Liaoning Province, is Northeast China's largest wholesale market and is reportedly the home of large-scale marketing of pirated and counterfeit goods at a variety of price points infringing on a wide range of international brands.

Cheng Huan Cheng International Auto Parts Market

Beijing, China

At the Cheng Huan Cheng International Auto Parts Market, a broad array of apparently counterfeit car parts and car-related articles are sold, potentially raising safety concerns for the driving public. Reportedly, at least some of the items attract customers by offering prices that are a small fraction of the price of authentic goods. Allegedly counterfeit articles are labeled with well-known mass-market brands as well as high-end luxury brands.

Silk Market

Beijing, China

Many retail vendors at the Silk Market reportedly distribute counterfeit consumer products. Despite posted signage indicating that the Silk Market should be a model of IPR enforcement, multiple vendors reportedly sell counterfeit goods at a small fraction of the price of authentic articles, and openly assert that the fakes are of high quality. Such conditions are reported to persist despite welcomed efforts by Chinese authorities to work with management and engage in enforcement actions, and even though some right holders have successfully sued the market's operators. It appears that past civil and administrative enforcement efforts, although imposing some costs, have not actually ended infringement.

Worldwide, from the Americas, Africa, Eastern Europe, and Southeast Asia, Chinese-origin counterfeit goods from these and other Notorious Markets in China reportedly find their way into markets, businesses, and homes. In some cases, parties with ties

to China manage the wholesale and retail distribution channels that facilitate the flow of counterfeit merchandise, including to notorious markets in places such as Lagos, Nigeria; Ciudad del Este, Paraguay; and Bangkok, Thailand.

Computer Village Market, Ikeja Lagos State, Nigeria
Oke-Arin & Apongbon Markets Lagos Island, Nigeria

Computer Village Market at Ikeja is the largest and most well-known market for counterfeit computer products and accessories in Nigeria. Raids by regulators continue, but store owners allegedly collude to thwart enforcement efforts. Up to an estimated 80 percent of the wide variety of electronic products at this market are allegedly counterfeit. Nearby, Oke-Arin and Apongbon Markets are reportedly known for counterfeit soft drinks, spirits, and popular consumer goods. Regulatory agencies have conducted raids and made some arrests, but the chaotic nature of these densely populated markets make enforcement difficult. Nigerian authorities face challenges in allocating sufficient resources and building the necessary infrastructure to engage in effective import controls against the tide of foreign-manufactured counterfeit products. The situation in Nigeria exemplifies why both effective enforcement at the point of import and at the country of export are essential in stopping the flow of counterfeit and pirated goods.

Ciudad del Este

Paraguay

Ciudad del Este has been named in either the List or the Special 301 Report for over 15 years. The border crossing at Ciudad del Este and the city itself have long been known as a regional hub for the distribution of counterfeit and pirated products in the Brazil-Argentina-Paraguay triple frontier and beyond. Regional organized crime groups are reportedly responsible for the bulk of counterfeit and copyright-infringing goods in Ciudad del Este. One private commercial group reports it has made efforts to legitimize its import activities in Ciudad del Este. However, despite the Government of Paraguay's stated goals to transform Ciudad del Este into a legitimate marketplace, including commitments to take specific steps to improve IPR protection and enforcement, effective seizures at Ciudad del Este have declined due to long lag times in obtaining warrants and low prosecution rates.

Galeria Pagé, Mercado Popular 25 de Março

Sao Paulo, Brazil

The center of Sao Paulo city—including the indoor Galeria Pagé mall, the open-air Mercado Popular 25 de Março, and smaller markets in the Bras and Santa Ifigenia neighborhoods—is reportedly the epicenter of counterfeits and piracy in the state and one of the most notorious examples of counterfeit markets in the country. According to the Sao

Paulo Federation of Industries, contraband, pirated, counterfeit, and stolen goods cost the state of Sao Paulo approximately \$4.4 billion and 111,500 formal sector jobs in 2015. Since the 2015 List, police have conducted at least two significant operations, including dismantling a large center of pirated CD and DVD production. The United States encourages the newly elected Mayor of Sao Paulo to commit to building a “City Free of Piracy.”

Harco Glodok & Mangga Dua

Jakarta, Indonesia

Harco Glodok is Indonesia’s largest trade center for consumer electronics and related goods. This market reportedly serves as the retail distribution point for a complex piracy and counterfeiting network. The Government of Indonesia’s efforts over the past few years have failed to rid this otherwise legitimate market of IPR-infringing goods and services. USTR urges the Indonesian Government, including the recently announced anti-piracy task force under the Creative Economy Agency, to launch a sustained, coordinated, and effective effort to tackle widespread counterfeiting and piracy at Harco Glodok and elsewhere. USTR also urges the Indonesia Government to take steps to address the broad array of allegedly counterfeit goods at Mangga Dua, another popular market in Jakarta.

Ninh Hiep

Hanoi, Vietnam

Nihn Hiep is one of the most well-known and largest retail markets in Hanoi. This market has been the target of raids and seizures of both counterfeit goods and labels. USTR urges the Government of Vietnam to continue to take enforcement actions to deter sales of counterfeit goods and labels at this and other nominated markets in Vietnam.

La Salada

Buenos Aires, Argentina

La Salada is well-known in South America as one of the largest black markets for IP-infringing goods. There are roughly 5,000 stalls that attract hundreds of thousands of shoppers when the market is open. Considerable quantities of a wide variety of counterfeit goods are reportedly sold at the market and re-sold throughout the city, country, and region. Most goods appear to be imported from China but some local assembly and finishing may also take place in and around La Salada. Large-scale raids related to counterfeiting or piracy have not occurred over the past year.

Gandi Nagar Delhi, India
Burma Bazaar Chennai, India
Kashmere Gate Delhi, India

Numerous markets in India have appeared in past Lists, with no identified meaningful, effective response by the Indian government. In the 2016 Notorious Markets process, stakeholders highlighted dozens of markets across India for counterfeit apparel, footwear, automobiles and auto parts, electronics, leather goods, mobile phones, CDs and DVDs, and luxury goods. Gandhi Nagar is highlighted for counterfeit apparel while Burma Bazaar is highlighted for a wide variety of counterfeit goods and pirated media discs. Kashmere Gate is an example of a market allegedly selling counterfeit auto parts. The United States continues to raise the importance of IPR protection and enforcement with India, underscoring the need to combat counterfeiting and piracy in both online and physical markets. The United States encourages India to take sustained and coordinated enforcement action at these and other previously-listed markets, as well as numerous other nominated markets.

Tepito Mexico City, Mexico
San Juan de Dios Guadalajara, Mexico

Significant levels of piracy and counterfeiting reportedly continue in Tepito, San Juan de Dios, and dozens of other markets across Mexico. The United States encourages Mexico to continue coordinated law enforcement efforts, including against high-level targets in the distribution chain, to reduce the availability of counterfeit and pirated product in markets across the country. We further encourage Mexico to empower customs officials to interdict infringing imports on their own authority and to enforce against counterfeit and pirated goods moving in-transit.

MBK Mall
Bangkok, Thailand

IPR holders face a difficult environment in Thailand due to the large number of markets offering counterfeit and pirated goods and services, and a relative lack of enforcement. We appreciate the Government of Thailand's efforts over the past year, including the enforcement statistics it provided in response to the Federal Register Request and steps to increase coordination among enforcement agencies. However, reports indicate that pervasive counterfeiting and piracy continue in most of the previously-listed markets, particularly the MBK Center (Bangkok), where infringing offerings range from counterfeit headphones and Bluetooth speakers to apparel and footwear to pirated DVDs. Additionally, Rong Kluea near the border with Cambodia, appears to be the largest wholesale and retail market for counterfeit goods in Thailand. USTR requests that Thai authorities conduct sustained, coordinated enforcement actions at the numerous nominated markets in

which counterfeiting and piracy are rampant with a view to deterring such activity. USTR will continue to monitor the situation. ■

Public Information

The 2016 Notorious Markets List is the result of the sixth OCR of Notorious Markets, which USTR initiated on Aug 25, 2016, through a Federal Register Request for Public Comments. The request and responses are available at WWW.REGULATIONS.GOV, Docket Number USTR-2016-0013. USTR developed the 2016 List in coordination with the Federal agencies represented on the Special 301 Subcommittee of the Trade Policy Staff Committee (TPSC). Information about Special 301, the TPSC, and other intellectual property rights-related processes and issues is available at [HTTPS://USTR.GOV/ISSUE-AREAS/INTELLECTUAL-PROPERTY](https://ustr.gov/issue-areas/intellectual-property).

To assist U.S. right holders and consumers who confront IPR infringement online, the U.S. Government continues to expand the tools available on WWW.STOPFAKES.GOV, including by providing links to infringement reporting mechanisms at a number of popular online retailers and markets. These resources are available at WWW.STOPFAKES.GOV/BUSINESS-TOOLS/RETAILER-REPORTING. Victims and interested parties may report IPR theft to U.S. law enforcement agencies either through a link at WWW.STOPFAKES.GOV or directly at WWW.IPRCENTER.GOV/REFERRAL. ■



EXECUTIVE OFFICE OF THE PRESIDENT

OFFICE *of the* UNITED STATES TRADE REPRESENTATIVE

600 17th Street NW, Washington, D.C. 20006

(202) 395-6121

www.ustr.gov



