OFFICE *of the* UNITED STATES TRADE REPRESENTATIVE

EXECUTIVE OFFICE OF THE PRESIDENT

2019 Review of Notorious Markets for Counterfeiting and Piracy

Table of Contents

Overview of the Results of the
2019 Review of Notorious Markets for Counterfeiting and Piracy

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 pose significant risks to consumer health and safety. The Notorious Markets List (NML) highlights prominent and illustrative examples of online and physical markets that reportedly engage in or facilitate substantial piracy or counterfeiting. A goal of the NML is to motivate appropriate action by the private sector and governments to reduce piracy and counterfeiting.

The Office of the United States Trade Representative (USTR) highlights the following markets because they exemplify global counterfeiting and piracy concerns and because the scale of infringing activity in these markets can cause significant harm to U.S. intellectual property (IP) owners, 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.

This year's NML includes several previously-identified markets because owners, operators, and governments failed to address the stated concerns. Other previously-identified markets may not appear in the NML for a variety of reasons, including that: the market has closed or its popularity or significance has diminished; enforcement or voluntary action has significantly reduced the prevalence of IP-infringing goods or services; market owners or operators are cooperating with right holders or government authorities to address infringement; or the market is no longer a noteworthy example of its kind. In some cases, online markets in the 2018 NML are not highlighted this year but improvements are still needed, and the United States may continue to raise concerns related to these markets on a bilateral basis with the relevant countries.

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

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

USTR developed the NML under the auspices of the annual Special 301 process[2] and solicited comments through a Request for Public Comments published in the Federal Register (https://www.regulations.gov, Docket Number USTR-2019-0013). The NML is based predominantly on publicly available information. USTR has identified notorious markets in the Special 301 Report since 2006. In 2010, USTR announced that it would begin publishing the NML separately from the annual Special 301 Report, pursuant to an out-of-cycle review. USTR first separately published the NML in February 2011.

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

Positive Developments Since the 2018 Out-of-Cycle Review of Notorious Markets

Since the release of the 2018 Notorious Markets List, there have been notable efforts to address widespread availability of pirated or counterfeit goods in some online and physical markets. The United States commends these efforts and encourages governments, right holders, service providers, and the owners and operators of these and other markets, including those newly identified in the 2019 NML, to engage in sustained and meaningful efforts to combat piracy and counterfeiting.

During the past year, some online piracy markets were the subject of several successful enforcement efforts. Notably, Ukraine's cyber police launched a nationwide anti-piracy operation that resulted in the shutting down of four popular video streaming sites with a combined daily audience of over 100,000 visitors: **Kinogo**, UAFilm, UKRFilm, and Kino-HD. Computer equipment was seized and the owners and operators of the sites are reportedly under investigation and face sentences of up to six years in prison. Also, in Uruguay, Interpol and the national police closed and arrested the operators of the **Pelispedia** websites, a popular linking service to unlicensed movies and TV shows that attracted an estimated 44 million visits a month. The operators of these websites were found guilty of copyright infringement and money laundering. **OpenLoad**, one of the largest cyberlockers that reportedly provided pirated content to 36 of the top 50 global illegal video streaming and linking sites, was also taken offline in October 2019, along with another popular cyberlocker that was nominated as a notorious market this year, Streamango. In Indonesia, the Ministry of Communications and Information in conjunction with industry groups pressured the operators of the notorious movie pirate site **IndoXXI** to cease operations. While IndoXXI is no longer operational, it appears that many copycat clones of IndoXXI have been recently created under different domain names to fill the void. We encourage the Indonesian government to continue enforcing its copyright laws against the operators of these pirate sites. Movie2free.com, Thailand's most-visited pirated movie and TV content provider that was nominated as a notorious market this year, was also shut down

after successful enforcement efforts, and the administrator of the site was arrested by the Thai Department of Special Investigation. Finally, Brazilian law enforcement executed *Operacao 404*, through which they took action against approximately 210 websites and 100 Internet Protocol television (IPTV) apps that facilitated the unauthorized streaming and downloading of films, TV shows, and live sporting events.

There continues to be notable enforcement actions taken against illegal IPTV providers. In September 2019, Eurojust in The Hague coordinated an international team of police in Bulgaria, France, Germany, Greece, Italy, and the Netherlands to raid multiple locations in order to shut down more than 200 servers used by Xtream Codes, which reportedly provided back-end management support to more than 5,000 IPTV apps, many of which streamed pirated content to an estimated 50 million viewers. In the days following this raid, worldwide illicit streaming traffic reportedly decreased by 50%. The seized information is expected to be used to shut down many providers of illegal IPTV apps worldwide. The Motion Picture Association (MPA) and Alliance for Creativity and Entertainment (ACE) have also successfully used legal systems around the world to suspend the domain names used by many providers of illicit streaming devices (ISDs), IPTV apps, and IPTV services, such as Vader Streams, One Step TV, and Omniverse One World Television. Finally, in a landmark ruling, a Singaporean court found a major retailer criminally liable for willfully authorizing copyright infringement by selling Android TV boxes loaded with apps that provided unauthorized access to copyright-protected content, including English Premier League matches, movies, and TV shows.

Another notorious online market from last year, **beoutQ**, a massive piracy operation widely available throughout the Middle East that streamed illicit content over satellite, through IPTV apps, and via web browsers has stopped operating. In addition, sales of beoutQ ISDs appear to have stopped. However, numerous ongoing concerns about these recent developments remain. First, the reason that beoutQ stopped operating remains unknown—there was no successful public judicial or enforcement action taken against beoutQ by a government or the private sector. Second, despite international recognition that beoutQ based its operations in

Saudi Arabia and broadcast its signal over Arabsat satellites,[3] Arabsat has continued to deny its involvement. Third, the popularity of beoutQ resulted in millions of beoutQ-branded IPTV boxes in homes and businesses throughout the region, some of which reportedly have been repurposed with other illicit IPTV streaming applications. The Saudi Authority for Intellectual Property (SAIP) has taken several actions to counteract the cultural acceptance of pirated content that beoutQ encouraged, such as conducting public awareness campaigns and supporting raids on stores selling ISDs, but significant work remains. USTR continues to monitor for the resurgence of beoutQ or any affiliated operations.

Payment processors continue to play a role in countering the sale of pirated and counterfeit goods. **Mp3va**, a notorious market listed in last year's report that takes on the appearance of a legal music site but provides unlicensed downloads for unreasonably low prices, significantly dropped in popularity after U.S. credit card and payment processors voluntarily agreed to terminate support for the site in response to right holders' concerns.

Regarding physical markets, several countries have significantly increased IP enforcement efforts. Police in Buenos Aires and Misiones, **Argentina**, carried out raids and arrested approximately 100 people in September 2019 to break up a mobile street vendor (colloquially known as *manteros*) operation tied to Senegalese organized crime. The alleged leaders of the operation were charged with trademark counterfeiting, tax evasion, and human trafficking. In **Brazil**, officials conducted a series of IP-enforcement raids called *Operação Comércio Legal*

[3] *See, e.g.*, T. Panja, FIFA and Premier League Document Saudi Link in BeIN Piracy Fight (Sept. 16, 2019), https://www.nytimes.com/2019/09/16/sports/fifa-beoutq-premier-league-uefa.html (citing and linking to MarkMonitor, beoutQ Investigation (Apr. 2019), https://img.fifa.com/image/upload/bsaawfqlbtm3vdubuehl.pdf (pg. 51 "Our analysis shows beyond any doubt that the beoutQ channels received via the beoutQ HD Sport application on the beoutQ [set top box] are transmitted from the Arabsat geostationary satellite network at 26 degrees East.")); J. Murray, BBC TV License Scandal: Tens of Millions of Pounds LOST in Saudi Arabia Piracy Operation (Sept. 12, 2019), https://www.express.co.uk/news/uk/1177048/bbc-tv-licence-saudi-arabia-piracy-middle-east-north-africa-news-latest; Joint Statement by FIFA, the AFC, UEFA, the Bundesliga, LaLiga, the Premier League and Lega Serie A Regarding the Activities of beoutQ in Saudi Arabia (July 31, 2019), https://www.fifa.com/about-fifa/who-we-are/news/joint-statement-by-fifa-the-afc-uefa-the-bundesliga-laliga-the-premier-league-an; A. Ritman, Could This Be the World's Biggest State-Sponsored Piracy Operation? (June 20, 2019), https://www.hollywoodreporter.com/features/could-be-worlds-biggest-state-sponsored-piracy-operation-1217919; H. Gold, NBA and Sky Accuse Saudi Arabia of Harboring Media Pirates (Feb. 14, 2019), https://www.cnn.com/2019/02/14/media/saudi-arabia-pirate-beoutq/index.html; M. Stancata, An Unlikely Victim of Saudi Arabia's Dispute With Qatar: TV Rights (Sept. 6, 2018), https://www.wsj.com/articles/an-unlikely-victim-of-saudi-arabias-dispute-with-qatar-tv-rights-1536266561.

(Operation Legal Commerce) that has resulted in the seizure of over 400 tons of counterfeit goods worth at least $74 million since January 2019, including approximately ten tons of counterfeit toys and cosmetics and approximately 500,000 counterfeit watches from the notorious **Rua 25 de Março** market and surrounding markets. In a July 2019 enforcement operation in **Romania**, approximately 700 police officers raided one of the largest remaining counterfeit markets in the country, Europa Market in Bucharest, shutting down 900 vendors, arresting 22 individuals, and seizing twelve truckloads of counterfeit goods. In the **United Arab Emirates**, enforcement of intellectual property rights by Dubai Police and the Dubai Department of Economic Development (DED) has resulted in counterfeit goods no longer being openly displayed inside **Dragon Mart**. In July 2019, **Vietnam**'s General Department of Customs carried out enforcement activities in Mong Cai City, Quang Ninh Province, and seized counterfeits worth over $1 million.

Several studies this year addressed global trade in counterfeit and pirated goods. The Organization for Economic Cooperation and Development (OECD) issued a report on the latest trends in trade in counterfeit and pirated goods, based on data from 2016.[4] This report found that trade in counterfeit and pirated physical goods has risen steadily in the last few years and now stands at 3.3% of global trade ($509 billion), with some industries being significantly more affected than others—22% for footwear, 15% for clothing, 13% for leather goods, and 12% for electrical equipment. The OECD report identifies corruption, poor IP enforcement, free trade zones, China's role as a top producer of counterfeit and pirated goods, and the use of post or courier services to send small shipments[5] as key factors behind this growth. The Better Business Bureau (BBB) investigated the "epidemic of counterfeit goods sold online" in the United States and issued a report finding that "[o]rganized criminals operating out of China are behind the vast majority of this fraud," and that they are "supported by a large ecosystem of groups that arrange

[4] OECD, Trends in Trade in Counterfeit and Pirated Goods (Mar. 18, 2019), https://www.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en.

[5] *See also* OECD, Misuse of Small Parcels for Trade in Counterfeit Goods: Facts and Trends (Dec. 12, 2018), https://www.oecd-ilibrary.org/governance/misuse-of-small-parcels-for-trade-in-counterfeit-goods_9789264307858-en.

for credit card processing."[6] The BBB recommended that credit card payment processors increase their efforts to combat the sellers of counterfeit goods. A study by Ghostdata of counterfeit goods sold on Instagram found that the "top payment system is by far WeChat Pay," which is owned by Chinese company Tencent.[7]

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

[6] BBB, Fakes Are Not Fashionable: A BBB Study of the Epidemic of Counterfeit Goods Sold Online (May 2019), https://www.bbb.org/globalassets/local-bbbs/council-113/media/scam-studies/bbb-study-of-counterfeit-goods-sold-online.pdf; *see also* H. Tian et al., Bullet-proof Payment Processors (May 2018), https://ieeexplore.ieee.org/document/8376208.

[7] A. Stroppa et al., Instagram and Counterfeiting in 2019: New Features, Old Problems (Apr. 9, 2019), https://ghostdata.io/report/Instagram_Counterfeiting_GD.pdf.

Issue Focus: Malware and Online Piracy

The "issue focus" section of the NML highlights an issue related to the facilitation of substantial counterfeiting or piracy. Past issue focuses highlighted free trade zones (2018), illicit streaming devices (2017), stream ripping (2016), emerging marketing and distribution tactics in Internet-facilitated counterfeiting (2015), and domain name registrars (2014).

This year's issue focus explores the nexus between online piracy and malware, which has been discussed in past publications of the NML in the context of specific online markets such as 1Fichier, MPGH, and ThePirateBay. Malware, a combination of the words malicious and software,[8] is unwanted software that is installed on computers or mobile devices without consent and is often used to take advantage of computers or personal information in unwanted ways.[9] The most insidious form of malware is perhaps backdoor Trojans, which secretly grant remote access privileges of an infected device to attackers, who may proceed to steal any personal information or financial records stored on the device, provide unauthorized access to a device, monitor device activities, and install additional malware.[10] Cryptominers, run as a program or on a malicious website, take control of the computing power of an infected device and turn it toward mining cryptocurrency, which greatly slows down the performance of the device and increases electricity consumption.[11] Ransomware denies access to a device by encrypting all stored data and demanding payment in return for keys to unlock the encryption.[12]

---

[8] Some definitions of malware also include "adware," which is often undesirable software used to deliver ads to users but may not be malicious.

[9] Federal Trade Commission, Malware (Nov. 2015), https://www.consumer.ftc.gov/articles/0011-malware.

[10] *See* Malwarebytes Labs, 2019 State of Malware, https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf.

[11] *See* Malwarebytes Labs, 2019 State of Malware, https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf; O. Harpaz & D. Goldberg, The Nansh0u Campaign – Hackers Arsenal Grows Stronger (May 29, 2019), https://www.guardicore.com/2019/05/nansh0u-campaign-hackers-arsenal-grows-stronger; D. Fuscaldo, Crypto Mining Malware Grew 4,000% This Year (Dec. 28, 2018), https://www.forbes.com/sites/donnafuscaldo/2018/12/28/crypto-mining-malware-grew-4000-this-year.

[12] *See* C. Stupp, Hackers Get More Sophisticated With Ransomware Attacks (Dec. 18, 2019), https://www.wsj.com/articles/hackers-get-more-sophisticated-with-ransomware-attacks-11576665001; P. Muncaster, Over 1000 US Schools Hit by Ransomware in 2019 (Dec. 18, 2019), https://www.infosecurity-magazine.com/news/over-1000-us-schools-hit-by; D. Winder, Infection Hits French Hospital Like It's 2017 as Ransomware Cripples 6,000 Computers

Botnets turn infected devices into "robots" that, in coordination with other infected devices, conduct mass cyberattacks, such as distributed denial-of-service (DDOS) attacks.[13]

The nexus between online piracy and malware is tied to financial incentives. Cybercriminals who create and operate malware benefit in correlation with the spread of the malware among infected devices: they sell stolen personal and financial information, mine for cryptocurrency, collect ransoms, rent botnets, and sell cyberattack capabilities. These bad actors pay piracy websites and apps to deliver malware to those who visit the websites or use the apps—between $50–$200 per 1,000 malware installations, according to a 2015 study.[14] This study estimated that 229 piracy websites, including notorious online markets identified by USTR in its 2015 NML, generated roughly $3.3 million that year by delivering malware to their visitors. Cybercriminals also pay for advertisements on pirate websites, and some of these advertisements will install malware when displayed or clicked.[15] According to a 2016 study, 51% of ads on 260 suspected piracy websites contained malware.[16] The money collected by the

---

(Nov. 20, 2019), https://www.forbes.com/sites/daveywinder/2019/11/20/infection-hits-french-hospital-like-its-2017-as-ransomware-cripples-6000-computers.

[13] *See* C. Cimpanu, A Decade of Malware: Top Botnets of the 2010s (Dec. 3, 2019), https://www.zdnet.com/article/a-decade-of-malware-top-botnets-of-the-2010s; Council to Secure the Digital Economy, International Botnet and IOT Security Guide 2020 (Nov. 2019), https://securingdigitaleconomy.org/wp-content/uploads/2019/11/CSDE_Botnet-Report_2020_FINAL.pdf; A. Moshirina, Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat, 93 Ind. L. J. 975 (2018).

[14] Digital Citizens Alliance & RiskIQ, Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data (Dec. 2015).

[15] A 2015 study found that 55% of malware was downloaded when a user clicked on a link, often a prompt that resembled a legitimate action, and 45% of malware was downloaded invisibly in the background upon visiting a webpage. Digital Citizens Alliance & RiskIQ, Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data (Dec. 2015). A malicious advertisement can automatically install malware without user interaction by can exploiting out-of-date software or browsers with incorrectly configured security options. *See* D. Bradbury, Chrome Will Soon Block Drive-by-Download Malvertising (Mar. 13, 2019), https://nakedsecurity.sophos.com/2019/03/13/chrome-will-soon-block-drive-by-download-malvertising. Malicious advertisements can also hijack traffic from the sites that host the ads and redirect the traffic to malicious domains that host malware. *See* R. Wright, Inside 'Master 134': Propeller Ads connected to malvertising campaign (Apr. 30, 2019), https://searchsecurity.techtarget.com/feature/Inside-Master134-Propeller-Ads-connected-to-malvertising-campaign (describing the "Master 134" malvertising campaign, tied to the AdsTerra and Propeller Ads network).

[16] European Observatory on Infringements of Intellectual Property Rights, Digital Advertising on Suspected Infringing Websites (Jan. 2016), https://euipo.europa.eu/ohimportal/documents/%2011370/80606/Digital+Advertising+on+Suspected+Infringing+Websites.

cybercriminals from the pirate websites and apps, as well as revenue generated through other advertising, donations, and subscriptions, significantly enables and incentivizes the facilitation of online piracy.

The nexus between online piracy and malware is also tied to the pirated content itself. Websites that require users to download rather than stream the infringing content, such as cyberlockers or bittorrent sites, may contain malware-infected content, including software, games, movies, music, and books. Pirated games are a particularly popular vector of this type of malware infection, since many pirated games require the user to download additional programs, known as "cracks," to circumvent the game's built-in technological protection measures, and cracks are common places to hide malware.[17] Pirated games are also a popular target for cryptominer malware as computers used for gaming tend to have high-end hardware that makes mining more efficient.[18] Cybercriminals also disguise malware as TV shows or movies—malware masquerading as Game of Thrones episodes reportedly accounted for 17% of all infected pirated content in 2018.[19] In addition, malware is commonly disguised as pirated essays or textbooks, targeting students who search for this free content.[20]

Illicit IPTV apps that run on set-top boxes can stream unlicensed sports, movies, and TV shows to a user's television, but these apps may themselves be malware.[21] According to a 2019 report on these apps, researchers found that some apps attempted to access every smart device

---

[17] *See* A. Moshirina, Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat, 93 Ind. L. J. 975 (2018).

[18] *See* A. Moshirina, Typhoid Mario: Video Game Piracy as Viral Vector and National Security Threat, 93 Ind. L. J. 975 (2018).

[19] M. Kan, Pirating 'Game of Thrones'? That File Is Probably Malware (Apr. 1, 2019), https://www.pcmag.com/news/367529/pirating-game-of-thrones-that-file-is-probably-malware; *see generally* Ernesto, Game of Thrones is the Most Torrented TV-Show of 2019 (Dec. 28. 2019), https://torrentfreak.com/game-of-thrones-is-the-most-torrented-tv-show-of-2019-191228.

[20] R. Hodge, Back-to-School Malware Is Hiding in Those Digital Textbooks (Sept. 3, 2019), https://www.cnet.com/news/back-to-school-malware-is-hiding-in-those-digital-textbooks; W. Maxson, Free Movies, Costly Malware (Apr. 12, 2017), https://www.consumer.ftc.gov/blog/2017/04/free-movies-costly-malware.

[21] Research into the availability and popularity of these malicious IPTV apps is still needed. *See* Andy, Rampant Kodi Malware? It's Time to Either Put Up or Shut Up (Jun. 10, 2018), https://torrentfreak.com/rampant-kodi-malware-its-time-to-either-put-up-or-shut-up-190610 ("[T]here are at least some [apps] that are clearly malicious but [do not] seem to serve other real purpose for the [] users.").

connected to the same network as the malware, install additional malware on those devices, collect information stored on those devices, and send the information to a remote location.[22] The apps also allowed remote access to and control of the device.

To avoid malware infections from piracy sites, consumers should rely on legitimate sources of copyright-protected content, such as licensed video streaming providers, and should purchase software and games from licensed vendors.[23] Purchasing legitimate content reduces exposure to malware; unsurprisingly, users who access pirated content have more malware infections.[24] Consumers should also proactively protect their devices from malware infection by installing antivirus software from legitimate providers.

[22] Digital Citizens Alliance, Fishing in the Piracy Stream: How the Dark Web of Entertainment Is Exposing Consumers to Harm (Apr. 2019), https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf; *see also* A. Puig, Malware from Illegal Video Streaming Apps: What to Know (May 2, 2019), https://www.consumer.ftc.gov/blog/2019/05/malware-illegal-video-streaming-apps-what-know.

[23] A. Puig, Malware from Illegal Video Streaming Apps: What to Know (May 2, 2019), https://www.consumer.ftc.gov/blog/2019/05/malware-illegal-video-streaming-apps-what-know.

[24] R. Telang, Does Online Piracy make Computers Insecure? Evidence from Panel Data (Mar. 2018), https://ssrn.com/abstract=3139240 (estimating that doubling the visits to a pirated sites adds an extra 0.05 of a piece of malware per month); Digital Citizens Alliance & RiskIQ, Digital Bait: How Content Theft Sites and Malware are Exploited by Cybercriminals to Hack into Internet Users' Computers and Personal Data (Dec. 2015) (finding that 1 out of every 3 piracy websites contains malware and that visitors were 28 times more likely to get malware from an infringing site than on a similarly situated non-infringing site).

Results of the
2019 Review of Notorious Markets

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

Owners and operators of notorious markets that are willing to address piracy and counterfeiting have many options for doing so. Such owners and operators can, for example, adopt business models that rely on the licensed distribution of legitimate content and can negotiate appropriate licenses with right holders. If an otherwise legitimate business has become a platform for piracy or counterfeiting, the owner or operator can work with right holders and law enforcement officials to help discourage and curtail acts of infringement. Industry groups have developed a variety of best practices that can help combat counterfeiting and piracy.[25] In the absence of good faith efforts, responsible government authorities should investigate reports of piracy and counterfeiting in these and similar markets and pursue appropriate action against such markets and their owners and operators. Governments should also ensure that appropriate enforcement tools are at the disposal of right holders and government authorities, which may require closing loopholes that permit operators to evade enforcement laws.

[25] *E.g.*, International Trademark Association, Addressing the Sale of Counterfeits on the Internet (Feb. 2018), https://www.inta.org/Advocacy/Documents/2018/Addressing_the_Sale_of_Counterfeits_on_the_Internet_021518.pdf; BASCAP, Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain, International Chamber of Commerce (Mar. 2015), https://iccwbo.org/publication/roles-responsibilities-intermediaries.

Online Markets

The 2019 Notorious Markets List identifies examples of various technologies,[26] obfuscation methods, revenue models, and consumer harms associated with infringing activity. USTR based its selections not on specific types of technologies but on whether the owners, operators, or users of a nominated market or affiliated network of markets reportedly engage in or facilitate substantial piracy or counterfeiting to the detriment of U.S. creators and companies.

Those who submitted public comments this year highlighted the complex ecosystem that is abused by providers of pirated content, including domain name registrars, reverse proxy services, hosting providers, caching services, advertisers and ad placement networks, payment processors, social networks, and search engines. Each component in this ecosystem can play a role in facilitating or reducing piracy. For example, as noted above, last year's notorious market MP3va saw a significant decline in popularity due to actions by U.S. payment processors to stop accepting payments from the site. Additionally, for the first time this year, an ad placement network, Propeller Ads, is identified as a notorious market for its role in funding piracy websites.

This year's review process also identified a growing concern about the proliferation of counterfeits facilitated by social media platforms. For example, right holders have expressed increasing concerns with a growing trend of counterfeit products being offered for sale on e-commerce features related to large platforms, such as WeChat. USTR will further study and monitor these concerns. Platforms can begin to address these concerns by establishing industry-standard IP enforcement policies, increasing transparency and collaboration with right holders to quickly address complaints, and working with law enforcement to identify IP violators.

In its Federal Register Notice, USTR did not request submissions on U.S. based e-commerce platforms and online third-party marketplaces, such as Amazon.com. However, the Administration has been looking further at their role following the issuance in April 2019 of a

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

Presidential Memorandum addressing trafficking in counterfeit and pirated goods.[27] In January 2020, in response to the Presidential Memorandum, the Department of Homeland Security (DHS) issued a report on "Combating Trafficking in Counterfeit and Pirated Goods."[28] The DHS report notes that, although e-commerce has supported the launch of thousands of legitimate businesses, e-commerce platforms, third-party marketplaces, and their supporting intermediaries have also served as powerful stimulants for the trafficking of counterfeit and pirated goods. Selling counterfeit and pirated goods through e-commerce platforms and related online third-party marketplaces can be a highly profitable venture. For counterfeiters, production costs are low, millions of potential customers are available online, transactions are convenient, and listing goods on well-known platforms provides an air of legitimacy. Moreover, when sellers of illicit goods are in another country, they are exposed to relatively little risk of criminal prosecution or civil liability under current law enforcement and regulatory practices. USTR agrees that actions should be taken to protect American consumers and businesses against the harm and losses inflicted by counterfeiters.

In light of these concerns, USTR believes e-commerce platforms need to take additional actions to combat trafficking in counterfeit and pirated goods and reduce the availability of such goods on their platforms. For example, the DHS "Combating Trafficking in Counterfeit and Pirated Goods" report called for the swift adoption by e-commerce platforms that operate third-party marketplaces and other third-party intermediaries of the following ten high priority best practices:

1. Comprehensive "Terms of Service" Agreements
2. Significantly Enhanced Vetting of Third-Party Sellers
3. Limitations on High Risk Products
4. Efficient Notice and Takedown Procedures
5. Enhanced Post-Discovery Actions

---

[27] Memorandum on Combating Trafficking in Counterfeit and Pirated Goods (Apr. 3, 2019), https://www.whitehouse.gov/presidential-actions/memorandum-combating-trafficking-counterfeit-pirated-goods.

[28] Combating Trafficking in Counterfeit and Pirated Goods (Jan. 24, 2020), https://www.dhs.gov/publication/combating-trafficking-counterfeit-and-pirated-goods.

6. Indemnity Requirements for Foreign Sellers

7. Clear Transactions Through Banks that Comply with U.S. Enforcement Requests

8. Pre-Sale Identification of Third-Party Sellers

9. Establish Marketplace Seller IDs

10. Clearly Identifiable Country of Origin Disclosures

Without such actions, U.S. right holders stand to be irreparably damaged by a flood of imported counterfeit and pirated goods on e-commerce platforms, regardless of where such platforms are based. Consistent with the Presidential Memorandum on Combating Trafficking in Counterfeit and Pirated Goods, USTR will continue to address the issue of counterfeit and pirated goods with our trading partners and is considering seeking more information regarding e-commerce platforms, including those based in the United States, in future reviews of Notorious Markets.

1337x

Nominated as 1337x.to. Related sites include 1337x.se, 1337x.st, x1337x.ws, x1337x.eu, and x1337x.se. Reportedly hosted at FlokiNET in Finland, but utilizes reverse proxy services to mask the location of its hosting servers.

This popular website provides links to torrent files, which are small files that contain the information necessary to download other files from the bittorrent distributed peer-to-peer network, for unlicensed movies, TV shows, music, and software. Variants of the site have been subject to blocking orders in the United Kingdom, Denmark, Portugal, Belgium, Indonesia, Ireland, Malaysia, India, Austria, Australia, and Italy.

1FICHIER

Nominated as 1fichier.com. Related sites include alterupload.com, cjoint.net, cloudstorage.fr, desfichiers.com, dl4free.com, megadl.fr, and tenvoi.com. Hosted in France.

This cyberlocker[29] is popular in France and reportedly makes premium pirated content, such as unlicensed movies and video games, available to the public. Right holders regularly

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

complain about 1Fichier's extremely low response rate to takedown requests—0.12%, down from 0.59% last year and 2% the previous year. This site continues to have millions of visitors a month despite payment processors suspending services and Internet browsers warning of malicious content.

AMAZON'S FOREIGN DOMAINS

Nominated as amazon.ca, amazon.co.uk, amazon.de, amazon.fr, and amazon.in.

Submissions by right holders expressed concerns regarding the challenges related to combating counterfeits with respect to e-commerce platforms around the world. One submission specifically highlighted examples of the challenges right holders face with alleged high levels of counterfeit goods on the e-commerce platforms amazon.ca in Canada, amazon.de in Germany, amazon.fr in France, amazon.in in India, and amazon.co.uk in the United Kingdom.[30] For example, right holders expressed concern that the seller information displayed by Amazon is often misleading such that it is difficult for consumers and right holders alike to determine who is selling the goods and that anyone can become a seller on Amazon with too much ease because Amazon does not sufficiently vet sellers on its platforms. They also commented that Amazon's counterfeit removal processes can be lengthy and burdensome, even for right holders that enroll in Amazon's brand protection programs.

In addition, as the scale and sophistication of the counterfeiters have continued to grow and evolve over the years, these right holders indicate that Amazon should commit the resources necessary to make their brand protection programs scalable, transparent, and most importantly, effective. More specifically, they ask that Amazon take additional actions to address their concerns, including by collecting sufficient information from sellers to prevent repeat infringers from creating multiple storefronts on the platforms, making detailed information about the real seller of a product obvious to consumers and right holders, being more responsive to complaints

[30] See September 30, 2019 Submission of American Apparel & Footwear Association (AAFA) in response to 2019 Special 301 Out-of-Cycle Review of Notorious Markets, available at https://www.regulations.gov/document?D=USTR-2019-0013-0021/.

of counterfeits by right holders, and being more proactive in preventing counterfeit goods from appearing on the platform.

BESTBUYIPTV

Nominated as bestbuyiptv.com. Reportedly hosted in Italy.

This service offers illicit IPTV apps that are compatible with most platforms and operating systems. The BestBuyIPTV website boasts over 7,300 HD channels, including unlicensed sports, entertainment, and movie channels, as well as 9,600 videos-on-demand. BestBuyIPTV also provides reseller and re-streamer services with over 900,000 viewers, 12,000 resellers, and 2,000 re-streamers.

BUKALAPAK

Nominated as bukalapak.com. Also available as a mobile app. Reportedly hosted in Indonesia.

Bukalapak, founded in 2010, is one of the largest e-commerce markets in Indonesia. This website provides a platform for third-party sellers to connect with buyers, and these sellers offer a wide variety of products, including consumer electronics, books, automobile parts, and apparel. Right holders report that the majority of branded products on this platform are not genuine and that items are often openly labeled "replicas" of branded products. While Bukalapak provides a link on its platform for right holders to report illegal and infringing goods and merchants, right holders report that this mechanism is ineffective. Specifically, they state that Bukalapak does not respond promptly to reports of counterfeit listings and that the procedures to report counterfeit listings are burdensome. The platform also reportedly fails to deter repeat infringers, and some known sellers of counterfeit products have been active on the platform for as long as six years. Bukalapak claims to operate a blacklisted keyword system to prevent certain listings, but this appears to be ineffective in addressing the scope of the problem on its platform.

CAROUSELL

Nominated as carousell.com. Also available as a mobile app. Reportedly hosted in Singapore, but utilizes reverse proxy services to mask the location of its hosting servers.

Carousell is an online and mobile e-commerce platform based in Singapore. Right holders are concerned about the platform's lack of an official IP-infringement reporting program. Carousell reportedly only has an open "report a violation" tool that does not allow a right owner to register with the system. Once a counterfeit is reported, Carousell does not confirm that it received the report and does not follow up to indicate if action was taken or not taken, which requires the reporter to continually monitor the identified listing to determine whether the counterfeit product was taken down. Right holders also report that any attempt to follow up on a report is ignored. Carousell typically waits 30 days before taking action, if at all, and it lacks proactive IP enforcement tools. Moreover, there is no system to prevent repeat sellers of counterfeit goods to continue to sell counterfeits on the site. Carousell's deficient IP protection and enforcement procedures are becoming more worrisome to right holders as its popularity and geographic reach continue to grow.

CHOMIKUJ

Nominated as chomikuj.pl. Reportedly hosted in the Netherlands, but utilizes reverse proxy services to mask the location of its hosting servers.

Chomikuj is the most popular cyberlocker in Poland. Right holders report that a broad range of unlicensed songs by U.S. artists are available on this platform. Chomikuj allegedly rewards users who upload popular content that is then downloaded by other users. Right holders report that in 2017, the Krakow Court of Appeal ordered the site to pay damages to right holders on the basis that it had directly infringed the making available right and was not able to claim safe harbor protection because it was not a passive actor. However, the site continues to provide unlicensed content to millions of visitors per month.

CIMACLUB

Nominated as cimaclub.com. Related sites include cima4u.tv. Utilizes reverse proxy services to mask the location of its hosting servers, but cimaclub.com is reportedly hosted in France and cima4u.tv is reportedly hosted in Russia.

Cimaclub is the most popular Arabic language piracy website in the world, with over 40 million visits per month. Nominated by the movie industry, Cimaclub is a major source of unlicensed video content for the Middle East and North Africa.

DHGATE

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

DHgate is the largest business-to-business cross-border e-commerce platform in China with over 21 million registered buyers and over 22 million products for sale. Over 2 million Chinese merchants, many of which are small- and medium-sized enterprises, sell their products on the platform. During the past year, DHgate has taken steps to decrease the number of counterfeit goods on its platform. For example, DHgate increased the penalties for sellers of counterfeit goods, automated the process of collecting global brand information, launched an image recognition system to identify pictures of likely counterfeit goods, and added many brand-related keywords to its counterfeit filter system. DHgate has also acted on USTR's recommendations in the 2018 NML to "make information about infringing sellers available to right holders or law enforcement authorities." As a result, fewer commenters nominated DHgate as a notorious market this year. Nevertheless, DHgate remains a notorious market given the widespread availability of counterfeits on its platform and the ease with which counterfeits are located. USTR urges DHgate to continue improving its seller vetting, listing policies, reporting procedures, and proactive monitoring to significantly decrease the availability of counterfeit goods.

DYTT8

Nominated as dytt8.net. Related sites include dy2018.com. Hosted in Taiwan.

DYTT8 is one of the most popular non-English torrent sites in the world, providing links to unlicensed movies, TV shows, music, and software. With a user-friendly interface, DYTT8 remains a particular threat to legitimate content providers both within and outside China.

FLOKINET

FlokiNET is an example of the growing problem of so-called "bulletproof" hosting providers that support known notorious websites by refusing to respond to notices of infringement and by failing to cooperate with right holders and law enforcement. FlokiNET's website advertises anonymity: "We do not require any personal details or identification, any valid e-mail address is enough information to be a client." With servers reportedly in Romania and Iceland, FlokiNET hosts many websites associated with infringing activity, including 1337x.

FLVTO

Nominated as flvto.biz. Related sites include 2conv.com. Reportedly hosted in the Netherlands and operated out of Russia, but utilizes reverse proxy services to mask the location of its hosting servers.

Flvto is highlighted again this year as an example of the stream-ripping[31] phenomenon that continues to threaten legitimate streaming audio and video services, music performers, and composers. This site allows users to download converted YouTube videos as digital audio files, but it does not appear to have permission from YouTube or from right holders for a wide variety of music represented by major U.S. labels.

FMOVIES

Nominated as fmovies.is. Related sites include fmovies.to and fmovies.se. Reportedly hosted in Ukraine, but utilizes reverse proxy services to mask the location of its hosting servers.

According to right holders, Fmovies allegedly streams unauthorized movies and TV shows directly to computer desktops or through IPTV apps on illicit streaming devices. The continued listing of Fmovies in the NML demonstrates the ongoing challenges of streaming piracy. According to right holders, several countries have taken action against this site, including Australia, Denmark, Malaysia, Singapore, and Sweden.

[31] For a description of stream-ripping, see the 2016 NML.

HOSTING CONCEPTS B.V. (D/B/A OPEN PROVIDER) AND REGIONAL NETWORK INFORMATION CENTER JSC

Hosting Concepts B.V. (d/b/a Open Provider) and Regional Network Information Center JSC are recognized for providing domain name registration and hosting services to illegal online pharmacies. Counterfeit pharmaceuticals sold through illegal online pharmacies are particularly pernicious because not only do they cause damage to the reputation of brands and to legitimate pharmacies, but they also may put consumers' health at risk. Some 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 the domain names registered to illegal online pharmacies. However, a few hosting providers do not have such policies, and according to right holders, a vast majority of rogue pharmacies are hosted by these providers. USTR encourages all registrars and hosting providers to employ and enforce policies that curb the online sale of counterfeit pharmaceuticals.

Hosting Concepts B.V. and Regional Network Information Center JSC continue to be examples of hosting providers without the types of beneficial policies listed above. These companies host many known illegal online pharmacies, some of which offer counterfeit controlled substances such as opioids, and they are reportedly non-responsive to abuse notifications.

MP3JUICES

Nominated as mp3juices.cc. Related sites include eaoe.cc. Reportedly hosted in Russia, but utilizes reverse proxy services to mask the location of its hosting servers.

MP3juices is a popular stream-ripping website that allegedly permits a user to select YouTube music videos and make permanent downloads of audio-only mp3 files that users can add to their music library. According to right holders, the site provides a search functionality to locate desired YouTube videos and then utilizes a separate service as the back-end for delivering the audio file to the user.

MPGH

Nominated as mpgh.net. Reportedly hosted in the Czech Republic, but utilizes reverse proxy services to mask the location of its hosting servers.

A growing concern for the video game industry is the unauthorized sales of in-game digital items, where cheat software (such as bots and hacks) enable the modification of a game to give the player an advantage, as well as the ability for the player to collect and aggregate virtual goods that would otherwise be purchased in-game. The rise of unauthorized digital goods and cheat software negatively affects video game companies and consumers by diverting significant revenue away from video game developers and publishers. It also increases the threat of consumer fraud, including through account takeovers via phishing or trying to steal the payment information connected to in-app purchases. Mpgh is an example of a site that provides "cheats" and reportedly offers several hundred thousand free cheats to over 5.6 million users. The site generates revenue through advertisements and by offering premium accounts, and Internet browsers reportedly detect and warn of malware on the site.

NEWALBUMRELEASES

Nominated as newalbumreleases.net. Reportedly hosted in the Czech Republic.

Newalbumreleases is an example of a website that reportedly provides unauthorized downloading of newly-released popular music that has not yet been commercially released to the public. According to right holders, the site hosts its infringing content on cyberlockers like Rapidgator, another notorious market, and provides users with links to the files for download. Takedown notices sent by right holders have been ineffective, and while the domain name registration was suspended briefly in 2018, service has since resumed.

PHIMMOI

Nominated as phimmoi.net. Hosted in Vietnam.

According to the movie industry, Phimmoi has become one of the most notorious piracy sites in the world with nearly 75 million monthly visits from 11 million visitors. Notwithstanding complaints about the site and an official letter of denunciation filed with the Vietnamese Ministry of Public Security, the authorities have yet to take action against the site.

PINDUODUO

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

Pinduoduo, a "social commerce" app, is now China's second largest e-commerce platform as measured by the number of users. Since its addition to the 2018 NML report, Pinduoduo has reported several actions that it has taken to decrease the availability of counterfeit goods and has indicated that it dedicates a significant percentage of its staff to these anti-counterfeit efforts. In February 2019, Pinduoduo launched a Brand Care program where it creates customized anti-counterfeiting plans for the brands that it deems to have the highest counterfeit exposure, in order to proactively detect and block listings. In September 2019, Pinduoduo released an English language version of its IP Protection portal, which is a notice-and-takedown system where right owners can make Pinduoduo aware of their trademarks and initiate and track takedown requests. Pinduoduo reports that these measures have resulted in a satisfactory counterfeit-free rate for some right holders, but other right holders note that the presence of counterfeits for some brands remains high.

Pinduoduo has also described the success of its other anti-counterfeiting programs. According to Pinduoduo, all merchants must provide personal identity cards and live 3-D facial scans before offering any items for sale. Pinduoduo says that it uses this information to hold the merchants personally accountable for sales of counterfeits, to provide verifiable information to right holders and law enforcement in relation to counterfeit investigation and enforcement activities, and to prevent sellers of counterfeit goods from re-registering as a merchant under a different account. Pinduoduo also reported that all merchants must submit a deposit that is used to reimburse purchasers of counterfeit goods. If Pinduoduo confirms the sale of counterfeits through a "secret buy," the deposit is forfeited at 10 times the value of an entire batch of goods. However, Pinduoduo does not have a clear and transparent policy for how or when sellers of counterfeit goods will be held accountable, when a merchant will be banned from the platform, or under what circumstances it will share information with right holders or law enforcement. Right holders convey that Pinduoudo's lack of a clear and transparent IP

enforcement policy is indicative of its nascent IP enforcement system that, while headed in the right direction, is currently insufficient to deal with the availability of counterfeits on its platform.

Pinduoduo has pioneered some anti-counterfeiting tactics, such as its 10-for-1 compensation policy, and its efforts designed to address counterfeiting on its platform are promising. However, it is currently premature to gauge the full impact of these efforts given the reported prevalence of counterfeits on the Pinduoduo platform. USTR encourages Pinduoduo to continue improving its IP enforcement system, develop a strict and transparent enforcement policy, increase cooperation with right holders and law enforcement in enabling offline enforcement, and address right holder concerns that search results outside of Pinduoduo's featured recommendation feeds still contain a high number of counterfeit listings.

PRIVATE LAYER-HOSTED SITES

Private Layer, reportedly operated from Panama with data center and hosting operations in Switzerland and elsewhere, is another example of a bulletproof hosting provider. This is the sixth consecutive year that the NML has stressed the significant international trade impact of Private Layer's hosting services and the pirate sites it hosts, such as Torrentz2. 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. Right holders report that Switzerland remains a popular host country for websites offering infringing content and the services that support them. Switzerland's new amendments to its copyright law, expected to go into force in early 2020, contain provisions to facilitate civil and criminal enforcement against online piracy. USTR encourages Swiss officials and right holders to avail themselves of these new provisions so that notorious online markets based in Switzerland will cease operations.

PROPELLER ADS

Nominated as propellerads.com. Based in Cyprus.

Many of the notorious online piracy markets in this year's NML are funded by advertising revenue. Propeller Ads is one of the world's largest online advertising networks with over 100 million desktop and mobile users per day viewing ads published by the network. Propeller Ads

accepts advertisements from many companies, including large worldwide brands as well as providers of illicit goods. Many websites have signed up with Propeller Ads to display the advertisements as banners on a webpage, pop-up or pop-under windows, or mobile push notifications. Propeller Ads reportedly does not screen the advertisements offered by its network, nor does it screen the websites that sign up with its network to display the advertisements. Right holders identify Propeller Ads as providing significant advertising revenue for many popular torrent sites, cyberlockers, and other pirate websites. Propeller Ads has also been linked to serious "malvertising" operations whereby malware is distributed through online advertisements.

In recent years, several governments and private sector stakeholders have developed innovative approaches to disrupting ad-backed funding of pirate 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 by maintaining an Infringing Website List that advertisers, agencies, adtech platforms, and other intermediaries can consult and decide voluntarily to cease ad placement on those sites.[32] 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.[33] At least one web browser with global popularity proactively filters ads that do not fall within the Coalition for Better Ads' "Better Ads Standards," which could disrupt ad revenue flows to pirate sites.[34]

[32] Operation Creative and the Infringing Website List (May 25, 2016), https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx.

[33] Report 2015–2016 of the Charter of Good Practices in Advertising for the Respect of Copyright and Neighboring Rights (Mar. 23, 2017), https://www.culture.gouv.fr/Espace-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.

[34] Improving User Experience with the Better Ads Standards, https://admanager.google.com/home/resources/feature-brief-better-ads-standards; *see* Coalition for Better Ads, https://www.betterads.org.

RAPIDGATOR

Nominated as rapidgator.net. Related sites include rg.to. Reportedly hosted in Russia, but utilizes reverse proxy services to mask the location of its hosting servers.

Commenters from the book publishing, movie, and music industries all nominated Rapidgator, one of the largest file sharing websites in the world, for inclusion on this year's NML. Right holders report that it is easy to find unlicensed high-quality and recent content. Rapidgator collects revenue through its premium membership and subscription plans and employs rewards and affiliate schemes to compensate users based on downloads and sales of new accounts. German courts issued preliminary decisions finding Rapidgator liable for copyright infringement, and a Russian court ordered ISPs to block access to the website.

RARBG

Nominated as rarbg.to. Hosted in Bosnia and Herzegovina.

Rarbg is a globally popular torrent site even though it is subject to blocking orders in Australia, Belgium, Denmark, Finland, Greece, India, Indonesia, Ireland, Italy, Malaysia, Portugal, and the United Kingdom. Right holders from the movie, television, and music industries report that unlicensed high-quality and recent content can be found easily on this site. Rarbg reportedly generates revenue through advertisements and pay-per-install of potential malware.

RUTRACKER

Nominated as rutracker.org. Hosted in Russia.

RuTracker remains one of the most popular torrent sites in the world with almost 14 million active accounts, despite a still-outstanding order issued in 2015 by the Moscow City Court that ordered ISPs in Russia to block the domain. The Russian search engine Yandex allegedly indexes links to RuTracker despite it being illegal to do so in Russia according to a recent law.

SCI-HUB

Nominated as sci-hub.io. Related sites include sci-hub.cc, sci-hub.ac, sci-hub.bz, gen.lib.rus.ec, bookre.org, booksc.org, book4you.org, and b-ok.org. Hosted in Russia.

Right holders continue to report that Sci-Hub and its mirror sites[35] facilitate unauthorized access to over 70 million journal articles and academic papers. A 2018 study found that 85% of articles published in toll-access journals were available for free in Sci-Hub's database, more than what is available legally to many major institutional subscribers.[36] Right holders allege that at least some of the material available on Sci-Hub was obtained through credentials of victims of phishing scams, and there are documented instances where Sci-Hub paid for credentials of unknown provenance to access university subscriptions. Right holders have been taking legal action against Sci-Hub and have been successful in having U.S. district courts grant them injunctions, damages, and control over Sci-Hub's U.S.-based domain names. Sci-Hub is subject to blocking actions in Denmark, France, Germany, Italy, Portugal, Russia, and the United Kingdom.

LibGen, also known as the "Library Genesis Project," is another nominated notorious market that includes the libgen.is, libgen.lc, and libgen.me domains. LibGen is a known related site to Sci-Hub that reportedly obtains most of its pirated scientific, technical, and medical journal articles from Sci-Hub.

SEASONVAR

Nominated as seasonvar.ru. Hosted in Russia.

Seasonvar is one of the world's most popular websites for streaming pirated content. According to right holders, more than 12,000 different TV series are available on Seasonvar without authorization. Variants of this website are subject to blocking orders in Russia.

---

[35] A "mirror site" is a website that is a proxy or clone of an original site and may offer the same, new, or cached 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.

[36] D. Himmelstein et al., Sci-Hub Provides Access to Nearly All Scholarly Literature, 7 eLife e32822 (Mar. 1, 2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5832410.

SHOPEE

Nominated as shopee.sg. Related sites include shopee.com.my, shopee.ph, shopee.co.th, shopee.vn, shopee.tw, and shopee.co.id. Also available as a mobile app. Reportedly hosted in China.

Shopee is an online and mobile e-commerce market based in Singapore and serving the Southeast Asian market. Right holders report very high levels of counterfeits being sold on all of Shopee's platforms, including counterfeit medicine. During the notice and takedown process, Shopee reportedly seeks more information from right holders than what it states on its platforms and acts with no urgency even after right holders provide the additional information. According to right holders, removals of infringing products can take more than two weeks, and there is no process to remove or penalize sellers of counterfeit goods.

SNAPDEAL

Nominated as snapdeal.com. Related sites include shopo.in and exclusively.com. Also available as a mobile app. Hosted in India.

Snapdeal, one of India's largest e-commerce platforms, is known as a place to purchase counterfeit watches and shoes. According to a November 2018 survey, 37% of its customers reported that they had received a counterfeit product from Snapdeal. In July 2019, Snapdeal's founders were arrested for selling counterfeit products. Right holders have also sued Snapdeal for selling counterfeit goods.

TAOBAO

Nominated as taobao.com. Also available as a mobile app. Hosted in China.

Owned by Alibaba Group, Taobao is one of China's largest e-commerce platforms. Taobao was first listed in the NML in 2016 in response to significant right holder interest and nominations, and subsequent reports identified a number of recommendations to curb the offer and sale of infringing products on Taobao.[37] Alibaba has reported that Taobao has taken a

[37] In the 2018 NML, USTR recommended that Alibaba should: (1) expand its reported ban on automotive air bags and air bag components to the taobao.com platform and to widely counterfeited products not ordinarily sold in consumer-to-consumer marketplaces; (2) enforce its current policies related to automotive parts; (3) improve the

number of actions to implement these recommendations and address other right holder concerns. However, according to right holders, Taobao remains one of the largest sources of counterfeit sales in China. Some right holders commended Taobao's improved response times and policies, but complained about the number of counterfeits offered for sale on Taobao and the lack of transparency regarding filters and other proactive anti-counterfeiting measures. USTR will continue to monitor whether Taobao's actions are demonstrably effective in addressing ongoing complaints about the pervasiveness of counterfeit goods on Taobao.

THEPIRATEBAY

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

While some ThePirateBay websites have been shut down over the past year, right holders continue to report high levels of infringing activities taking place on this platform. As one of the first bittorrent indexing websites and one of its most vocal in openly promoting piracy, ThePirateBay continues to be one of the most frequently visited websites in the world. Authorities around the world have found ThePirateBay and its operators liable for infringing copyright, including most recently in Romania and Greece where ISPs were ordered to block the site. Enforcement actions have also taken place in Argentina, Australia, Austria, Belgium, Denmark, Finland, France, Iceland, Indonesia, Ireland, Italy, Malaysia, the Netherlands, Norway, Portugal, Spain, Sweden, the United Kingdom, and at the Court of Justice of the European Union. Yet, ThePirateBay has managed to continue operating by constantly hopping to new top level domains.

TOKOPEDIA

Nominated as Tokopedia.com. Also available as a mobile app. Hosted in Indonesia.

Tokopedia is one of Indonesia's largest e-commerce markets. It serves as a platform for third party vendors to post listings, and the site offers a vast range of goods, including clothes, electronics, and textbooks. Right holders report finding high rates and high volumes of

---

effectiveness of its repeat-infringer policy; (4) seek input from SMEs (not just trade associations); and (5) improve tools to prevent the unauthorized use of product images.

counterfeit clothing, counterfeit cosmetics and accessories, pirated textbooks, and other pirated English-language materials on this platform. Products advertised as "replicas" of genuine brands are allegedly sold openly on the site. Right holders report difficulties with enforcement of their rights as the reporting procedures provided by this platform are difficult to navigate, the documentation requirements are onerous for right holders, and the platform makes little effort to deter repeat infringers. In fact, some sellers of counterfeit products have been in business on Tokopedia for allegedly as long as seven years. The continued proliferation of counterfeit goods year after year from these sellers calls into question the overall effectiveness of Tokopedia's anti-counterfeiting measures.

TORRENTZ2

Nominated as torrentz2.eu. Related sites include torrentz2eu.xyz and torrentz2.is. Reportedly hosted by Private Layer in Bulgaria, but utilizes reverse proxy services to mask the location of its hosting servers.

Torrentz2 emerged as the second version of the original Torrentz.eu site, which shut down in 2016. This site indexes and aggregates over 80 other torrent sites and is reported to currently link to over 61,110,000 torrents, many of which are for pirated content. Torrentz2 is subject to blocking orders in Australia, Belgium, Denmark, Greece, India, Italy, and Portugal.

TURBOBIT

Nominated as turbobit.net. Hosted in the Netherlands.

Turbobit was nominated as one of the top cyberlocker sites for music piracy with nearly 360,000 links to unlicensed songs in the past year. Popular in France and Turkey, Turbobit reportedly derives revenue from premium accounts, advertising placed on the site, and through revenue-sharing arrangements with the uploaders of popular content that will attract the most traffic to the site. Other music piracy sites allegedly use Turbobit to store infringing files for download.

UPLOADED

Nominated as uploaded.net. Related sites include ul.to and uploaded.to. Hosted in Germany.

This cyberlocker reportedly operates through multiple redundant domains and provides access to a broad range of infringing content such as unlicensed digital books, movies, TV shows, and music, including pre-release music. Uploaded uses a combination of multi-tiered subscriptions, a referral program, and a rewards scheme to generate revenue, incentivize unauthorized sharing of popular copyright-protected content, and expand its user base. For example, the site pays rewards to users based on large file sizes, such as those for copyright-protected movies and TV shows. It also pays rewards based on the number of times a file is downloaded, paying more for downloads originating from so-called "Top-Countries." Courts in Germany, India, and Italy have found the site liable for copyright infringement and issued orders against the site. For example, in 2016, a court in Germany found that the operator of this website was liable for content shared by its users because it failed to proactively combat piracy. However, a higher regional court reversed that ruling in 2017 and found the operator not liable. In November 2018, the German Supreme Court referred questions on this case to the Court of Justice of the European Union, where it is still pending.

UPTOBOX

Nominated as uptobox.com. Related sites include uptostream.com. Reportedly hosted in France, but utilizes reverse proxy services to mask the location of its hosting servers.

UpToBox is a direct download cyberlocker that also allows streaming and embedding. Pirate sites in Europe reportedly embed infringing content from UpToBox on their own websites to generate advertising revenue or generate revenue by linking to pirated content on UpToBox through pay networks such as adf.ly. The site claims to incentivize users to upload large files, such as copyright-protected movies and TV shows, and offers a referral/reseller program to attract more users.

VK

Nominated as vk.com. Also available as a mobile app. Hosted in Russia.

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 its neighboring countries. VK reportedly facilitates the distribution of copyright-infringing files, with thousands of infringing videos identified by the U.S. motion picture industry each month. Social networking sites can serve as a uniquely valuable communication platform, enabling beneficial commercial, cultural, and social exchanges. However, they should do so in ways that do not involve the active facilitation of copyright infringement. Reports that VK is taking steps to address piracy and is constructively engaging with the music industry are encouraging. VK's parent company, Mail.Ru Group, recently signed an Anti-piracy Memorandum aimed at establishing a legal procedure to reduce the availability of pirated content based on voluntary takedown by the platforms when notified by local right holders. USTR encourages VK to institutionalize appropriate measures to promote respect on its platform for IP of all right holders which are comparable to those measures used by other social media sites.

WARMANE

Nominated as warmane.com. Utilizes reverse proxy services to mask the location of its hosting servers.

Warmane is an example of an unauthorized third-party server that hosts online games for users to play without paying the monthly subscription fees charged by the legitimate site hosting the particular online game. According to right holders, this particular server enables approximately 20,000 active users to play World of Warcraft, an online video game, without paying the monthly subscription fee established by the game's publisher.

Firestorm-Servers.com (also fstorm.cc) is another example of an unauthorized third-party server that reportedly enables approximately 5,000 users to play World of Warcraft without paying the monthly subscription fee to the publisher.

Physical Markets

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

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

- effective border enforcement measures to prevent the exportation of counterfeit and pirated goods manufactured in their countries, the importation of such goods into their countries, and the transiting or transshipment of such goods through their countries on the way to destination countries;
- the ability for customs and criminal authorities to detain, seize, and destroy counterfeit and pirated goods entering into and exiting from free trade zones;[38]
- robust border enforcement authority to interdict small consignment shipments, such as those sent through postal or express-courier services;
- asset forfeiture, which is a tool that can be used to reach owners of the markets or facilities where infringing products are 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 products that threaten health and safety.

Another key to reducing piracy and counterfeiting lies in the ability to influence demand and redirect consumers to legitimate alternatives.

[38] For a description of free trade zones, see the 2018 NML.

ARGENTINA

La Salada, Buenos Aires

La Salada, an area covering about 50 acres that incorporates three markets, remains on the NML because it will take sustained enforcement action and stronger legal tools to reverse its long-standing reputation as one of the largest black markets for illegal goods in the region, including IP-infringing goods. The last significant enforcement action occurred in 2017, and the number of vendors selling counterfeit goods has reportedly returned to pre-2017 levels. La Salada is also home to small factories that reportedly assemble and finish counterfeit goods, and counterfeit goods purchased at La Salada are resold throughout the city, country, and region.

BRAZIL

Rua 25 de Março, Sao Paulo

The region surrounding Rua 25 de Março in Sao Paulo is notorious for hosting shopping malls that sell counterfeit and pirated goods, including Galeria Pagé, Shopping 25 de Março, and Santa Ifigenia. Despite recent enforcement efforts, this market remains the most notorious counterfeit market in the country and is reportedly a distribution center for counterfeit and pirated goods throughout Sao Paulo. In January 2019, a multinational team of enforcement officials and right holders raided 80 stores in Rua 25 de Março and seized and destroyed approximately ten tons of counterfeit toys and cosmetics, with an estimated value of $2.6 million. In May 2019, Brazilian officials conducted another raid in this area and seized approximately 500,000 counterfeit watches worth approximately $12.6 million. Despite these successes, commercial landlords are reportedly using civil litigation to reopen shops known for selling counterfeit and pirated goods, and there have been no recent criminal prosecutions of these landlords.

CAMBODIA

Central Market, Phnom Penh

Central Market is a sprawling market and historic landmark in Phnom Penh. Stores throughout the market reportedly sell many kinds of counterfeit goods, including clothing and

leather goods. While authorities have conducted periodic raids of the market, right holders have not observed any improvement. USTR urges Cambodia to conduct more frequent raids to eliminate the illicit goods from this market.

CHINA

As in past years, several commenters continue to identify China as the primary source of counterfeit products. Together with Hong Kong, through which Chinese merchandise often transships, China accounted for 85% of the value (measured by manufacturer's suggested retail price) and 87% of the volume of counterfeit and pirated goods seized by U.S. Customs and Border Protection in 2018. Some Chinese markets, particularly in larger cities, have adopted policies and procedures intended to limit the availability of counterfeit merchandise. However, these policies are not widely adopted, and enforcement remains inconsistent. Consequently, major notorious markets remain highly visible even in China's biggest cities. While right holders acknowledged that raids and seizures continued at some of these markets, enforcement actions in other markets were virtually non-existent.

On January 15, 2020, the United States and China signed an historic and enforceable agreement on a Phase One trade deal that requires structural reforms and other changes to China's economic and trade regime in the areas of intellectual property, technology transfer, agriculture, financial services, and currency and foreign exchange. The IP chapter addresses numerous longstanding concerns, including in the area of enforcement against pirated and counterfeit goods. In particular, the IP chapter obligates China to significantly increase the number of enforcement actions against pirated and counterfeit goods at physical markets in China and that are exported or in transit.

USTR encourages China to adopt and expand the scope of robust enforcement actions to more effectively combat the scale of the reported problem in China, with a special focus on the following key markets:

Garment wholesale and retail malls near Zhanxi Road, including the Jinlongpan, Kindo, Yulong, and Zhanxi markets, Guangzhou, Guangdong Province

These large, mall-sized markets near Zhanxi Road in Guangzhou are located within a mile of each other and offer mainly apparel and shoes. Right holders report that counterfeit products composed between 30%–70% of merchandise at these markets. These markets are popular with foreign buyers who reportedly purchase counterfeit goods to ship around the world. There is no apparent IP enforcement in this area beyond posters hung at various places urging vendors and buyers to respect IP.

Southern Watch Trade Center, Guangzhou, Guangdong Province

This two-story market with at least 150 vendors is adjacent to the garment wholesale markets near Zhanxi Road. According to right holders, virtually all of the stores sell counterfeit watches, many of which are reportedly high-quality imitations selling for hundreds of dollars. Despite the presence of security personnel, there is reportedly little IP enforcement at this market. The Southern Watch Trade Center is promoted by tour guides and is also a popular destination for foreign buyers looking to export counterfeit goods.

Huaqiangbei Electronics Malls, including the Yuan Wang, Long Sheng, and Man Har Digital Plaza Malls, Shenzhen, Guangdong Province

The malls in this area each contain several hundred vendors of electronic devices and components. Right holders report that vendors offer counterfeit computer chips, wiring, capacitors, and LEDs used by manufacturers of counterfeit consumer electronic devices in China and around the world. Vendors at these malls also offer counterfeit smartphones, SD cards, and video game consoles. Enforcement actions in these malls are reportedly rare, with the mall operators taking repeated steps to thwart right holders' efforts.

Luohu Commercial City, Shenzhen, Guangdong Province

This is a well-known mall located next to the Luohu border crossing between Shenzhen and Hong Kong. Right holders report that its location and size gives it a high international profile and makes it a popular destination for tourists and cross-border travelers. Reportedly half of the

merchandise at the market consists of counterfeit or pirated goods. Law enforcement conducts regular raids at the market and connected warehouses and factories, but the continued prevalence of infringing products requires increased efforts.

Silk Market, Beijing

Listed in the NML since 2011, Silk Market remains a market of concern in 2019 due to the lack of fundamental changes in its IP enforcement. Right holders report that most of the merchandise in this market continues to be counterfeit. While fewer visibly infringing products were reported in March 2019 due to heightened enforcement around World Consumer Rights Day, the enforcement level soon tapered off and infringing products returned. Right holders have recognized temporary successes in suspending sellers from the market, but the overall enforcement environment has remained difficult with market operators refusing to cooperate with right holders.

Wu'ai Market, Shenyang, Liaoning Province

This is the largest market in Northeastern China, with over 6,000 shops, and is a hub for the distribution of counterfeit shoes, handbags, luggage, and apparel throughout the region. In 2018, authorities brought 29 trademark infringement cases against vendors at this market. However, the combined value of those cases amounted to only $12,666, and existing efforts appear largely ineffective at addressing the scale of the infringement problem.

Yiwu International Merchandise City, Yiwu, Zhejiang Province

This is the biggest small commodities market in the world, and its 50,000 vendors sell almost every conceivable consumer product, mostly in bulk, to global clientele. Many of the goods sold in this market are unbranded and non-differentiable, but right holders report that some vendors, perhaps eyeing higher profit margins, openly display and sell infringing handbags, shoes, and apparel. Right holders also report that local authorities have conducted regular raids and seizures against shops and related warehouses associated with infringing products and have levied administrative and criminal penalties against infringers. The operator of the market has

also cooperated with right holders by posting warnings against counterfeiters, creating a list of protected brands, and distributing IP protection brochures. However, right holders report that these efforts have been inadequate at reducing the visibility of infringing products at this market.

ECUADOR

La Bahia Market, Guayaquil

La Bahia Market is a large market where various counterfeit products—mainly apparel, footwear, DVDs, and CDs—may be found, and it remains on the NML in 2019. Vendors reportedly sell counterfeit products in open view of the public and largely with impunity. No enforcement operations, raids, or seizures were reportedly taken last year. USTR urges Ecuador to ensure that there are adequate criminal penalties and strong enforcement to deter counterfeiters.

INDIA

Tank Road, Delhi

Tank Road remains on the NML in 2019. Right holders confirm that this market continues to sell counterfeit products, including apparel and footwear. Wholesale counterfeit goods are also reportedly supplied from this market to other Indian markets, including Gaffar Market and Ajmal Khan Road. The wholesale vendors appear to operate freely, allowing them to build well-established businesses over many years.

Millennium Centre, Aizawl, Mizoram

The five-story Millennium Centre on the eastern border of India is a major market for goods produced in China, Korea, and Thailand. Reports note that a majority of the clothing and electronic items found at this location are counterfeit.

Heera Panna, Mumbai

This indoor market houses approximately 140 shops reportedly selling high-quality counterfeit watches, leather goods, shoes, consumer electronics, and cosmetics. According to

right holders, IP enforcement in this market is very difficult because the market and store owners are well-protected by local authorities and law enforcement.

Kidderpore, Kolkata

Locally known as "Fancy Market," Kidderpore reportedly sells counterfeit consumer electronics, apparel, cosmetics, and pirated software and media, often at wholesale quantities.

INDONESIA

Mangga Dua Market

Mangga Dua is a popular market in Jakarta selling a variety of counterfeit goods, including handbags, wallets, children's items, clothing, and fashion accessories, with reportedly minimal government enforcement to combat the rampant sale of the counterfeit goods. USTR urges Indonesia 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 NMLs.

KYRGYZ REPUBLIC

Dordoy/Dordoi Market, Bishkek

This market stretches for more than a kilometer on the north-eastern outskirts of Bishkek and is one of the largest markets in Asia. Right holders report that many kinds of counterfeit goods are available at the Dordoy Market. While the Kyrgyz Republic has recently increased efforts to uphold IP rights and diminish illicit trade in the country in general, no specific action has been taken against the Dordoy Market.

MALAYSIA

Petaling Street Market, Kuala Lumpur

Petaling Street Market is a well-known market in Kuala Lumpur that sells counterfeit items, including watches, shoes, handbags, wallets, sunglasses, and other consumer goods. USTR continues to urge Malaysia to launch a sustained, coordinated, and effective effort to tackle

widespread counterfeiting and piracy at Petaling Street Market and other markets throughout Malaysia, such as Plaza GM and Tamaran Johor Jaya.

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. Right holders report that El Tepito remains dangerous, making it nearly impossible for right holders to enforce their rights. El Tepito is also reportedly a major distribution hub for counterfeit goods in local markets across Mexico. Infringing items sold at El Tepito include video games, modified game consoles and devices that enable the circumvention of technological protection measures, counterfeit apparel, and counterfeit medicine. USTR 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 products in markets across the country. USTR further urges Mexico to enforce against counterfeit and pirated goods moving in-transit.

Mercado San Juan de Dios, Guadalajara

Mercado San Juan de Dios, located in Guadalajara, is the largest indoor market in Latin America with approximately 3,000 vendors, and attracts 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 devices that enable the circumvention of technological protection measures.

PARAGUAY

Ciudad del Este

Ciudad del Este has been named in the NML or the Special 301 Report for over 17 years. The border crossing at Ciudad del Este and the city itself have long been known as a regional hub for the manufacture, assembly, and distribution of counterfeit and pirated products in the Brazil-Argentina-Paraguay tri-border area and beyond. Ciudad del Este thrives on a mainly Brazilian

customer base attracted by the 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. While USTR commends the recent efforts by Paraguay to improve IP enforcement in this market, such as increasing by 73% the number of IP-related investigations compared to 2018, these efforts remain inadequate to stem the tide of counterfeit products. Notably, the increase in investigations did not lead to an appreciable increase in counterfeit-related convictions. The alleged transit of counterfeit pesticides from China through Ciudad del Este adds a human health dimension to the issue that requires an urgent response from authorities. USTR urges Paraguay's authorities to improve coordination and information sharing among its enforcement agencies, particularly between the National Directorate of Intellectual Property (DINAPI) and the Attorney General.

PERU

Polvos Azules, Lima

Polvos Azules is a popular shopping center located in the heart of Lima. Vendors reportedly sell a broad range of illicit goods, including counterfeit clothing, shoes, appliances, toys, and electronics. USTR commends Peruvian authorities for conducting raids in this market to seize counterfeit goods and urges Peru to continue conducting raids as right holders remain concerned that counterfeit goods remain widely available. Right holders also report that, due to the strong influence of business interests benefiting from the illicit trade, local authorities may be reluctant to commit resources commensurate with the scope of the problem.

PHILIPPINES

Greenhills Shopping Center, San Juan, Manila

Greenhills Shopping Center is a large mall located in San Juan, Metro Manila. The market has been the subject of raids and monitoring by enforcement officials. However, sellers have reportedly been able to evade enforcement by moving to new stalls or by discreetly selling illicit goods behind counters and underneath tables. Large volumes of counterfeit handbags and shoes are reported to be sold openly to the public, and counterfeit clothing, toys, games,

computer and phone accessories, household goods, jewelry, watches, and electronics also remain available. USTR urges the Philippines to enhance and sustain enforcement actions to deter sales of counterfeit goods at this market.

RUSSIA

Sadovod Market, Moscow

Sadovod Market is the largest trading center for consumer goods in Russia, spanning nearly 100 acres with over 8,000 stores frequented by approximately 36 million people a year. Businesses from across Russia and Central Asia allegedly use the market to make wholesale purchases of counterfeit apparel, accessories, and toys, which are widely available. Vendors reportedly openly admit that the products they sell are counterfeit, and they facilitate the trade in these illicit goods by claiming that the goods are of superior quality. The open trade in counterfeit goods suggests a lax attitude toward IP enforcement, and USTR encourages the local authorities to take appropriate action to help curtail the illicit trade in counterfeit goods.

Gorbushkin Dvor Mall, Moscow

While many physical notorious markets sell counterfeit apparel, footwear, and luxury goods, Gorbushkin Dvor Mall is known for its high volume of counterfeit electronics and high-end home appliances, such as refrigerators, washing machines, and flat screen televisions. The local authorities reportedly do not have a presence in this market and do not cooperate with right holders.

SPAIN

Els Limits de La Jonquera, Girona

Els Limits de La Jonquera is a popular market in Girona, a province in the Catalonia region of Spain that is popular with tourists and close to the French border. It appears that a substantial volume of sales of counterfeit luxury and other items continue to be sold at this market due to a lack of sustained enforcement efforts. In recent years, it has been reported that some raids were thwarted by the practice of stitching labels at the point of sale and that judicial orders obtained

by right holders were later reversed. The popularity of stores selling counterfeits is apparently driving sellers of legitimate goods out of the market. USTR urges Spain to work with landlords, investigate warehouses and supplies, and ensure that enforcement actions against counterfeit merchants are effective and sustained.

THAILAND

Patpong Market, Bangkok

The Patpong Market is a popular night market in Bangkok selling a range of counterfeit goods, including sports apparel, watches, handbags, pharmaceuticals, and pirated DVDs. Despite monitoring and enforcement actions by the Royal Thai Police and the Economic Crime Suppression Division, right holders report that the quantity of counterfeit goods available remains high. USTR encourages Thailand to continue its enforcement efforts to prevent further harm to legitimate right holders.

TURKEY

Grand Bazaar, Istanbul

The Grand Bazaar in Istanbul 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, some of which reportedly sell counterfeit jewelry, watches, perfumes, cosmetics, wallets, handbags, and leather goods. Although the number of vendors selling counterfeit goods has decreased over the past few years as rents have increased, the scale of the problem remains significant.

UKRAINE

7th Kilometer Market

The 7th Kilometer Market is one of the largest wholesale and retail markets in Europe and is an important contributor to the local economy with an estimated 150,000 customers per day. However, vendors in this market sell large volumes of counterfeit goods, reportedly sourced from China, including clothing, jewelry, luxury goods, and perfume. According to right holders and local media, the market operates according to its own laws and with its own police force.

Landlords disclaim liability for the rampant and open sale of counterfeits, and enforcement actions are rare. As a result, sellers continue to engage in counterfeit sales with virtual impunity. USTR urges Ukraine to undertake serious enforcement actions to deter sales of counterfeit goods at this and other markets in Ukraine.

Barabashova, Kharkiv

Barabashova is the largest market in eastern Ukraine and is reportedly a popular destination for shoppers from other former-Soviet countries. Right holders report that this market is the center for the distribution of IP-infringing products in the region. The operators of the market have been reluctant to cooperate with right holders, and local law enforcement reportedly lacks interest in enforcing IP rights.

UNITED ARAB EMIRATES

Ajman China Mall, Ajman

Ajman China Mall continues to serve as a significant market for China-sourced counterfeit goods. A substantial portion of the goods sold at this market and adjacent buildings is distributed to foreign markets, particularly in the Middle East, North Africa, and Europe. Right holders report few successes of convincing Ajman Police and the Ajman Department of Economic Development (DED) to raid this market, although they have had many successes with IP enforcement elsewhere in the emirate. An estimated 80% of the companies operating in the Ajman China Mall are Chinese, and China supports it as part of the China Council for the Promotion of International Trade's 2010 "Going Out" strategy paper.

Markets in Deira District, Dubai

The Deira District is home to a number of markets including the Dubai Souk, Deira Old Souk, Dubai Gold Souk, Dubai Spice Souk, and Perfume Souk. Right holders report that these markets are well-known among tourists and locals alike for selling IP-infringing goods. Right holders report that Dubai Police and the Dubai Department of Economic Development (DED) conduct frequent raids against sellers of infringing products at these markets. However, while

authorities will fine sellers for IP violations, they usually do not enact additional penalties, such as closing the shops of repeat violators or bringing criminal actions, and the amounts of the fines are not at deterrent levels. USTR encourages authorities in Dubai to increase penalties against sellers of infringing products in order to effectively deter such activities.

VIETNAM

Ben Thanh Market, Ho Chi Minh City

Ben Thanh Market in Ho Chi Minh City, along with Dong Xuan Market in Hanoi (listed below), are two of the most well-known retail markets in Vietnam. Ben Thanh Market is one of the oldest of its kind in Ho Chi Minh City and is reportedly a symbol of the city, attracting many tourists and visitors. It hosts a large variety of goods, ranging from foodstuffs and locally-produced souvenirs to apparel, footwear, accessories, and cosmetics, much of which is reportedly counterfeit. According to right holders, authorities conduct relatively frequent raids at these markets. For example, in July and August 2019, local authorities reportedly conducted two raids that seized infringing goods with a street value of $14,200. However, these efforts appear inadequate for a market that is the size of an entire city block, and vendors selling infringing goods are reportedly undeterred by these measures. USTR urges Vietnam to enhance and sustain enforcement actions to deter sales of counterfeit goods and labels at these and other nominated markets in Vietnam.

Dong Xuan Market, Hanoi

Dong Xuan is a three-story market located in the old quarter of Hanoi, and its vendors sell a variety of goods, including reportedly counterfeit apparel, footwear, accessories, and cosmetics. According to right holders, local authorities asked vendors to sign a commitment to not sell infringing goods, and fewer locals are reportedly shopping for infringing goods at this market due to generally rising living standards and changing tastes among local consumers. However, the overall IP problem here remains significant, in part because of the size of the market.

Public Information

The 2019 Notorious Markets List is the result of the tenth out-of-cycle review of notorious markets, which USTR initiated on August 19, 2019, through a Federal Register Request for Public Comments. The request and responses are available at https://www.regulations.gov, Docket Number USTR-2019-0013. USTR developed the 2019 NML in coordination with the federal agencies represented on the Special 301 Subcommittee of the Trade Policy Staff Committee (TPSC). Information about Special 301 and other intellectual property-related processes and issues is available at https://ustr.gov/issue-areas/intellectual-property.

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