OFFICE *of the* UNITED STATES TRADE REPRESENTATIVE

EXECUTIVE OFFICE OF THE PRESIDENT

2017 Out-of-Cycle Review of Notorious Markets

Table of Contents

Overview of the Results of the 2017 Out-of-Cycle Review of Notorious Markets

Commercial-scale copyright piracy and trademark counterfeiting[1] 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 can pose significant risks to consumer health and safety. The Notorious Markets List (List) highlights prominent and illustrative examples of online and physical marketplaces that reportedly engage in, facilitate, turn a blind eye to, or benefit from substantial piracy and counterfeiting. A goal of the List is to motivate appropriate action by owners, operators, and service providers in the private sector of these and similar markets, as well as governments, to reduce piracy and counterfeiting.

USTR highlights the following marketplaces because they exemplify global counterfeiting and piracy concerns and because the scale of infringing activity in these marketplaces can cause significant harm to U.S. intellectual property (IP) owners, consumers, legitimate online platforms, 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.

The List includes several previously identified markets because owners, operators, and governments failed to address previously stated concerns. 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 IP-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. In some cases, online markets in the 2016 List 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 countries concerned.

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

The List is not an exhaustive account of all physical and online markets worldwide in which IP infringement may take place. The List 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 on or around April 30 of each year (please refer to the Public Information section at the end of this document).

The Office of the United States Trade Representative (USTR) developed the List under the auspices of the annual Special 301 process.[2] USTR solicited comments through a Request for Public Comments published in the Federal Register (WWW.REGULATIONS.GOV, Docket Number USTR-2017-0015). The List 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 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.

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

Positive Developments since the 2016 Out-of-Cycle Review of Notorious Markets

Since the release of the 2016 Notorious Markets List (2016 List) on December 22, 2016, some market owners and operators undertook notable efforts to address widespread availability of pirated or counterfeit goods in their 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 2017 List, to engage in sustained and meaningful efforts to combat piracy and counterfeiting.

In 2017, the operator of Sharebeast pled guilty in United States federal court to the illegal distribution of copyrighted music and albums on a massive scale following charges by federal prosecutors. Law enforcement in the United Kingdom (UK) and the Netherlands assisted in 2015 with seizures of the Sharebeast and related domain names. Several sites that used the Sharebeast platform and that were previously nominated for inclusion on the List, including Emp3world, Viperial, AlbumKings, AudioCastle, and im1music, have also reportedly shut down.

During the past year, some previously listed online markets have been the subject of successful enforcement efforts. For example, an unauthorized stream ripping site highlighted in the 2016 List, **youtube-mp3.org**,[3] recently shut down as a result of a civil action and other sites have reportedly stopped promoting or allowing unauthorized audio ripping from music videos and legitimate streaming services. Though circumstances exist where stream ripping could be lawful, such as if the content were licensed for that purpose and the conversion were permitted under the legitimate service's terms of use, the operations of many unauthorized stream ripping sites reportedly continue to contribute overwhelmingly to copyright infringement. One such example, **Convert2mp3.net**, appears in the list below.

Nanjing Imperiosus Technology Co., Ltd, which reportedly provided domain name services to illegal online pharmacies, is no longer operating and no longer appears in the List.

[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. Previously-nominated markets are not bolded unless they have also been listed.

The Internet Corporation of Assigned Names and Numbers (ICANN) terminated the Registrar Accreditation Agreement with Nanjing Imperiosus in January 2017 for continued breach of the terms of the Agreement, including failure to provide records to ICANN related to abuse reports.

The previously listed **Putlocker** operation, known for streaming of pirated movies and television shows and formerly operating as Putlocker.is and Putlockers.ch, is no longer functioning, although third party phishing scams may be using the Putlocker name to prey on users. After four years on the List, **Extratorrent** is removed this year as operators announced in May 2017 that they were shutting down Extratorrent and its mirror sites.

Some previously listed online markets reportedly took various measures to prevent and deter infringing activities. Such measures include 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.

Several country code top-level domain (ccTLD) registrars, including for the Spain and European Union (EU) ccTLDs, stepped up efforts this year to enforce their ccTLD policies. For example, Red.es (a public entity) cancelled seven websites with the Spanish ccTLD ".es" following the request of the Spanish Intellectual Property Commission as provided by Spanish law.[4] The United States encourages other countries and ccTLDs registrars to take similar steps.

Again this year, the List highlights online piracy sites that are funded by advertising revenue. According to an independent review of the top 5000 IP Infringing URLs in the United States, EU, and Australia, about 25-30% of advertising on websites posing an IP risk are from major brands.[5] One advertising network based in Canada, WWWPromoter, is reportedly the fastest growing ad network among infringing sites and provides services to notorious markets listed below, including **primewire.ag** and **123movies.to**. In recent years, several governments and private sector stakeholders have developed innovative approaches to disrupting ad-backed

[4] Law 21/2014, 158*ter*(5); *See* Report on the Activities of Section Two of the Intellectual Property Commission (Data as of October 1, 2017), *available at* http://www.mecd.gob.es/cultura-mecd/dms/mecd/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pirateria/2017_3Q_Report-Secc2-CPI/2017_3Q_Report%20Secc2%20CPI.pdf.

[5] *See* https://www.white-bullet.com/quarterly-report/.

funding of infringing sites. In the United Kingdom, the London Police Intellectual Property Crime Unit (PIPCU), with funding from the UK Intellectual Property Office, seeks to cut off advertising revenue to copyright infringing sites. PIPCU maintains an Infringing Website List that advertisers, agencies, adtech platforms, and other intermediaries can consult and decide voluntarily to cease ad placement on those sites.[6] Since 2015, the French Ministry of Culture has facilitated a voluntary Code of Good Advertising Practices for the Enforcement of Copyright and Neighboring Rights between right holders, advertisers, and advertising professionals to contribute to the fight against piracy, promote online creation, and develop confidence in the digital economy.[7] One web browser with global popularity has announced it will launch an ad blocker in 2018 that will affect advertisements that do not fall within the Coalition for Better Ads' "Better Ads Standards," which could also disrupt ad revenue flows to pirate sites.

Regarding physical marketplaces, both Argentina and Thailand have significantly stepped up enforcement and used novel approaches to increase the sustainability of their efforts. In January 2017, with the support of Argentina's national government, Buenos Aires city authorities evicted 2,000 illegal street vendors from the Once neighborhood. The government relocated these street vendors to nearby commercial facilities and provided them with a stipend and a two-month business-training course organized by the Argentine Confederation of Small and Medium-Sized Enterprises. Nearly one-half of the evicted street vendors are now operating legally from two new locations in Buenos Aires. High profile arrests of two alleged leaders and many associates of notorious market **La Salada** in June and October 2017, followed by large-scale enforcement operations in December 2017, have sent a firm message that the Argentine government is cracking down on marketplaces known for counterfeit and pirated goods.

At the direction of the Prime Minister, Thailand has focused enforcement efforts on thirteen previously listed notorious markets as well as other markets throughout the country. From January to September 2017, Thai authorities carried out more than 700 raids and seized almost 150,000 infringing items. Thailand authorities established on-site IP Enforcement Centers in five high-priority shopping areas to enhance timely responses to complaints, visibility

---

[6] *See* https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx.

[7] *See* http://www.culturecommunication.gouv.fr/Documentation/Rapports/Rapport-2015-2016-de-la-Charte-de-bonnes-pratiques-dans-la-publicite-pour-le-respect-du-droit-d-auteur-et-des-droits-voisins.

of enforcement, coordination among Thai enforcement agencies, and cooperation with right holders. Also in 2017, the Thai IP office and other enforcement agencies have worked closely with public and private property owners including by sending formal letters requesting property owners to monitor and warn their tenants to refrain from selling counterfeit and pirated goods.

The International Chamber of Commerce, Business Action to Stop Counterfeiting and Piracy (BASCAP) released in September 2017 a new resource on best practices to combat counterfeiting and piracy challenges for landlords and property owners, governments, and enforcement agencies.[8] For example, the resource includes model lease provisions prohibiting counterfeit and piracy activities that could assist property owners in the physical markets identified in this List.

The United States commends these efforts and encourages its trading partners to continue their individual and cooperative efforts to combat piracy and counterfeiting.

[8] *See* https://cdn.iccwbo.org/content/uploads/sites/3/2017/09/ICC-BASCAP-Landlords-Paper.pdf.

Issue Focus: Illicit Streaming Devices[9]

Global sales and use of illicit streaming devices (ISDs) are growing and pose a direct threat to content creators, sports leagues, and live performances, as well as legitimate streaming, on-demand, and over-the-top media service providers.[10] ISD piracy is the combination of media boxes, set-top boxes, or other devices with piracy applications (apps) that allow users to stream, download, or otherwise access unauthorized content from the Internet. ISDs may be "fully loaded" at the point of sale with an open-source media player, apps, and add-ons configured to access unlicensed content via cyberlockers and streaming websites. Alternatively, the devices may be combined with add-ons after purchase to achieve the same objective. Such add-ons are sold or provided through online markets for accessing infringing content with streaming devices.

ISD piracy denies right holders their ability to control their IP, bypasses the right holders' terms of use, and undermines the licensing fees paid by distributors on which content creators depend. Internet Protocol TV is the fastest growing segment of total revenues in the pay TV landscape, with an increase of more than four percent in market share between 2015 and 2016. The growth of ISDs is a troubling threat to the pay TV and other content industries and undermines incentives for companies to improve services or offer a greater selection of content in more markets. As ISD piracy grows, it is critical for governments and stakeholders to work together to combat this threat to revenues for legitimate methods of distribution for television, movies, sports casting, and other live events. Law enforcement authorities in several foreign jurisdictions have apprehended sellers of pre-loaded devices that allow users to stream pirated content to their TVs[11] and foreign courts have clarified that selling such devices specifically configured for film and TV piracy is illegal under their laws.[12] Some online retailers have taken

---

[9] The Notorious Markets List refers to "illicit streaming devices" instead of "media boxes" because media boxes and set-top boxes have non-infringing uses, whereas ISDs refer to devices that are used to access pirated content.

[10] In their IP Crime and Enforcement Report, the UK government found that use of ISDs is growing with 19 percent of consumers accessing unlicensed materials using ISDs between 2016 and 2017. In North America roughly 6.5 percent of households or 106 million users are accessing known subscription television piracy services. *See* https://www.sandvine.com/downloads/general/global-internet-phenomena/2017/global-internet-phenomena-spotlight-subscription-television-piracy.pdf.

[11] *See* http://www.cornwalllive.com/kodi-boxese-this-is-what-official-piracy-experts-say-about-what-s-legal-and-what-s-not/story-30132149-detail/story.html.

[12] Judgement of 26 April 2017, Filmspeler, C-527/15, ECLI:EU:C:2017:300; Bell Canada et al v. 1326030 Ontario Inc. dba ITVBox.net et al, T-759-16 (2016 FC 612); China Cent. Television v. Create New Technology (HK) Ltd.,

steps to prevent the sale of these devices on their platforms[13] and one popular open-source media player has been forced to defend its brand against becoming synonymous with ISD piracy.[14]

Some ISDs have the look and feel of legitimate services, but pirated content is unlawful regardless of whether it is ultimately streamed to a computer, a television set, or a phone. The ISD piracy ecosystem, including unlawful device sellers and unlicensed video providers and video hosts, stands to bring in revenue of an estimated $840 million a year in North America alone, at a cost to the entertainment industry of roughly $4-5 billion a year.[15] Less money to invest in original programming threatens employment in a broad range of affected industries—movies, premium television, local television, news, international content, sports, live performances, pay-per-view events, and videogames. Unsuspecting users of unofficial add-ons and "builds" are at risk of malware and hackers that exploit ISDs and related services to infect consumers' computers and other devices.[16] Additionally, some seized devices in the UK were found to pose a risk of electrocution or fire.[17] Finally, ISDs may constantly stream and use tremendous amounts of "phantom bandwidth," or transmit data that no one views, resulting in overage charges for subscribers and inefficient network use and poor performance for Internet service providers.[18] In recognition of these threats to the creative community, legitimate streaming services, and consumers, illustrative examples of infringing apps and portals that connect streaming devices to illicit content—**TVPlus**, **TVBrowser** and **KuaiKan—**are added to the 2017 List.

No. CV 15-01869, 2015 WL 3649187 (C.D. Calif. June 11, 2015); Munhwa Broadcasting Corp. v. Create New Technology (HK) Co. Ltd., No. CV 14-4213-RGK-RZK, 2015 WL 9694889 (C.D. Calif. Sept. 2, 2015).

[13] Amazon, Facebook, and Alibaba have reportedly taken such steps. *See* http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA-%20Closed%20Captions-Final.pdf; Alibaba submission to the 2017 Notorious Markets OCR.

[14] *See* https://kodi.tv/article/piracy-box-sellers-and-youtube-promoters-are-killing-kodi.

[15] https://www.sandvine.com/downloads/general/global-internet-phenomena/2017/global-internet-phenomena-spotlight-subscription-television-piracy.pdf.

[16] One estimate notes approximately 200 million video players and streamers are currently running vulnerable software. *See* http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA-%20Closed%20Captions-Final.pdf.

[17] *See* http://www.independent.co.uk/life-style/gadgets-and-tech/news/kodi-boxes-dangers-catch-fire-electrocute-users-streaming-big-vision-a7857226.html.

[18] *See* https://www.sandvine.com/downloads/general/global-internet-phenomena/2017/global-internet-phenomena-spotlight-subscription-television-piracy.pdf.

Results of the 2017 Out-of-Cycle Review of Notorious Markets

The 2017 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 IP protection and enforcement environment in any affiliated country or economy. The List is not an exhaustive inventory 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 that are willing to address piracy and counterfeiting have many options for doing so. Owners and operators of notorious markets 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 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.[19] 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 loopholes that permit operators to evade the law.

USTR continues to monitor markets that no longer appear on the List. Markets may be re-listed if there is a change in circumstances, such as if a website or physical market that ceased to operate because of enforcement or other action resumes unauthorized activities or the corrective actions that merited removal from the List prove inadequate or short-lived. In some

[19] *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.

cases, the situation in a particular market or geographic area presents unique challenges not effectively addressed in this OCR process.

Online Markets[20]

The 2017 List of notorious online markets includes examples of various technologies, obfuscation methods, revenue models, and consumer harm. USTR based its selections not on specific types of technologies but on whether a nominated site or affiliated network of sites reportedly engages in or facilitates substantial piracy and counterfeiting to the detriment of U.S. creators and brand owners, as well as legitimate sellers and distributors.

In addition to facilitating IP 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.[21] Remote Access Trojans (RATs) reportedly use content theft sites as tools to spread malware.[22] It is estimated that between 227,000[23] and 1.3 million[24] new malware files are released every day.

---

[20] 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 15, 2017.

[21] Digital Citizens Alliance, "Enabling Malware," July 2016, *available at* https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0057c1cf-28f6-406d-9cab-03ad60fb50e4.pdf. For more information about consumer protection concerns of pirate sites see Free Trade Commission, "Free Movies, Costly Malware" Apr. 21, 2017 *available at* https://www.consumer.ftc.gov/blog/2017/04/free-movies-costly-malware and public service announcements of fifteen state attorneys general, Mar. 30, 2017 *available at* https://www.youtube.com/playlist?list=PLennsxwCA5VCS7UQG6oWpUIANpX97jcf_.

[22] RATs can be used to download, upload and delete your files (potentially even clearing a hard drive completely); steal passwords, credit card numbers, emails and files; watch you type and log your keystrokes; watch your webcam and save videos; listen in on your microphone and save audio files; take control of your computer; install additional tools including viruses and worms; and use your computer for a distributed denial of service (DDoS) attack. *See* http://www.digitalcitizensalliance.org/clientuploads/directory/Reports/2017_7The_Gateway_Trojan.pdf.

[23] *See* http://www.pandasecurity.com/mediacenter/src/uploads/2017/02/Pandalabs-2017-Predictions-en.pdf.

[24] *See* https://www.symantec.com/security_response/publications/monthlythreatreport.jsp.

1FICHIER.COM

This cyberlocker[25] is hosted in and popular in France and allegedly makes available illegal video game copies and other copyrighted content. According to the video game industry, 1Fichier is responsive to just 2% of takedown notices, one of the lowest response rates of cyberlockers that allegedly host infringing game files. The site derives revenue through a subscription service although some major credit card processors do not service the site due to allegedly illegal activity. Additionally, the site reportedly contains harmful content, including pages that contain suspicious or unknown software.[26]

4SHARED.COM

This cyberlocker site is well-known globally and is particularly popular in Brazil.[27] While 4Shared also provides legitimate file-storage services, the site 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 nearly 68 million removals of 4Shared URLs from results of a prominent search engine since

[25] 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.
[26] Google, Safe Browsing site status available at https://transparencyreport.google.com/safe-browsing/search.
[27] 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 69th most popular website in Brazil which has the highest percentage of global visitors (22 percent) and according to SimilarWeb, 4Shared.com had more than 57 unique monthly visitors and is the 82nd most popular site in Brazil which has the highest percentage of unique visitors (31 percent). Both the Alexa rankings and SimilarWeb data that appear in this document are current as of January 2, 2018.

June 2011, more than any other domain.[28] 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.[29] 4Shared is registered to an entity in the British Virgin Islands and hosted by the subsidiary of a Cyprus-based parent company.

CONVERT2MP3.NET

Convert2MP3.net is one of the most popular stream-ripping sites worldwide and is highlighted this year as an example of the stream-ripping phenomena that continues to threaten legitimate streaming audio and video services, music performers, and composers.[30] As the name of the site suggests, users can use the embedded software to convert authorized video streams into allegedly unauthorized downloads from user generate content sites such as YouTube and DailyMotion. The site includes a search function that allows users to search for video titles of copyright-protected music videos. Convert2MP3.net does not appear to have permission from YouTube or other sites and does not have permission from right holders for a wide variety of music represented by major U.S. labels.

DHGATE.COM

This Chinese business-to-business e-commerce platform enables small- and medium-sized businesses in China to sell more than 33 million product listings to customers overseas. Over most of the last eight years, right holders have consistently reported challenges with a wide variety of counterfeit or copyright-infringing consumer goods on DHGate and continued to do so

[28] See Google Transparency Report, *available at* https://transparencyreport.google.com/copyright/explore?copyright_data_exploration=ce:domain;size:10&lu=copyright_data_exploration. Other nominated and previously nominated sites appear in the top 50 including **rapidgator.net**, **uploaded.net**, chomikuj.pl, zippyshare.com, **torrentz.eu**, **ul.to**, **torrentdownloads.me**, limetorrents.com, **extratorrent.cc**, **catshare.net**, **thepiratebay.se**, and **bitsnoop.com**.

[29] 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.digitalcitizensalliance.org/cac/alliance/content.aspx?page=cyberlockers. 4Shared.com disputes the allegations made in the report.

[30] For a description of stream ripping, see the 2016 Notorious Markets List.

this year. The site is also reportedly a leading online marketplace for the sale and distribution of counterfeit and pirated academic textbooks, with deliveries made in small parcels or via third party sellers. DHGate reports that it reached out to nominators to address concerns, including regarding difficulties in filing IP complaints. USTR urges DHGate to work closely with right holders to address their considerable concerns.

DOPEFILE.PK

After the U.S. Department of Justice shut down Sharebeast, uploaders of infringing music files have increasingly turned to Dopefile as a cyberlocker source for their allegedly infringing websites. The site's revenue sources include advertising and pay-per-install of third party applications. The hosting provider is located in Bulgaria, the registrant or operator is located in Pakistan and uses the Pakistan country-code top-level domain. Dopefile has the highest country rankings in Angola, South Africa, and Nigeria.

FIRESTORM-SERVERS.COM

Also directing from **FSTORM.CC**

Firestorm-Servers is an example of an unauthorized third-party server, known as a "pirate" server or "grey shard," that infringes on the copyrights and circumvents the technological protection measures of "free-to-play" video games. This particular site is popular in France and the hosting provider is located in Russia.

FMOVIES.IS

Also operating as **FMOVIES.SE** and **FMOVIES.TO**

Fmovies allegedly streams unauthorized movies and television series directly to computer desktops or through apps on streaming devices. The addition of Fmovies to the List is one example of the increasing challenges of streaming piracy.[31] The site is hosted in Sweden and has

[31] From January 2016 to December 2016, 77.7bn visits to piracy streaming websites were recorded, 34.0% of this piracy activity was via mobile devices. *See* https://www.muso.com/magazine/muso-releases-2017-global-film-tv-insight-report/.

been the subject of enforcement action by a Denmark District Court but is rising in popularity and is particularly popular in India. The site operates under several ccTLDs.

GOSTREAM.IS

Associated with **GOMOVIES.TO** and **123MOVIESHD.TO**

Gostream allegedly streams popular movie and television content from third-party cyberlockers. Formerly 123movies, the site was rebranded as Gomovies in March 2017 and then Gostream in July 2017. Despite enforcement action in Italy and the rebranding, the operation continues to be popular globally and its former names have spawned unaffiliated clone sites that capitalize on familiarity of the Gomovies and 123movies "brands" with slight variations. The site reportedly contains harmful content including pages that send visitors to harmful websites.[32] Gostream is reportedly operated from Vietnam and hosted in Ukraine.

INDIAMART.COM

Domain name registration services provided by **HOSTING CONCEPTS B.V. dba OPEN PROVIDER**

IndiaMart is an online marketplace based in India with 1.5 million suppliers and more than 10 million buyers. Among its legitimate listings, IndiaMart allegedly facilitates global trade in counterfeit and illegal pharmaceuticals. The marketplace disclaims all liability, delays responses and does not facilitate right holder attempts to remove listings. In contrast, other online marketplaces have instituted good practices such as robust screening systems to limit listings for counterfeit or illegal pharmaceuticals and providing a straightforward process for removing infringing listings. The domain name registrar that services IndiaMart, Hosting Concepts B.V., has a general Top Level Domain market share of 304,131 domains of which 2,530 are allegedly rogue Internet pharmacies.

[32] *See* https://transparencyreport.google.com/safe-browsing/search?url=gostream.is.

KINOGO.CLUB

Formerly **KINOGO.CO**

Kinogo hosts some of its own video content, suggesting that it could be a promising platform for legitimate content. However, the U.S. motion picture industry has reported sustained unacceptable levels of copyright infringing content for several years. Kinogo is hosted in the Netherlands and UK and targets the Ukraine and Russia markets. In June 2016, Kinogo was the subject of a Moscow City Court enforcement action and it is the 35th most popular site in Ukraine.

LIBGEN.IO and SCI-HUB.IO

Also **LIBGEN.PW**, **SCI-HUB.CC**, **SCI-HUB.AC**, **SCI-HUB.BZ**, **LIBGEN.INFO**, **LIB.RUS.EC**, **BOOKFI.ORG**, **BOOKZZ.ORG**, **BOOKER.ORG**, **BOOKSC.ORG**, **BOOK4YOU.ORG**, **BOOKOS-Z1.ORG**, **BOOKSEE.ORG**, and **B-OK.ORG**

Libgen, Sci-Hub and various mirror sites[33] reportedly make available for download millions of books and other publications, a significant number of which are distributed without the consent of copyright holders. Libgen.io may contain harmful content, including pages that contain suspicious or unknown software.[34] Sci-hub exists off infringing copyrighted material reportedly obtained with compromised user credentials obtained through phishing scams. Together these sites make it possible to download—all without permission and without remunerating authors, publishers or researchers—millions of copyrighted books by commercial publishers and university presses; scientific, technical and medical journal articles; and publications of technological standards. Following a 2015 injunction requiring U.S. domain registries to suspend the sites' domain names, the U.S. district court in the Southern District of New York entered a default judgement of $15 million against the sites in June 2017 for willful infringement of its copyrights. The judgement has not been paid and Sci-Hub continues to grow

[33] A "mirror site" is a website that is a proxy or clone of an original pirate site and may offer the same, new, or cached infringing content as the original site. Some mirror sites are designed to spread malware, steal personal information through spyware, or extort payments with ransomware. Mirror sites can complicate or delay sustained enforcement against the original pirate site. In some jurisdictions court-ordered injunctions can be designed to capture existing mirror sites and adapt quickly to new mirror sites.

[34] *See* https://transparencyreport.google.com/safe-browsing/search?url=libgen.io.

internationally, undermining the market for U.S. publishers abroad. Another right holder filed suit against Sci-Hub for copyright infringement and trademark counterfeiting in September 2017. Libgen and Sci-Hub are allegedly based in Russia.

MOVSHARE GROUP

Operating as **NOWVIDEO.SX**, **WHOLECLOUD.NET**, **AURORAVID.TO**, **BITVID.SX**, **NOWDOWNLOAD.CH**, **CLOUDTIME.TO** and formerly **MEWATCHSERIES.TO** and **WATCHSERIES.AC**

This coordinated network of extremely popular sites, with ties to Switzerland, Ukraine, Sweden, France, the Netherlands, Panama, and other countries, reportedly uses multiple technologies to make available countless unauthorized copies of movies, games, music, audio-books, software, and sporting event broadcasts. Cyberlockers, linking sites, forums, and streaming sites all conspire 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. Sites in the Movshare Group have been the subject of court-ordered enforcement action in Italy and India. Right holders report that Nowvideo and others in the Movshare group are entirely unresponsive to takedown notices.

MOVIE4K.TV

Movie4K.tv is hosted in Russia and reportedly specializes in copyright infringing movies. About half of web traffic to Movie4K.TV originates from Germany. Despite court-ordered enforcement action in Denmark, Italy, Norway, Austria and the UK, the site brazenly asserts that it is one of the biggest websites on the Internet for a wide range of free movies.

MP3VA.COM

MP3va.com is one of several music download sites based in Russia or Ukraine that allegedly engages in the unauthorized sale of U.S. sound recordings. The hosting provider is located in Russia and the registrant is reportedly based in Russia. The site attracts more than 2

million visits a month, more than three times as many visits as last year. Mp3va is popular in South Africa and has grown increasingly popular in Japan over the past year. The site has the look and feel of legal music download sites but sells tracks for pennies. MP3va continues to claim on its FAQ page that it has a license from Avtor, a rogue Ukrainian collecting society, and elsewhere purports to have a license from the "Russian Rightholders Federation for Collective Copyright Management of Works Used Interactively." Despite the alleged participation in these CMO's, the site's music download sales are reportedly not authorized and authors are not paid. Major U.S. credit card and payment processors do not service the site. The landing page for MP3va.us claims "Check It. It's Legal!" and provides a single link to MP3va.com.

OPENLOAD.CO

Also **OLOAD.TV** directs to **OPENLOAD.CO**

This combination cyberlocker and streaming operation is reportedly well-known for housing infringing movie content and has increased in popularity over the past year to become one of the 150 most popular websites worldwide. The site is used frequently in combination with add-ons in illicit streaming devices. In November 2017, users visited Openload.co a staggering 270 million times. The site incentivizes users to upload large, popular files by paying a fixed reward per 10,000 downloads or streams. Openload has moved hosting providers from the Netherlands and is now reportedly hosted in Romania.

PRIVATE LAYER-HOSTED SITES

Including **1337X.TO**, **PRIMEWIRE.AG**, **TORRENTZ2.EU** and mirror sites (**TORRENTZ2.ME, TORRENTZ2.IS**)

This group of websites is hosted by Switzerland- and Panama-based Private Layer, and is an example of the popularity among a wide variety of pirate sites of certain Swiss hosting services. 1337x.to and Torrentz2.eu are two of the most popular torrent sites that allegedly infringe U.S. content industry's copyrights. While the exact configuration of websites changes from year to year, this is the fourth consecutive year that the List has stressed the significant international trade impact of Private Layer's hosting services and the allegedly infringing sites it hosts. Other listed and nominated sites 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. Switzerland has announced plans to close a loophole in its law that restricts enforcement against pirate sites. In November, the Swiss Federal Council approved the proposal for a revision of the Copyright Act and sent the proposed draft Amendment to Parliament. USTR urges Switzerland to ensure that this legislation closes the gap. Right holders continue to report that Switzerland is an increasingly popular host country for infringing sites.

RARBG.TO

This site, located in Bosnia and Herzegovina, was nominated by commenters from the movie, television, and music industries. Rarbg was started almost a decade ago to target the Bosnian market but now has a global user base and consistently ranks in the top 300 websites worldwide. It reportedly has changed hosting services to prevent shutdowns in recent years. Rarbg generates revenue through ads and pay-per-install of potential malware. Although Rarbg has been the subject of enforcement and voluntary actions in Denmark, Italy, Portugal and the United Kingdom, it continues to operate.

REBEL

Rebel is added to the List again this year after a brief hiatus as the reported domain name registrar with the most disproportionate representation of allegedly counterfeit or otherwise 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. While not as egregious as Nanjing Imperiosus, which was listed last year, one social welfare organization continues to assert that Rebel is not responsive to abuse notifications. In contrast, other 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.[35]

[35] For example, Rightside and Realtime Register received ASOP Global's First Internet Pharmacy Safety E-Commerce Award in March 2017 in recognition of their "corporate policies and practices; responsiveness to illegal online drug sellers; prevention of illegal use of domain names for illegal online drug sales; cross-industry

REPELIS.TV

Repelis.tv has more than 150,000 links to more than 10,000 allegedly illegally reproduced movie and television series titles. This Spanish language website has connections and audiences across the Spanish-speaking diaspora including Mexico, Argentina, Spain, Peru and Venezuela. Repelis is monetized through a large number of national and international advertising and may contain harmful content, including links that send visitors to harmful websites.[36]

RUTRACKER.ORG and RAPIDGATOR.NET

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 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. Operators of the site allegedly net an estimated millions of dollars annually. RuTracker, a BitTorrent portal with almost 14 million active accounts, is also hosted in and reportedly operated from Russia. The site is currently one of the most popular in the world and a top site in Russia, with an Alexa ranking among the top 50 sites. RuTracker has been subject to a Moscow City Court ordered enforcement action.

TAOBAO.COM

A high volume of infringing products reportedly continue to be offered for sale and sold on Taobao.com and stakeholders continue to report challenges and burdens associated with IP enforcement on the platform. In particular, SMEs continue to have problems accessing and utilizing takedown procedures on Taobao.com. In 2017, more SMEs have requested assistance from U.S. government agencies and embassies regarding Taobao.com than any other e-

collaboration; and public and consumer awareness efforts." *See* http://buysaferx.pharmacy/news-release-alliance-for-safe-online-pharmacies-announces-recipients-of-its-first-internet-patient-safety-e-commerce-award/.

[36] *See* https://transparencyreport.google.com/safe-browsing/search?url=repelis.tv.

commerce platform. Created and owned by the Alibaba Group (Alibaba), Taobao.com is China's largest mobile commerce destination and the third-most popular website in China. Alibaba has undertaken efforts, some within the last six months, to curb the offer and sale of infringing products on Taobao.com, and some right holders report an improved outlook as a result. At the same time, the prevalence of infringing listings and sales continues to be a challenge and there are additional steps Alibaba must take to address ongoing concerns.

One U.S. automotive parts trade association reported that searches for branded products turn up few legitimate listings and some Taobao.com sellers reportedly use U.S. brand names on product listings that divert Chinese and global buyers away from legitimate offerings. Despite USTR's call in the 2016 List for Taobao.com to expand its Good Faith takedown program, the enforcement program reportedly continues to be burdensome and insufficient to end the sale of counterfeit products on the platform. While two U.S. trade associations reported better dialogue with Alibaba and some improvements in online enforcement on Taobao.com and other Alibaba platforms, the relatively high numbers of counterfeits on these sites continue to be a challenge for many U.S. brands. According to one of those associations, some member companies also reported ongoing problems, including with respect to delays or burdensome aspects of takedown programs. That association emphasized the importance of addressing these problems, given the sheer size, global reach, and growth of Alibaba's network.

In its submission, Alibaba reported it created a one-stop site for takedown requests across all Alibaba platforms with a simple user interface, step-by-step user instructions, and imposes no requirement to create an account before using the takedown mechanism. The company asserted that it closed more than 230,000 Taobao.com vendors for selling IP infringing goods over a recent one-year period, decreased takedown process times on the Taobao family of marketplaces (including Taobao.com, TMall and TMall Global), and that it increased proactive takedown efforts on Tabobao.com. In an additional proactive measure, Alibaba.com and AliExpress have barred listings for automotive air bags and air bag components. Alibaba has also reportedly provided numerous leads to Chinese law enforcement that resulted in arrests and facility closures. As evidence of the impact of its actions, Alibaba reported that Taobao.com, TMall and TMall Global received 25 percent fewer takedown requests in a recent annual period compared

to the prior one despite an 11 percent increase in the number of registered IP accounts across all of its e-commerce platforms.

We commend Alibaba for its efforts to date. However, while Alibaba presented its considerable efforts to address many concerns identified in the 2016 List, important unresolved concerns remain. For example, Alibaba has not identified metrics to assess objectively the scale of infringing products sold on Taobao.com nor objectively demonstrated that the volume or prevalence of counterfeit goods has decreased over the last year. The data provided by Alibaba to date do not directly reflect the scope and status of the counterfeiting problem on the Taobao.com platform, but instead is merely suggestive of progress made. For example, a decline in the number of takedown requests, while perhaps indicative of a positive trend across platforms, does not speak to the overall scope of the problem on Taobao.com. Additionally, Alibaba's efforts to address right holders' concerns appear to be aimed more towards global brands rather than SMEs, and the claimed results of those steps remain to be objectively verified.

Alibaba reports that the changes it discussed during this year's review were implemented in the latter half of 2017. Alibaba should continue to implement reported reforms across its platforms, while also working with brand owners to fine tune these tools and react quickly to emerging counterfeit trends. Important unfinished work includes the development of metrics demonstrating the scale of counterfeited and pirated offerings in its marketplace, and close engagement with interested parties to improve its processes for all stakeholders, including SMEs and those not represented by trade associations.

Over the next year, among other actions, Alibaba should: 1) seriously consider expanding its reported ban on automotive air bags and air bag components listings on the Alibaba.com and AliExpress.com platforms to the Taobao.com platform, and to other widely-counterfeited products not ordinarily sold in C2C marketplaces, such as brake pads and other automotive parts; 2) take efforts to ensure that its referrals of criminal leads to Chinese authorities lead to meaningful enforcement outcomes, such as by targeting large manufacturers and distributors of counterfeit goods; 3) seek to improve the effectiveness of the repeat infringer policy; 4) make available to right holders the contact information of infringing sellers and details on the volume of infringing sales after infringing listings are removed so that right holders can follow-up with enforcement action; 5) seek SME input and provide advisory opportunities to develop more

effective policies to address the challenges SMEs face on Taobao.com and other platforms; 6) improve tools to prevent the unauthorized use of product images for the sale of infringing products; and 7) ensure that infringing sellers and goods do not migrate from TMall or Taobao.com to other platforms owned and operated by Alibaba such as Xian Yu, located at 2.taobao.com.

It is incumbent upon Alibaba to develop more effective means to address the concerns of the full range of U.S. businesses that continue to find infringing versions of their products for sale on Taobao.com. Alibaba must not relax its efforts to combat counterfeiting and piracy on Taobao.com and other platforms. We ask affected industries and Alibaba to report back expeditiously on the status of Alibaba's continued IP enforcement efforts on Taobao.com. The United States will continue to closely monitor recent and prospective reforms.

THEPIRATEBAY.ORG

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

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 of admittedly illegal downloads of movies, television, music, and other copyrighted content. The site is in the top 100 most popular sites worldwide, is available in 35 languages and celebrated its 10-year anniversary by releasing the PirateBrowser, a portable web browser with preset bookmarks to BitTorrent websites. 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 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. In 2017, The Court of Justice of the European Union concluded that BitTorrent services provided by The Pirate Bay fall under the definition of "communication to the public," standing for a primary infraction of copyright, due to the key role played by the Pirate Bay website to ease the

exchange of files, by way of classifying, indexing, and arranging metadata included in the torrent files.[37] Also over the past year, The Pirate Bay site reportedly was occasionally unavailable.

TVPLUS, TVBROSWER and KUAIKAN

These app and add-on developers are reportedly operated by related companies in China to provide users around the world with television, live sports, and content protected by copyright and related rights. This family of apps has been downloaded more than 64 million times and each download connects users to allegedly pirated content hosted by third parties. These apps allow viewers in China to stream infringing content on mobile devices or high definition televisions posing an additional threat to an already fragile market for legitimate over-the-top and online content platforms in China.

UPLOADED.NET

Also **UL.TO** and **UPLOADED.TO**

This cyberlocker reportedly operates through multiple redundant domains and provides access to a broad range of reportedly infringing 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,[38] 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." Courts in Germany, Italy, and India have found the site liable for copyright infringement and issued orders against the site. Uploaded is owned by a Swiss company and hosted in the Netherlands.

[37] Court of Justice of the European Union, *Stichting Brein* C-610/15, June 14 2017.
[38] 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-netnam-es-cyber-profibility-1.compressed.pdf.

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 2016, VK reached licensing agreements with major record companies, took steps to limit third-party applications dedicated to downloading infringing content from the site, and experimented with content recognition technologies. Despite these positive signals, VK reportedly continues to be a hub of infringing activity and the U.S. motion picture industry reports that they find thousands of infringing files on the site each month. VK 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, which are comparable to those measures used by other social media sites.

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 set-top boxes, steaming devices, thumb-drives) continue 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 more online markets 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:

- 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;
- ability for customs and criminal authorities to detain and seize counterfeit and pirated goods entering into and exiting from Free Trade Zones.
- 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;

- criminal procedures and penalties for trafficking in counterfeit labels and packaging; and
- enhanced criminal penalties for particularly serious cases, such as trafficking in counterfeit trademark products that threaten health and safety.

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.

CHINA

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:

Silk Market, Beijing

Many retail vendors at the Silk Market reportedly sell and distribute counterfeit products. Even though some right holders successfully sued the market's operators in prior years, and despite administrative and criminal raids in prior years, the Silk Market reportedly remains one of the largest markets for the sale of counterfeit products in Beijing. Thus, it appears that past civil and administrative enforcement efforts, although imposing some costs, have not actually ended infringement.

Hongqiao Market, Beijing

Hongqiao Market, and the adjoining Tianya Jewelry Market, has more than 1,000 shops. According to local media reports, some of the shops selling counterfeits are clandestine – doors remain closed except to known customers, while other shops solicit shoppers by showing

them photos of the counterfeit goods in the street and then escorting them into shops or warehouses. Some shops even provide mailing services to send counterfeit products abroad. Hongqiao market was recently the subject of a January 2017 ruling in Beijing's Dongcheng District Court declaring that Hongqiao Market bore joint liability along with the counterfeit sellers and had to pay $75,000 in damages to one right holder. Additionally, in April and July 2017, Chinese enforcement officials raided Hongqiao Market and seized a significant number of counterfeit products. The Beijing Administration of Industry and Commerce (BAIC) has placed Hongqiao Market on its priority-watch list for trademark infringement.

In addition to the foregoing markets, the following markets also exemplify the problem of widespread counterfeiting of consumer products. Right holders have investigated and in some cases have taken enforcement actions against markets or sellers therein, but those efforts have reportedly not led to the cessation of the sale of counterfeit goods in these markets. In many of these markets, sellers reportedly openly characterize their products as "high quality" counterfeit products, reflecting an ability to engage in counterfeit sales with impunity:

- **Shenzhen Jindu Garment Wholesale Market, Shenzhen, Guangdong Province**
- **Jinxiang Foreign Trade Garment Market, Guangzhou (formerly known as the Jinbao Foreign Trade Garment Market)**
- **Jinshun Garment Market, Guangzhou**
- **Zhanxi Area Markets, Guangzhou**

ARGENTINA

La Salada, Buenos Aires

In contrast to recent years, in 2017, Argentina conducted raids and other significant enforcement actions related to counterfeiting or piracy in La Salada and in Barrio Once district of Buenos Aires. In 2017, Argentine authorities arrested two alleged leaders of the La Salada market, along with several associates. The criminal charges against the leaders, including illicit association, extortion and attempted murder, are indicative of the strong ties reported between counterfeiting and criminal organizations in Argentina and other markets. La Salada continues

to be included in this List as it will take sustained enforcement action and stronger legal tools to reverse the long-standing reputation of La Salada as one of the largest black markets for IP-infringing goods. Considerable quantities of a wide variety of counterfeit goods are reportedly still 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.

CANADA

Pacific Mall, Markham, Ontario

With over 270,000 square feet of retail space and more than 500 small shops, the sale of counterfeit goods at Pacific Mall in Ontario is sprawling and pervasive. The mall is touted as the largest Chinese mall in the western world and a recognized tourist destination but it has also been a well-known market for the sale of counterfeit and pirate goods for over a decade. Sales of counterfeit goods in the Pacific Mall reportedly continue despite extensive efforts by brand owners to enforce their trademarks. Vendors in Pacific Mall appear to operate largely with impunity, and requests for assistance from local law enforcement have reportedly gone unanswered. Many of the counterfeit goods including cosmetics, sunglasses, and fragrances pose a risk to public health and safety.

INDIA

Tank Road, Delhi

Tank Road returns to the List in 2017. Stakeholders confirm that it remains a market selling counterfeit products, including apparel and footwear. Counterfeit products from Tank Road are also reportedly found in other Indian markets, including Gaffar Market and Ajmal Khan Road. The United States encourages India to take sustained and coordinated enforcement action at the Tank Road market, previously-listed markets, and numerous other non-listed markets in its territory.

INDONESIA

Mangga Dua, Jakarta

Mangga Dua is a popular market in Jakarta selling a variety of counterfeit goods, including handbags, clothing, and fashion accessories, with reportedly minimal enforcement by the government to combat the rampant sale of the counterfeit goods. USTR urges the Indonesian Government to launch a sustained, coordinated, and effective effort to tackle widespread counterfeiting and piracy at markets throughout Indonesia, including Mangga Dua and other markets mentioned in previous Lists.

ITALY

Mercato dei venerdi, Ventimiglia

The Ventimiglia Mercato dei venerdi, or "Friday Market," was nominated this year in a coordinated and well-documented effort by international and European brands. The public open-air market is reportedly one of the largest in Italy and IP protection and enforcement in the market has been declining in recent years according to right holders. Although the market is open only on Fridays, 60-90 unauthorized sellers sell an estimated 20,000 infringing articles annually. In some stalls, managed through the town hall of Ventimiglia, official vendors also reportedly sell counterfeit clothing. USTR encourages local and national authorities to work with affected brand owners to develop a sustainable solution.

MEXICO

El Tepito, Mexico City

Significant levels of piracy and counterfeiting reportedly continue in El Tepito, an open-air 80 square block market in the middle of Mexico City. Stakeholders are concerned that El Tepito market has become increasingly dangerous making it nearly impossible for right holders to enforce their rights. Infringing items sold at El Tepito include video games, modified consoles and game circumvention devices, counterfeit apparel, and more, which are typically stored in small lockers. The United States encourages Mexico to continue coordinated law

enforcement efforts, including against high-level targets in the distribution chain and storage locker owners, 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.

Mercado San Juan de Dios, Guadalajara

Mercado San Juan de Dios, located in Guadalajara, remains on the List in 2017. With approximately 3,000 vendors, Mercado San Juan de Dios is the largest indoor market in Latin America, attracting a significant number of Mexican and foreign visitors. Amongst a plethora of pirated and counterfeit goods sold in the market, roughly one third of vendors allegedly sell video game circumvention devices. Stakeholders have raised concerns with the Mexican practice that requires each infringing game disc to be accompanied in the prosecution files by a copy of a legitimate original for comparison by experts in order for legitimate videogame right holders to enforce their rights. This requirement can be burdensome when there are multiple infringing copies of the same game disc under consideration. The United States encourages Mexico to address this issue, to ensure that legitimate right holders are able to adequately and effectively enforce their rights.

PARAGUAY

Ciudad del Este

Ciudad del Este has been named in the List and/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. Ciudad del Este thrives on a mainly Brazilian customer base attracted by low prices of counterfeit goods. Regional organized crime groups are reportedly responsible for the bulk of trade in counterfeit and pirated goods in Ciudad del Este. 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 are inadequate and in decline. The lag time to obtain warrants is long and the prosecution rates by the local office of the Attorney General are low. Better coordination and information sharing is needed between the National Directorate of Intellectual Property and the Attorney General.

SPAIN

Els Limits de La Jonquera, Girona

Els Limits de La Jonquera is a popular market in Girona, a city in the Catalan region of Spain that, like Ventimiglia, is close to the French border and popular with tourists. The market has been the subject of raids by the Spanish civil guard, but sellers are known to evade enforcement using various tactics including by stitching infringing labels at the point of sale. Right holders have obtained judicial orders to prevent the sale of infringing goods but those orders have been reversed. USTR urges the Spanish government to work with landowners, investigate warehouses and suppliers, and ensure that enforcement actions against counterfeit merchants are sustained.

TURKEY

Grand Bazaar, Istanbul

The Grand Bazaar in Istanbul, Turkey is among the largest and oldest markets in the world, and a top tourist attraction in Turkey. The market's 61 covered streets include over 4,000 shops that reportedly sell counterfeit handbags, wallets, and other leather goods, jewelry, watches, and perfumes. Right holders report that periodic raids by Turkish police have been insufficient to overcome the scale of the problem.

UNITED ARAB EMIRATES

DragonMart and Ajman China Mall

DragonMart and the Ajman China Mall, located on the Hatta - Al Ain Highway and Al Jerf Industrial Area, respectively, serve as important markets for China-sourced counterfeit

goods. Together, these two markets host over 5,000 stores selling a broad range of goods, including appliances, stationery, communication and acoustic equipment, lamps, household items, building materials, furniture, toys, machinery, garments, textiles, footwear, bags, and watches. In addition to serving the UAE market, these two marketplaces also serve as gateways to distribute counterfeit goods to foreign markets, particularly in the Middle East, North Africa, and Europe. An estimated 80 percent of the companies operating in the Ajman China Mall are Chinese, and the Chinese Government supports the project as part of the China Council for the Promotion of International Trade's 2010 "Going Out" strategy paper.

VIETNAM

Nin Heip Market, Hanoi, and Tan Binh Market, Ho Chi Minh City

Nihn Hiep in Hanoi and Tan Binh Market in Ho Chi Minh City are two of the most well-known retail markets in Vietnam. Although some markets in Vietnam have been the target of raids and seizures of both counterfeit goods and labels, USTR urges the Government of Vietnam to enhance and sustain enforcement actions to deter sales of counterfeit goods and labels at these and other nominated markets in Vietnam.

Public Information

The 2017 Notorious Markets List is the result of the eighth OCR of Notorious Markets, which USTR initiated on Aug 16, 2017, through a Federal Register Request for Public Comments. The request and responses are available at WWW.REGULATIONS.GOV, Docket Number USTR-2017-0015. USTR developed the 2017 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.

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. Victims and interested parties may report IPR theft to U.S. law enforcement agencies through a link at WWW.STOPFAKES.GOV or directly at WWW.IPRCENTER.GOV/REFERRAL.