OFFICE *of the* UNITED STATES TRADE REPRESENTATIVE

EXECUTIVE OFFICE OF THE PRESIDENT

2018 Out-of-Cycle Review of Notorious Markets

Table of Contents

Overview of the Results of the 2018 Out-of-Cycle Review of Notorious Markets

Commercial-scale copyright piracy and trademark counterfeiting[1] cause significant financial losses for U.S. right holders and legitimate businesses, undermine critical U.S. comparative advantages in innovation and creativity to the detriment of American workers, and pose significant risks to consumer health and safety. The Notorious Markets List (List) highlights prominent and illustrative examples of online and physical marketplaces that reportedly engage in and facilitate substantial piracy and counterfeiting. A goal of the List 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 marketplaces because they exemplify global counterfeiting and piracy concerns and because the scale of infringing activity in these marketplaces can cause significant harm to U.S. intellectual property (IP) owners, consumers, legitimate online platforms, and the economy. Some of the identified markets reportedly host a combination of legitimate and unauthorized activities. Others openly or reportedly exist solely to engage in or facilitate unauthorized activity.

The List includes several previously identified markets because owners, operators, and governments failed to address previously stated concerns. Other previously identified markets may not appear in the present List for a variety of reasons, including that: the market has closed or its popularity or significance has diminished; enforcement or voluntary action has reduced or eliminated the prevalence of IP-infringing goods or services; market owners or operators are cooperating with right holders or government authorities to address infringement; or the market is no longer a noteworthy example of its kind. In some cases, online markets in the 2017 List are not highlighted this year but improvements are still needed, and the United States may continue to raise concerns related to these markets on a bilateral basis with the countries concerned.

The List is not an exhaustive account of all physical and online markets worldwide in which IP infringement may take place. The List does not make findings of legal violations. Nor does it reflect the U.S. Government's analysis of the general IP protection and enforcement climate in the countries connected with the listed markets. A broader analysis of IP protection

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

and enforcement in particular countries or economies is presented in the annual Special 301 Report published at the end of April each year (please refer to the Public Information section at the end of this document).

USTR developed the List under the auspices of the annual Special 301 process[2] and solicited comments through a Request for Public Comments published in the Federal Register (WWW.REGULATIONS.GOV, Docket Number USTR-2018-0027). The List is based predominantly on publicly available information. USTR has identified notorious markets in the Special 301 Report since 2006. In 2010, USTR announced that it would begin publishing the List separately from the annual Special 301 Report, pursuant to an Out-of-Cycle Review (OCR). USTR first separately published the List in February 2011.

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

Positive Developments Since the 2017 Out-of-Cycle Review of Notorious Markets

Since the release of the 2017 Notorious Markets List, some market owners and operators undertook notable efforts to address widespread availability of pirated or counterfeit goods in their markets. The United States commends these efforts and encourages governments, right holders, service providers, and the owners and operators of these and other markets, including those newly identified in the 2018 List, to engage in sustained and meaningful efforts to combat piracy and counterfeiting.

During the past year, some online markets have been the subject of successful enforcement efforts. A notable development was the apparent shuttering, following the launch of a criminal investigation in Vietnam and industry engagement, of piracy services that had been included in previous Lists and that had operated under the names **123movies.to** and **gomovies.to**.[3] Also, action against YouTube-ripping sites has continued in 2018, following the shutting down of **youtube-mp3.org** in 2016.[4] For example, sites such as pickvideo.net, video-download.co and easyload.co have reportedly stopped promoting or allowing unauthorized audio ripping from music videos and legitimate streaming services. Additionally, the Ukrainian cyberpolice reportedly took action against onlainfilm.co, a streaming site with half a million users. Peru also took significant action in 2018 against online piracy, including Indecopi action against the pirate sites of Roja Directa and International Federation of the Phonographic Industry (IFPI) action against 19 sites, 13 of which are now reportedly offline. Moreover, Peru has taken action to curb signal piracy, which has reportedly experienced a significant decrease in the last two years. In Romania, the Bucharest Tribunal ruled in a November 2018 decision to take required action against three pirated movie sites: filmhd.net, filmeonline2013.biz, and **thepiratebay.org**.

There have also been notable actions taken against Internet Protocol television (IPTV) providers. In September 2018, FAB IPTV, a major provider of unlicensed streaming content in

[3] Matthew Dunn, *The World's Largest Piracy Site Has Announced It's Closing Down For Good, Urges People To Buy Content*, News Corp Australia (Mar. 21, 2018), https://www.news.com.au/technology/online/piracy/the-worlds-largest-piracy-site-has-announced-its-closing-down-for-good-urges-people-to-buy-content/news-story/728380a53ddd4c7c576081b6a13f4d6d.

[4] Only previously and presently listed markets appear in bold text. In contrast, markets that have not appeared on this or the prior years' Lists are not in bold text. When a paragraph includes multiple references to a market, only the first instance appears in bold text. Previously nominated markets are not bolded unless they have also been listed.

the United Kingdom, announced that it was shutting down following a Europol-led raid, following a year-long investigation involving the Garda National Bureau of Criminal Investigation, Police Scotland, the UK Intellectual Property Office, the Audiovisual Anti-Piracy Alliance (AAPA), and Federation Against Copyright Theft (FACT). In Sweden, the Stockholm Patent and Market court convicted and fined individuals connected to the IPTV operation Advanced TV Network (ATN) in a landmark ruling, and ATN has since gone bankrupt.

Country code top-level domain (ccTLD) registrars continue to step up efforts to address domain name abuse, including domain name registrations associated with infringing activity. For example, in June 2018, the European Registry of Internet Domains (EURid) and the International AntiCounterfeiting Coalition (IACC) announced a joint initiative to combat cybercrime on .eu and .ею domain names, with a focus on clearing the registration database of fraudulent domain names through the exchange of knowledge and support pertaining to cybercrime, specifically counterfeiting and piracy.[5] Denmark's ccTLD body, DK Hostmaster, created stricter identity checks at the end of 2017, which DK Hostmaster claims have helped combat IP infringement. In fact, DK Hostmaster reported that the share of "online stores" with .dk domain name registrations suspected of infringing IP declined from 6.73% in November 2017, to 1.03% in March 2018.[6] The United States encourages other countries and ccTLDs registrars to take similar steps.

Additionally, registrars continue to take actions to combat the online sale of counterfeit medicines. Following the shutting down of **Nanjing Imperiosus Technology Co., Ltd**, other registrars, including Nics Telekomünikasyon Tic Ltd. Şti. (Turkey) and CV. Jogjacamp (Indonesia), have reportedly taken action to disrupt illicit online pharmacy operators.

Regarding physical marketplaces, several countries have significantly stepped up enforcement. Since the January 2017 eviction of 2,000 street vendors reportedly selling infringing goods from the Once neighborhood, Buenos Aires authorities have carried out extensive work reconstructing the neighborhood's train station façade and renovating streets and sidewalks with an investment of 9.5 million pesos. The City reallocated the evicted street vendors into three nearby commercial facilities, together with street vendors evicted from the

[5] EURid and IACC Team Up to Fight Cybercrime (June 27, 2018), https://eurid.eu/en/news/eurid-and-iacc-team-up-to-fight-cybercrime/.
[6] Danish Internet Forum, *Crime Prevention on the Internet* (2018), https://www.dk-hostmaster.dk/sites/default/files/2018-04/DIFOs-indsats-for-at-begraense-kriminaliteten-med-brug-af-dk-domaenenavne_onepager_EN_0.pdf.

Flores and Caballito neighborhoods, after passing a two-month business training provided by the Confederation of Small and Medium-Sized Enterprises (CAME). Of the 900 former illegal street vendors that occupied the commercial facilities in early 2018, CAME has reported that few remained as of October, but some of the vendors reportedly moved to other districts where enforcement is more lax.

In Canada, local police raided **Pacific Mall** in June and September 2018 and seized thousands of suspected counterfeit goods. While no charges have been brought yet, police say the investigation is ongoing, and additional search warrants are expected to be issued at storage facilities related to the kiosks searched by police.[7] In France, the police raided the Paris flea market at Saint Ouen in July 2018 and seized over 60,000 counterfeit goods. The Mexican government reportedly converted two markets known for selling counterfeit goods, Bazar Pericoapa and Plaza Meave, into legitimate shopping malls.

In the Philippines, the National Committee on Intellectual Property Rights (NCIPR), an inter-agency task force consisting of six enforcement agencies led by the Intellectual Property Office of the Philippines (IPOPHL) reportedly seized about $173 million in counterfeit goods during the first half of 2018, compared to $158 million in 2017.[8] NCIPR conducted 59 raids in various areas in the Philippines during the same period. In Thailand, the Department of Intellectual Property reported a series of activities by law enforcement and customs officers in 2018 that resulted in seizures of more than 10 million infringing items.[9] In May 2018, Hong Kong Customs carried out a series of raids against four retail outlets suspected of selling set-top boxes that reportedly provided unauthorized access to movies and TV shows.[10]

---

[7] Rachel D'Amore, *Police Seize Thousands of Suspected Counterfeit Goods After Raids At Pacific Mall*, CTV News Toronto (June 27, 2018), https://toronto.ctvnews.ca/police-seize-thousands-of-suspected-counterfeit-goods-after-raids-at-pacific-mall-1.3991123. *See also* The Canadian Press, *Police Say Seized Items From Pacific Mall Found To Be Counterfeit*, The Star (Sept. 12, 2018), https://www.thestar.com/news/gta/2018/09/12/police-say-seized-items-from-pacific-mall-found-to-be-counterfeit.html.

[8] Gabriel Pabico Lalu, *Intellectual Property Agency Notes Rise In Seized Fake Goods*, The Philippine Daily Inquirer (May 23, 2018), https://newsinfo.inquirer.net/993599/intellectual-property-agency-notes-rise-in-seized-fake-goods.

[9] Department of Intellectual Property, *IP Enforcement Statistics (Calendar Year) (By the Royal Thai Police, the Department of Special Investigation and the Customs Department) 2019 January, available at* https://www.ipthailand.go.th/en/statistics/item/สถิติการปราบปรามการละเมิดทรัพย์สินทางปัญญารายปีของสำนักงานตำรวจแห่งชาติ-กรมสอบสวนคดีพิเศษ-และกรมศุลกากร-ปี-พ-ศ-2562-มกราคม.html.

[10] Clifford Lo, *Got an Illegal Set-Top Box In Hong Kong? Be Careful, Customs Is Cracking Down Ahead of World Cup 2018 In Russia*, South Morning China Post (May 28, 2018), https://www.scmp.com/news/hong-kong/hong-kong-law-and-crime/article/2148163/got-illegal-set-top-box-hong-kong-be-careful.

Several studies this year highlighted the global trade of counterfeit goods. In September 2018, the International Chamber of Commerce, Business Action to Stop Counterfeiting and Piracy (BASCAP) released a new resource on best practices for maritime operators, brand owners, and suppliers to take steps against the maritime shipments of counterfeit goods.[11] Additionally, the Organization for Economic Cooperation and Development (OECD) issued a report in March 2018 on the connection between free trade zones (FTZs) and the trade in counterfeit goods.[12] This study found a positive correlation between the number of FTZs and the volume of trade in counterfeit goods, identified contributing factors to the trade of counterfeit goods in FTZs, and called for coordination at both the national and international levels to develop enforcement and governance frameworks in order to combat the misuse of FTZs in counterfeit goods trade. Another OECD report, issued in June 2018, identified additional factors that contribute to the production and trade of counterfeit goods, such as poor IP enforcement, well-developed production and logistics infrastructure, and trade facilitation policies that reduce transparency.[13] The report highlights good governance, including effective IP enforcement and customs oversight, as the crucial element in reducing trade in counterfeit goods.

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

---

[11] Business Action to Stop Counterfeiting and Piracy [BASCAP], *Know Your Customer, Due Diligence and Maritime Supply Chain Integrity*, International Chamber of Commerce [ICC] (Mar. 2018), *available at* https://cdn.iccwbo.org/content/uploads/sites/3/2018/09/icc-2018-kyc-and-supply-chain-paper.pdf.

[12] OECD / EUROPEAN UNION INTELLECTUAL PROP. OFFICE [EUIPO], TRADE IN COUNTERFEIT GOODS AND FREE TRADE ZONES: EVIDENCE FROM RECENT TRENDS (2018), *available at* https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade_in_Counterfeit_Goods_and_Free_Trade_Zones/Trade_in_Counterfeit_Goods_and_Free_Trade_Zones_en.pdf.

[13] *See* OECD / EUIPO, WHY DO COUNTRIES EXPORT FAKES? THE ROLE OF GOVERNANCE FRAMEWORKS, ENFORCEMENT AND SOCIO-ECONOMIC FACTORS (2017), *available at* https://read.oecd-ilibrary.org/governance/why-do-countries-export-fakes_9789264302464-en.

Issue Focus: Free Trade Zones

Free trade zones (FTZs) have become major facilitators of illegal and criminal activity, including the illicit trade in pirated and counterfeit goods, smuggling, and money laundering. FTZs are designated economic areas that are not subject to customs duties, taxes, or normal customs procedures of their host countries.[14] They can range in size from a single warehouse to entire harbors and cities, consisting of thousands of businesses.[15] FTZs are an increasingly important part of global trade, and play a particularly prominent role in the economies of developing countries. The number of free trade zones grew from 79 zones in 25 economies in 1975 to over 3,500 zones in 130 economies in 2018,[16] and according to some, exports from FTZs accounted for twenty percent of world exports in 2007.[17] While rationales for establishing FTZs vary among countries, generally they serve the purpose of attracting foreign investment, creating jobs, increasing exports, and testing new economic policies.[18]

The growth in the number of FTZs has been accompanied by the expansion of liberalization policies for their use.[19] To attract businesses, FTZs may provide various financial and regulatory benefits, typically including exemptions from taxes and customs duties. They may also offer simplified customs and administrative procedures, lighter regulation of corporate activities, and greater opportunities to distribute goods to diverse markets.[20] In addition, many

---

[14] OECD / EUIPO, MAPPING THE REAL ROUTES OF TRADE IN FAKE GOODS 19 (2017), *available at* https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Mapping_the_Real_Routes_of_Trade_in_Fake_Goods_en.pdf; OECD, THE ECONOMIC IMPACT OF COUNTERFEITING AND PIRACY 85 (2008), *available at* https://www.oecd.org/sti/38707619.pdf. The scope and nature of FTZs can vary, and FTZs can also be referred to as free zones, free ports, special economic zones, and export processing zones. *See* WORLD BANK GRP. [WBG], SPECIAL ECONOMIC ZONES: PERFORMANCE, LESSONS LEARNED, AND IMPLICATIONS FOR ZONE DEVELOPMENT 3 (2008), *available at* http://documents.worldbank.org/curated/en/343901468330977533/pdf/458690WP0Box331s0April200801PUBLIC1.pdf.

[15] OECD / EUIPO, *supra* note 14, at 19.

[16] OECD / EUIPO, *supra* note 12, at 16.

[17] *Id.* at 26.

[18] *Id.* at 13. *See also* WBG, *supra* note 14, at 3-5. According to a recent study, FTZs may have a "catalytic effect" by enhancing integration into the global value chain and creating linkages between the FTZs and the rest of the economy. *See* Ayçıl Yücer & Jean-Marc Siroën, *Trade Performance of Export Processing Zones*, 40 WORLD ECON. 1012, 1012-13 (2018).

[19] OECD / EUIPO, *supra* note 12, at 17.

[20] *Id.* at 21. *See also* http://documents.worldbank.org/curated/en/343901468330977533/pdf/458690WP0Box331s0April200801PUBLIC1.pdf.

export-oriented FTZs offer incentives, such as duty-free import of capital equipment, lighter environmental and labor regulations, and well-developed, subsidized infrastructure, to attract assembly, processing, and manufacturing businesses.[21] These benefits make it easy for businesses based in FTZs not only to import and export goods, but also to build workshops and factories that make new products using imported and local materials for export to another economy or for local consumption. In this manner, FTZs help businesses build efficient supply and marketing chains that "enable the production, movement and marketing of goods in a barrier-free environment."[22]

At the same time, without adequate and effective IP enforcement, the incentives provided by FTZs are attractive to those who want to engage in illegal activities, including the trade and manufacture of counterfeit and pirated goods.[23] For example, removing customs duties and simplifying customs procedures in FTZs may also reduce the need for customs authorities to inspect shipments, leading to less customs oversight on goods transiting through FTZs.[24] Ease of setting up businesses[25] and reduced vetting for business proprietors in some FTZs may provide openings for criminals to create legitimate shell companies for their illicit enterprises.[26] Further, bulk-breaking, packaging, and labelling activities, through which bulk shipments like containers are broken down and the goods divided into smaller parcels for distribution, are particularly prevalent in FTZs given their importance as trade and logistics hubs.[27] While these practices can be a normal part of legitimate trade, the reduced administrative procedures and oversight in FTZs give illicit actors opportunities to take advantage of such flexibilities to falsify and conceal a good's original point of production or departure, establish decentralized distribution centers for

---

[21] OECD / EUIPO, *supra* note 12, at 33.
[22] *Id.* at 32. *See also* https://www.researchgate.net/publication/303236805_Global_Value_Chains_and_Upgrading_Export_Promotion_in_FTZs, at 15-16.
[23] The recent OECD-EUIPO report on counterfeit trade routes demonstrates how counterfeit trade is often routed through economies that rely on FTZs. *See* OECD / EUIPO, *supra* note 14, at 17-19; *see also* OECD, GOVERNANCE FRAMEWORKS TO COUNTER ILLICIT TRADE 124 (2018).
[24] BASCAP, INT'L CHAMBER OF COMMERCE, CONTROLLING THE ZONE: BALANCING FACILITATION AND CONTROL TO COMBAT ILLICIT TRADE IN THE WORLD'S FREE TRADE ZONES 11 (2013), *available at* http://media.ip-watch.org/weblog/wp-content/uploads/2013/05/FTZ-report.pdf.
[25] *See, e.g.*, WBG, *supra* note 14, at 55.
[26] *See* FINANCIAL ACTION TASK FORCE, MONEY LAUNDERING VULNERABILITIES OF FREE TRADE ZONES 20 (2010), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20vulnerabilities%20of%20Free%20Trade%20Zones.pdf.
[27] *See* OECD / EUIPO, *supra* note 12, at 35.

counterfeit goods to ship "cleared" goods in small orders to final destination points, or repackage and re-label counterfeit goods with false trademarks.[28]

Another exacerbating factor is that in some countries, laws and regulations that are applied within customs territories to protect IP are often not applied or are relaxed or weakened in FTZs.[29] At one of the world's major ports of origin for counterfeit goods, Hong Kong, the Hong Kong Trade Description Ordinance prohibits imports and exports of goods bearing counterfeit marks but specifically excludes "goods in transit."[30] This creates an opening for illicit actors to ship counterfeit products through Hong Kong unhindered. In Colombia, the customs police (POLFA) does not have authority to enter primary inspection zones and lacks *ex officio* authority to inspect, seize, and destroy counterfeit goods in those zones.[31] Also, reports indicate that counterfeit goods are widely available in the International Center for Boundary Cooperation (ICBC), a strategically important FTZ that borders China and Kazakhstan, where IP enforcement is hampered by the lack of customs officials.[32] Bad actors leverage nonexistent or lax IP enforcement regimes in FTZs to facilitate illicit trade. Even when countries have the legal tools to enforce IP in FTZs, governance issues, such as a lack of political will, a lack of coordination amongst enforcement agencies, weak transparency, and poor oversight, often hinder effective IP enforcement.[33] One example is Dubai, where right holders' attempts to intercept sixteen containers full of counterfeit products imported into the Jebel Ali Free Zone (JAFZ) failed when JAFZ and Dubai Customs did not respond until the contents of the containers were already broken up and moved into different containers.[34] In Singapore, right holders report that the courts' unwillingness to issue search warrants for illicit goods imported into FTZs contributes to an overall insufficient level of enforcement.[35]

---

[28] *See id.* at 61.
[29] *See* BASCAP, *supra* note 24, at 20.
[30] *Id.* at 21.
[31] *See* https://www.state.gov/e/eb/rls/othr/ics/2017/wha/270056.htm.
[32] https://www.nytimes.com/2018/01/08/world/asia/kazakhstan-china-border.html. *See also* https://www.forbes.com/sites/wadeshepard/2016/07/26/an-inside-look-at-icbc-khorgos-china-and-kazakhstans-cross-border-free-trade-zone/#1c04330c5c8f.
[33] *See* BASCAP, *supra* note 24, at 20; OECD / EUIPO, *supra* note 14, at 13.
[34] *Id.* at 12.
[35] Lack of effective IP enforcement may be further aggravated in FTZs operated by private parties, whose main interests may be increasing zone occupancy and selling business support services to zone occupants and not enforcing IP. *See* OECD / EUIPO, *supra* note 12, at 14. *See also* WBG, *supra* note 14, at 21, http://documents.worldbank.org/curated/en/343901468330977533/pdf/458690WP0Box331s0April200801PUBLIC1.pdf.

Moreover, the growing number of small commercial parcels moving through international mail and express facilities presents challenges in the fight against counterfeiting and piracy in FTZs. According to U.S. Customs and Border Patrol (CBP), small shipments now represent a majority of all IP-related seizures, adding to the difficulty of enforcing IP in transit hubs.[36] A recent OECD/EUIPO study noted, in reference to Hong Kong, the United Arab Emirates, and Singapore, that "[f]ake goods arrive in large quantities in containers and are sent further in small parcels by post or courier services."[37] For example, parcels containing counterfeit clothing and textiles are frequently mailed to developed economies from "transit points" like Hong Kong and Singapore, both prominent FTZs.[38] In a press release for another study on trade in counterfeit and pirated goods, the OECD stated that "postal parcels are the top method of shipping bogus goods . . . . The traffic goes through complex routes via major trade hubs like Hong Kong and Singapore and free trade zones such as those in the United Arab Emirates."[39]

The International Chamber of Commerce (ICC) highlighted Turkey as an example where customs authorities can take enforcement actions in FTZs.[40] Specifically, Turkish customs authorities can detain shipments and inform right holders who can obtain an injunction from an intellectual property court.[41] The same ICC report noted that Chile's two FTZs are viewed as models of FTZ management.[42] In 2003, Chile passed Law 19.912 that gave Chile's customs officials the authority to inspect and seize illicit items at FTZs.[43] Customs officials are also equipped with X-ray machines and other technology that improve their ability to carry out inspections.[44]

Through the Revised Kyoto Convention, the World Customs Organization has emphasized the importance of treating FTZs as part of the territory of a Contracting Party,

---

[36] OFFICE OF THE INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, U.S. JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 96 (2017).
[37] OECD / EUIPO, *supra* note 14, at 13.
[38] *Id.* at 62.
[39] OECD / EUIPO, *Global Trade In Fake Goods Worth Nearly Half a Trillion Dollars a Year* (Apr. 18, 2016), http://www.oecd.org/industry/global-trade-in-fake-goods-worth-nearly-half-a-trillion-dollars-a-year.htm.
[40] BASCAP, *supra* note 24, at 26.
[41] *Id.*
[42] *Id.* at 24.
[43] *Id.*
[44] *Id.*

specifically stating that customs officials must have the right to inspect goods in FTZs.[45] Moreover, Specific Annex D of the Convention recommends the protection of patents, trademarks, and copyrights as among the few prohibitions or restrictions independently sufficient to refuse admission of goods to a free zone.

The lack of consistent and effective IP enforcement in FTZs, especially the re-exportation and transshipment of infringing goods in and through certain FTZs, remains an important problem and diminishes the value that zones provide for businesses, governments, and consumers.[46] One best practice is robust legislation and policies to ensure customs and enforcement officials have the legal tools to effectively enforce against counterfeit goods in FTZs. As the first major U.S. trade agreement to require signatories to provide *ex officio* authority against suspected counterfeit goods or pirated goods that are admitted into or exiting from FTZs and bonded warehouses, the United States-Mexico-Canada Agreement is a leading example of how governments can work together to tackle this issue.[47]

Other examples of best practices include mandatory electronic submission of customs data, efficient adjudication of violations in zones, enhanced security screening, and sufficient monetary fines for violations.[48] Governments should also empower national customs authorities to ensure adequate and effective IP enforcement within FTZs and foster greater cooperation between customs authorities.

---

[45] Protocol of Amendment to the International Convention on the Simplification and Harmonization of Customs Procedures, Specific Annex D; ch. 2, standard 4, June 26, 1999, 2370 U.N.T.S. 27.
[46] https://foreignpolicy.com/2013/02/13/free-trade-or-penalty-free-crime/.
[47] United States-Mexico-Canada Agreement, art. 20.84, *available at* https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/20_Intellectual_Property_Rights.pdf.
[48] OECD, *supra* note 23, at 34.

Results of the 2018 Out-of-Cycle Review of Notorious Markets

The 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 List is not an exhaustive inventory of all notorious markets around the world. Markets on the List 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 marketplaces 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.[49] 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.

[49] *See, e.g.*, BASCAP, *Roles and Responsibilities of Intermediaries: Fighting Counterfeiting and Piracy in the Supply Chain*, INTERNATIONAL CHAMBER OF COMMERCE (Mar. 2015), *available at* https://iccwbo.org/publication/roles-responsibilities-intermediaries; INTERNATIONAL TRADEMARK ASSOCIATION, *Addressing the Sale of Counterfeits on the Internet* (Sept. 2009), *available at* http://www.inta.org/Advocacy/Documents/INTA%20Best%20Practices%20for%20Addressing%20the%20Sale%20of%20Counterfeits%20on%20the%20Internet.pdf.

Online Markets[50]

The 2018 List of notorious online markets identifies examples of various technologies, obfuscation methods, revenue models, and consumer harms associated with infringing activity. USTR based its selections not on specific types of technologies but on whether a nominated site or affiliated network of sites reportedly engages in or facilitates substantial piracy or counterfeiting to the detriment of U.S. creators and brand owners, as well as legitimate sellers and distributors. Pirate streaming sites continue to gain popularity, overtaking pirate torrent and direct download sites for distribution of pirated content. This year's review process identified a growing concern about the proliferation of counterfeits on other online marketplaces, particularly those being sold through consumer-to-consumer sales. In order to meaningfully combat this problem, e-commerce platforms should take proactive and effective steps to reduce piracy and counterfeiting, for example, by establishing and adhering to strong quality control procedures in both direct-to-consumer and consumer-to-consumer sales, engaging with right holders to quickly address complaints, and working with law enforcement to identify IP violators.

In addition to facilitating IP infringement, these sites may lack safeguards for consumer privacy, security, and safety. Two reports produced in 2018—one by the European Union Intellectual Property Office (EUIPO)[51] and another by a professor at Carnegie Mellon University[52]—documented the proliferation of malware on websites engaging in online piracy. The Carnegie Mellon University study found that doubling one's time spent on infringing sites "leads to 20 percent increase in total malware files," such as adware, Trojans, and other tracking software, on the users' computers. Similarly, the EUIPO report found a large variety of malware on infringing websites download, install further unwanted malware, and remotely take control of the victim's computer. Such malware could result in the theft of personal and payment information.

---

[50] In most cases, the List identifies online markets by the domain name provided in the public responses to the *Federal Register* request. However, it is common for operators of online Notorious Markets to change a site's domain name ("domain name hopping") or to use multiple domain names at once to direct users to the main site. The List reflects each market's most commonly referred to or well-known domain name or names as of April 2019. Also, to the extent possible, the List reflects the actual or reported location of the hosting provider as of April 2019.

[51] *See* https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2018_Malware_Study/2018_Malware_Study_Exe_Summ_en.pdf.

[52] *See* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3139240.

1FICHIER.COM

This cyberlocker[53] is hosted in and popular in France and reportedly makes available illegal video game copies and other copyrighted content. According to the video game industry, the site allegedly hosts thousands of links to infringing content, and right holders continue to cite 1Fichier.com's extremely low response rate to takedown requests—0.59%, down from 2% previously. Payment processors have reportedly suspended services to this site due to allegedly illegal activity, and Internet browsers reportedly detect and warn of malicious content on the site.

BEOUTQ

Also operating as **beinmatch.com** and **kora-star.tv**. Formerly **beoutq.se**, **gowatch.se**, **cameraman.sx**, **blackhouse.sx**, **neverdie.pw**, **pikiwiki.pw**, **belssingwatchingbb.pw**, **cdn.neverdie.pw**, **c.blackhouse.sx**, **c.neverdie.pw**, **c.pikiwiki.pw**, **c.belssingwatchingbb.pw**, **streamuk.com**.

BeoutQ, an illicit pirate operation that has been widely available in Saudi Arabia and throughout the Middle East region and Europe during 2018, is an example of a single entity pirating content in multiple ways. It is suspected of satellite and online piracy, as well as supporting piracy devices and related services such as apps and illicit streaming devices (ISDs) that allow access to unlicensed movies and television productions, including sports events. As highlighted in the 2017 List, ISDs provide illegal access to movie and television content through a variety of means, including downloading content and unauthorized streaming of live television and sporting events. USTR strongly urges trading partners to report and take effective action against piracy facilitated by apps, ISDs, and satellite signals.

BUKALAPAK.COM

Bukalapak.com, founded in 2010, is reportedly one of the largest online marketplaces 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, and apparel. Right holders report that a vast majority of branded products on this platform are not genuine and that items are often openly labeled "replicas" of branded products. While Bukalapak.com provides a link on its platform for right holders to report illegal and infringing

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

goods and merchants, right holders report that this mechanism is ineffective. Specifically, they state that Bukalapak.com does not respond promptly to reports of counterfeit listings, that the procedures to report counterfeit listings are burdensome, and that the platform does not fully take down counterfeit listings. 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 three years and made thousands of sales during that period. Furthermore, the reporting system is reportedly not available in English, which can make it more difficult for non-Indonesian brand owners to enforce their rights.

CAROUSELL.COM

Formerly **au.carousell**, **hk.carousell**, **tw.carousell**, **id.carousell**, **my.carousell**, **ph.carousell**, **sg.carousell**, **us.carousell**.

Carousell.com is a mobile e-commerce platform based in Singapore and popular throughout Southeast Asia. Reportedly, a high percentage of branded goods sold on this network of platforms—between 40% and 80%—are counterfeits. Right holders submitted that reporting IP infringement to carousell.com is ineffective, because removing a listing can take up to five days, and the platform has no system in place to deter repeat offenders.

CHOMIKUJ.PL

Chomikuj.pl is reportedly the most popular cyberlocker in Poland. Right holders reported that a broad range of songs by U.S. artists are available on this platform, uploaded by its users. The site allegedly rewards users who upload popular content that is then downloaded by other users. Right holders reported that in September 2017, the Krakow Court of Appeal ordered the site to pay reparations 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.

DHGATE.COM

DHgate.com is a Chinese business-to-business e-commerce platform that features over 40 million product listings from small- and medium-sized businesses in China. The International Anti-Counterfeiting Coalition reported concerns about the high volume of sales of counterfeit

goods on DHgate.com, lax seller registration procedures that allow sellers to resume operations even after being removed from the platform, and limited means for right holders to enforce their rights. The trade association stated that DHgate.com refuses to provide information about confirmed counterfeit sellers, asserting privacy-related concerns. In its rebuttal submission, DHgate.com stated that its seller registration process requires certification of the seller's ID or business license and that sellers be checked against a historical "questionable seller" database. DHgate.com also reported that IP complaints dropped 38% in the past year and that its proactive screening tools employed more than 15,000 keywords, including brand names, similar or deformed words, and code words. DHgate.com has reportedly reached out to the trade association to address its concerns. In response to the 2017 List, DHgate.com reported that it had worked with the previous year's nominators to address their concerns by blocking all sales of published material from its platform and improving its screening tools in collaboration with a trade association. DHgate.com also changed its one-stop online Intellectual Property Protection System (IPPS) to accept complaints regarding unregistered IP (*e.g.*, photos, images, and publications) and invited another trade association to conduct training sessions with its employees on detecting counterfeit goods. DHgate.com reports that it removes listings for 97 percent of IP complaints, with a one-working-day processing time for over 90 percent of takedowns.

USTR urges the site to work closely with all right holders to address the challenges they face in combatting counterfeits. USTR recommends that DHgate.com seriously consider how it can make information about infringing sellers available to right holders or law enforcement authorities and ensure that these referrals lead to meaningful enforcement outcomes, such as targeting large manufacturers and distributors of counterfeit goods.

FIRESTORM-SERVERS.COM AND WARMANE.COM

Also directing from **fstorm.cc**.

Firestorm-Servers.com 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. According to right holders, this particular server enables approximately 8,800 active users to play World of Warcraft, an online video game, without paying the monthly subscription fee established by the game's publisher. This website appears to be operated out of

and hosted in Russia and is popular in Colombia and France. Warmane.com is another such server that reportedly enables 44,000 users to play World of Warcraft without paying the monthly subscription fee to the publisher.

FLOKINET

FlokiNET is an example of the growing problem of hosting providers that do not respond to notices of infringement or warning letters that the provider is hosting and supporting known infringing websites. With servers reportedly in Romania, Iceland, and Finland, FlokiNET allows anonymous hosting for different types of websites associated with infringing activity, including avxhome.se and djnotorioussam.com.

FLVTO.BIZ AND 2CONV.COM

Flvto.biz and 2Conv.com, essentially the same service operating from different front-end domains, are highlighted this year as examples of the stream-ripping phenomenon that continues to threaten legitimate streaming audio and video services, music performers, and composers.[54] The sites do not appear to have permission from YouTube or other sites and do not have permission from right holders for a wide variety of music represented by major U.S. labels.

FMOVIES.IS

Redirects to **123movies.com**. Also operating as **fmovies.to**. Formerly **fmovies.se**.

According to right holders, fmovies.is allegedly streams unauthorized movies and television series directly to computer desktops or through apps on streaming devices. The continued listing of fmovies.is on the List demonstrates the ongoing challenges of streaming piracy.[55] According to right holders, several countries have taken action against this site, including enforcement action by a Denmark District Court. The site is tied to multiple name registrations ending in different ccTLDs.

[54] For a description of stream-ripping, see the 2016 Notorious Markets List.
[55] From January 2016 to December 2016, 77.7 billion visits to piracy streaming websites were recorded, and 34.0% of this piracy activity was via mobile devices. *See* https://www.muso.com/magazine/muso-releases-2017-global-film-tv-insight-report/.

HOSTING CONCEPTS B.V. (DBA OPEN PROVIDER) AND REGIONAL NETWORK INFORMATION CENTER JSC

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.[56] 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. is an example of a hosting provider without the types of policies listed above. According to right holders, it hosts 2,523 known illegal online pharmacies, including Indiamart.com, a Notorious Market identified in the 2017 List. It has been reported that 10% of these 2,523 illegal pharmacies market controlled substances such as opioids. Regional Network Information Center JSC is also included in this year's List as another domain name registrar that provides domain name registration services to a large number of allegedly counterfeit or otherwise illegal online pharmacies. Both Hosting Concepts B.V. and Regional Network Information Center JSC have been reportedly non-responsive to abuse notifications.

INDOXX1.COM

Redirects to **indoxxi.cx**. Also known as **indoxxi.bz**.

Also known as "Indo 21," this website operates in Bahasa Indonesia and is one of the most popular websites in Indonesia. Nominated by the movie industry, this site appears to

[56] In its 2018 submissions, ASOP Global cited Name.com (US), Alpnames Limited, (Gibraltar), GoDaddy (US), Center of Ukrainian Internet Names dba UKRNAMES (Ukraine), Internet.bs (Bahamas), Blacknight (Ireland), PDR Ltd. d/b/a PublicDomainRegistry.com (India) Networking4All (Netherlands), 1&1 Internet AG (Germany), and BizCN (China) as good actor registrars. In addition, Realtime Register and Rightside received ASOP Global's First Internet Pharmacy Safety E-Commerce Award in March 2017 in recognition of their "corporate policies and practices; responsiveness to illegal online drug sellers; prevention of illegal use of domain names for illegal online drug sales; cross-industry collaboration; and public and consumer awareness efforts." *See* http://buysaferx.pharmacy/news-release-alliance-for-safe-online-pharmacies-announces-recipients-of-its-first-internet-patient-safety-e-commerce-award/.

provide links of copyright infringing audiovisual content to its users. Right holders reported that while this website responds to takedown requests, infringing content is often rapidly restored.

KINOGO.CC

Formerly **kinogo.club** and **kinogo.co**.

Kinogo.cc continues to be a popular streaming link site and reportedly hosts some of its own video content, a practice that is increasingly common among major Russian-language video streaming links sites. Right holders continue to report infringing content being shared on this website. The Moscow City Court ordered the blocking of this website in Russia in June 2016. Kinogo.cc targets the Ukraine and Russia markets and, according to right holders, is hosted by a hosting provider registered in the Netherlands while the operators of the website are believed to be based in Ukraine.

MP3JUICES.CC

Formerly operating through **mjcdn.cc** and **yxww.xyz**.

MP3juices.cc is a popular stream-ripping website that allegedly permits a user to select YouTube music videos and to make a permanent download of an audio-only mp3 file that can be added to the user's 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 mp3 downloads to the user. The registrar for this site is based in Panama, and its hosting provider is based in Russia.

MP3VA.COM

While this website takes on the appearance of a legal music site, right holders report that it is engaged in the unlicensed sale of music. Downloads are reportedly available for unreasonably low prices, such as single tracks for 15 cents and full albums for about $1.50. While major U.S. credit card and payment processors have reportedly ceased servicing mp3va.com, offshore payment intermediaries can still be used. Publicly available traffic information indicates that there were roughly 8 million visitors to this website in the past year. The hosting provider for this site is located in Russia, and the registrar is based in Canada. Mp3va.com continues to claim on its FAQ page that it has a license from Avtor, a rogue

Ukrainian collecting society, and elsewhere purports to have a license from the "Rightholders Federation for Collective Copyright Management of Works Used Interactively." Despite the alleged participation of these CMOs, mp3va.com's music download sales are reportedly not authorized and authors are not paid. The landing page for mp3va.us claims "Check It. It's Legal!" with a single link to mp3va.com.

MPGH.NET

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 collection and aggregation of virtual goods and the modification of a game to allow an advantage for the player. 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.net is an example of a site that provides "cheats" and reportedly offers several hundred thousand free cheats to over 4 million users. The site generates revenue through advertisements and by offering premium accounts, and Internet browsers reportedly detect and warn of malicious content on the site.

NEWALBUMRELEASES.NET

Newalbumreleases.net is an example of a website that reportedly provides unauthorized downloading of tracks and albums that have not yet been commercially released to the public. According to right holders, the site hosts its infringing content on cyberlockers and provides users with links to services like **Rapidgator.net** where the files are available 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.

OPENLOAD.CO

Also **oload.tv** directs to **openload.co**.

This very popular steaming and download cyberlocker incentivizes users to upload large files, such as television episodes and movies, by allegedly paying a fixed reward per 10,000

downloads/streams, with higher rewards for downloads by users in Australia, Canada, the United Kingdom, and the United States. The site reportedly claims that the files it hosts "will never be deleted, especially if somebody is downloading them." Right holders report that the website is being masked behind a reverse proxy service, allegedly to curb right holders' ability to identify its precise host.

PELISPEDIA.TV

Pelispedia.tv has more than 50,000 links to more than 8,000 movie and television series titles that allegedly have been illegally reproduced. This Spanish language website has connections and audiences across the Spanish-speaking diaspora, including Mexico, Argentina, Chile, Spain, and Venezuela. Pelispedia.tv is monetized through a large number of national and international advertisements.

PINDUODUO.COM

Pinduoduo.com is a new addition to the 2018 List. In a relatively short period, this so-called "social commerce" platform has become the third largest e-commerce platform in China by number of users. Relying on a catalogue of improbably low-priced goods to attract customers, pinduoduo.com allegedly draws its main user base from provincial towns and the countryside outside China's major cities. Many of these price-conscious shoppers are reportedly aware of the proliferation of counterfeit products on pinduoduo.com but are nevertheless attracted to the low-priced goods on the platform. A particularly common and pernicious form of counterfeit products on pinduoduo.com is so-called "Shanzhai" products, also known as "parasite brands." These are products whose brand name and trademark imitate a legitimate brand in a bid to fool consumers into thinking that they are buying from the better-known brand, taking advantage of loopholes in Chinese trademark law. Many brand owners reported an increase in consumer complaints after "Shanzhai" versions of their products were listed on pinduoduo.com. Several brands issued public notices to warn consumers that products listed on pinduoduo.com under their brand names are counterfeits.

Following a recent period of intense public scrutiny after pinduoduo.com's stock listing on NASDAQ in July 2018, the company reportedly took down listings of counterfeit products, announced an effort to cooperate with brands to launch flagship stores with legitimate products

on its platform, and invested in artificial intelligence tools to police the platform automatically for counterfeit products. However, these measures fell short of fully addressing the problem. For example, accounts of these so-called flagship stores are reportedly not always controlled by the brand owners themselves but often by third parties with only a tenuous or even nonexistent link to the brand owners. Meanwhile, counterfeit and pirated products, including counterfeit copies of legitimate products sold in the flagship stores, appear to remain widely available on the platform. USTR encourages pinduoduo.com to take additional measures to curb the sale of counterfeit products from its platform.

PRIVATE LAYER-HOSTED SITES

Including **torrentz2.eu** and mirror sites **torrentz2.cc**, **torrentz2.is**, and **torrentz2.tv**.

This group of websites is hosted by Private Layer, which reportedly is operated from Panama with data center and hosting operations in Switzerland and elsewhere. Torrentz2.eu, believed to be hosted in Bulgaria, is one of the most popular torrent sites that allegedly infringe the U.S. content industry's copyrights. While the exact configuration of the websites changes from year to year, this is the fifth consecutive year that the List has stressed the significant international trade impact of Private Layer's hosting services and the allegedly infringing sites it hosts. Other listed and nominated sites may also be hosted by Private Layer but are using reverse proxy services to obfuscate the true host from the public and from law enforcement. Right holders report that Switzerland remains a popular host country for websites offering infringing content and the services that support them. Switzerland continues to progress on previously announced plans to close a loophole in its law that prevents copyright holders and prosecutors from collecting and using certain data in anti-piracy actions, making it difficult to enforce Swiss copyright law online. A proposed amendment to the Copyright Act would allow right holders to identify infringing websites by using IP addresses, permits criminal procedures, and provides additional measures for addressing online piracy. This legislative process, which began in 2012, is expected to come to a resolution in 2019.

RAPIDGATOR.NET, RUTRACKER.ORG, AND SEASONVAR.RU

Commenters from the book publishing, movie, and music industries all nominated rapidgator.net, one of the largest file sharing websites in the world, for inclusion on this year's

List. Rapidgator.net appears to be operated from Russia but provides most of its allegedly infringing content to users outside of the country. Right holders report that high-quality and recent content can be found easily on this site. Rapidgator.net 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. Rutracker.org, a BitTorrent portal with almost 14 million active accounts, is also reportedly hosted in and operated from Russia. This site is one of the most popular in the world and a top site in Russia despite a still-outstanding order issued in 2015 by Moscow City Court that ordered ISPs in Russia to block rutracker.org. The Russian search engine yandex.com allegedly indexes links to rutracker.org despite it being illegal to do so in Russia according to a recent law. Seasonvar.ru, also reportedly hosted in Russia, is one of the world's most popular infringing streaming websites. According to right holders, more than 12,000 different TV series are available on seasonvar.ru without authorization. Right holders are seeking enforcement action against this website in Australia, and some variants of this website were reportedly subject to blocking orders in Russia.

RARBG.TO

Rarbg.to is a globally popular BitTorrent index site nominated by commenters from the movie, television and music industries, and is hosted on servers located in Bosnia and Herzegovina. While this site and its variants have been subject to blocking orders in Australia, Belgium, Denmark, Finland, Indonesia, Ireland, Italy, Malaysia, Portugal, and the United Kingdom, it continues to operate. Right holders reported that high-quality and recent content can be found easily on this site. Rarbg.to reportedly generates revenue through advertisements.

SCI-HUB AND LIBGEN.IO

Also known as the "Library Genesis Project" and **sci-hub.tw**, **sci-hub.se**, **lib.rus.ec**, **gen.lib.rus.ec**, **booksc.org**, **book4you.org**, **bookos-z1.org**, **booksee.org**, and **b-ok.org.** Formerly **bookfi.org**, **bookzz.org**, **booker.org**, **libgen.info**, **libgen.pw**, **sci-hub.cc**, **sci-hub.ac**, **sci-hub.bz,** and **sci-hub.hk**.

Right holders continue to report Sci-Hub and its mirror site[57] libgen.io as the most flagrant pirate sites that facilitate unauthorized access to over 70 million journal articles and

[57] A "mirror site" is a website that is a proxy or clone of an original pirate site and may offer the same, new, or cached infringing content as the original site. Some mirror sites are designed to spread malware, steal personal

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. Right holders allege that at least some of the material available on Sci-Hub were 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. Sci-Hub's U.S.-based domain names were transferred to the plaintiff by U.S. domain name registries per a June 2017 ruling by the U.S. District Court for the Southern District of New York, which made permanent a 2015 preliminary injunction in addition to awarding a publisher $15 million in damages from Sci-Hub. A separate ruling by the U.S. District Court for the Eastern District of Virginia in November 2017 awarded another publisher $4.8 million in damages, enjoined Sci-Hub from dissemination of the publishers' content, and ordered further action to impede access to Sci-Hub's Internet sites that made available content that the court found to be infringing. Furthermore, right holders report that a number of scientific, technical, and medical publishers in Europe began pursuing blocking actions against Sci-Hub and its affiliates in Europe. The operator of Sci-Hub is believed to be based in Russia and the content is believed to be hosted either in the Netherlands or the Seychelles.

SHOPEE.PH

Also **shopee.com.my**, **shopee.co.th**, and **shopee.co.id**.

Shopee.ph is an online marketplace based in Singapore and serving the Southeast Asian market. Right holders report very high levels of counterfeits being sold on all of shopee.ph's platforms and that the operators are uncooperative when right holders seek to protect their brands. For example, shopee.ph 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 up to two weeks.

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.

TAOBAO.COM

China's largest e-commerce platform **taobao.com** is owned and operated by parent company **Alibaba Group (Alibaba)**. Although Alibaba has taken some steps to curb the offer and sale of infringing products, right holders, particularly SMEs, continue to report high volumes of infringing products and problems with using takedown procedures.

Serious concerns remain about Alibaba's responsiveness to SMEs, who continue to express concerns over ineffective takedown procedures, burdensome enrollment requirements for a Good Faith program that reduces the evidentiary burden for takedown requests, and Alibaba's delays in responding to SMEs. Enrollment by SMEs in the Good Faith program and the trade association program remains, by Alibaba's own admission, disappointingly low. The press also reports that Taobao.com continues to feature large volumes of infringing products.[58] Furthermore, USTR identified a number of actions in the 2017 List for Alibaba to consider.[59] While it described efforts related to certain of those actions, Alibaba's submission was silent on whether it took steps to implement other actions identified in USTR's recommendations.

One U.S. automotive parts trade association reported on Alibaba's efforts to work with its member companies, though it also raised continuing concerns regarding the significant volume of infringing products and complicated takedown processes. In its submission, Alibaba described efforts taken to improve enforcement.[60] Alibaba provided video instruction and conducted proactive outreach to right holders regarding its one-stop Intellectual Property Protection Platform (IPP Platform), funded a trade association program for submitting good faith takedown requests, and collaborated with industry associations to improve its proactive

[58] *See* Agent France-Presse, *"Ababis" and "Star Wars": Knock-Offs Thrive*, *available at* https://www.news.com.au/finance/business/retail/chinas-annual-shopping-frenzy-shatters-records-again/news-story/054e2c41866eb2dd4dd6f9ef791f567c.

[59] In the 2017 List, USTR recommended that Alibaba should: 1) seriously consider expanding its reported ban on listings of automotive air bags and air bag components on the alibaba.com and aliexpress.com platforms to the taobao.com platform, and to other widely-counterfeited products not ordinarily sold in C2C marketplaces, such as brake pads and other automotive parts; 2) take efforts to ensure that its referrals of criminal leads to Chinese authorities lead to meaningful enforcement outcomes, such as by targeting large manufacturers and distributors of counterfeit goods; 3) seek to improve the effectiveness of the repeat infringer policy; 4) make available to right holders the contact information of infringing sellers and details on the volume of infringing sales after infringing listings are removed so that right holders can follow up with enforcement action; 5) seek SME input and provide advisory opportunities to develop more effective policies to address the challenges SMEs face on taobao.com and other platforms; 6) improve tools to prevent the unauthorized use of product images for the sale of infringing products; and 7) ensure that infringing sellers and goods do not migrate from TMall or taobao.com to other platforms owned and operated by Alibaba such as Xian Yu, located at 2.taobao.com.

[60] 2018 Special 301 Out-of-Cycle Review of Notorious Markets: Comments Submitted by Alibaba Group, *available at* https://www.regulations.gov/document?D=USTR-2018-0027-0019.

screening tools. According to Alibaba, its criminal referral of infringing sellers led to the arrest of 1,752 suspects and the closure of 1,282 manufacturing and distribution centers, and Alibaba itself brought 48 civil lawsuits against counterfeiters. Alibaba's statistics, however, reflect enforcement endeavors affecting right holders worldwide and across all of Alibaba's platforms and do not provide data for cases affecting U.S. right holders or from only the taobao.com marketplace.

USTR encourages the company to continue to enhance cooperation with all stakeholders, especially SMEs, to address ongoing complaints. USTR repeats its recommended actions from the 2017 List and requests that Alibaba clearly demonstrate the extent to which it takes those actions, particularly where Alibaba's submission had been silent. These actions include: (1) expanding 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) enforcing its current policies related to automotive parts; (3) improving the effectiveness of its repeat-infringer policy; (4) seeking input from SMEs (not just trade associations); and (5) improving tools to prevent the unauthorized use of product images. USTR will continue to monitor taobao.com in the coming year for evidence of whether the new enforcement changes are demonstrably effective in addressing ongoing concerns.

THEPIRATEBAY.ORG

Also operating as **thepiratebay.gd**. Formerly registered at the following domains: .gl, .is, .sx, .ac, .pe, .gy, .gs, .am, .la, .mn, .vg, .fm, .sh, .my, .tw, .se, and .ms.

While The Pirate Bay websites have experienced periodic downtime 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, The Pirate Bay continues to be one of the most frequently visited websites in the world. Authorities around the world have found The Pirate Bay and its operators liable for infringing copyright, including most recently in Romania and Greece where ISPs were ordered to block the site. Past actions also took place in Argentina, Australia, Austria, Belgium, Denmark, Finland, France, Iceland, Indonesia, Ireland, Italy, Malaysia, the Netherlands, Norway, Portugal, Spain, the United Kingdom, and at the Court of Justice of the European Union. The Pirate Bay has managed to operate by constantly hopping to new top level domains, most recently to .se, the

country code top level domain of Sweden, and .vg, the country code top level domain of the British Virgin Islands. The Swedish Supreme Court in December 2017 upheld an earlier ruling that ordered the seizure of thepiratebay.se. However, the Pirate Bay managed to migrate again, this time to its original .org domain.

TOKOPEDIA.COM

Tokopedia.com is one of Indonesia's largest online marketplaces. It serves as a platform for third party vendors to post listings, and the site offers a huge range of goods, including clothes, electronics, and textbooks. Right holders have reported finding high rates and high volumes of counterfeit clothing, counterfeit cosmetics and accessories, pirated textbooks, and 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 brand owners, and the platform makes little effort to deter repeat infringers. In fact, some sellers of counterfeit products have been in business on tokopedia.com for allegedly as long as four years.

TURBOBIT.NET

Right holders reported that nearly 360,000 infringing links were identified on this cyberlocker in the past year. Popular in France and Turkey, it 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.net to store infringing files for download. According to right holders, the host for this website is based in the Netherlands and uses a masking service in the Bahamas.

TVPLUS, TVBROWSER, AND KUAIKAN

These apps and developer add-ons are reportedly operated by related companies in China to provide users around the world with television, live sports, and content protected by copyright and related rights. According to right holders, these apps have been downloaded more than 64 million times. These apps reportedly allow people in China to view unauthorized streams of

movies, TV, and live events (*e.g.*, sports) on any device of their choosing, posing an additional threat to legitimate content platforms in China.

UPLOADED.NET

Directing from **ul.to** and **uploaded.to**.

This cyberlocker reportedly operates through multiple redundant domains and provides access to a broad range of infringing content such as books, movies, television, and music, including pre-release music. Uploaded.net uses a combination of multi-tiered subscriptions, a referral program, and a rewards scheme to generate revenue,[61] incentivize unauthorized sharing of popular copyrighted content, and expand its user base. For example, the site pays rewards to users based on large file sizes, such as those for movies and television. It also pays rewards based on the number of times a file is downloaded, paying more when the downloads come from "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 operators not liable. In September 2018, the German Supreme Court referred questions on this case to the Court of Justice of the European Union.[62] Uploaded.net is owned by a Swiss company and hosted in Germany.

UPTOBOX.COM

As an additional example of a direct download cyberlocker, uptobox.com also allows streaming and embedding through its site, uptostream.com. The site is reportedly widely used among pirate sites in Europe to generate revenue based on advertisements on their own sites with embedding or by linking downloads through pay networks such as adf.ly. The site reportedly incentivizes users to upload large files, such as copyrighted television episodes and movies, and offers a referral/reseller program to attract more users. According to right holders, uptobox.com

[61] In 2014, one report estimated that uploaded.net generated approximately $6.6 million in annual revenue through premium accounts and advertising. *See* https://www.netnames.com/assets/shared/whitepaper/pdf/dca-netnam-es-cyber-profibility-1.compressed.pdf.

[62] https://www.limegreenipnews.com/2018/09/provider-liability-first-youtube-now-uploaded-next-case-before-the-cjeu/.

is owned by a Swiss company and is hosted in France. It uses a proxy mask to allegedly curb right holders' ability to identify its precise host.

VK.COM

Nominated again this year, vk.com 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.com reportedly facilitates the distribution of copyright-infringing files, and the U.S. motion picture industry reports that they find thousands of infringing files on the site each month. Social networking sites can serve as a uniquely valuable communication platform, enabling beneficial commercial, cultural, and social exchanges. Most successful social networking sites do so in ways that do not involve the active facilitation of copyright infringement and these sites adopt operating models that also provide access to legitimate content. Reports that vk.com is taking steps to address piracy and is constructively engaging with the music industry are encouraging. In 2016, vk.com reached licensing agreements with major record companies, took steps to limit third-party applications dedicated to downloading infringing content from the site, and experimented with content recognition technologies. Also, in 2018, vk.com was a signatory to a landmark anti-piracy agreement with technology companies in Russia. Under this agreement, a centralized database with links to illicit sites will be populated via input from the entertainment industry, and signatories would query the database and remove infringing content from their platforms. USTR encourages vk.com to build upon these positive developments. Specifically, USTR encourages vk.com 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.

Physical Markets

The sale and distribution of counterfeit and pirated goods online is a growing concern, however, physical marketplaces 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 FTZs;
- 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 marketplaces 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 trademark 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.

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 78 percent of the value (measured by manufacturer's suggested retail price) and 87 percent of the seizures by CBP in 2017. 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. At the same time, some online markets are cooperating with law enforcement on counterfeiting and piracy operations offline. It is reported that, in many instances, Chinese authorities engage in routine enforcement actions in physical markets. USTR welcomes these efforts and recommends their expansion to more effectively combat the scale of the reported problem in China with a special focus on the following key markets:

Huaqiangbei Electronics Markets, Shenzhen, Guangdong Province

The Huaqiangbei District is home to numerous technology malls, which serve as global hubs for the distribution of counterfeit electronics, parts, and accessories. In particular, stakeholders have highlighted the Yuan Wang, Long Sheng, and Man Har Digital Plaza malls as especially egregious. The Yuan Wang mall alone reportedly has about 10,000 stores selling allegedly counterfeit electronics and hosts an estimated 100,000 daily visitors. The Long Sheng market is reportedly among the largest markets for smart phone parts in the region, with most stores selling counterfeit parts. Wholesale buyers from across China and from other countries reportedly travel to these and other markets in Huaqiangbei to purchase counterfeit products and to arrange for their shipment to ports around the world. While Chinese authorities have carried out frequent enforcement actions in cooperation with brands, large-scale counterfeit sales continue as mall operators have developed strategies to interfere with enforcement efforts.

Luohu Commercial City, Shenzhen, Guangdong Province

Luohu Commercial City returns to the List this year and is a market where reportedly up to half of the products on sale are counterfeit, including clothing and fashion accessories. Authorities regularly conduct raids, resulting in the seizure of infringing products and fines or jail time for sellers. However, these efforts have apparently not stopped counterfeit sales.

Silk Market, Beijing

Many retail vendors at the Silk Market reportedly sell and distribute counterfeit products. Even though, in prior years, some right holders successfully sued the market's operators and administrative and criminal raids were conducted, the Silk Market reportedly remains one of Beijing's largest markets for the sale of counterfeit products and caters to large numbers of tourists. Management is also reportedly uncooperative, taking few steps to monitor the market.

Past civil and administrative enforcement efforts, although imposing some costs on counterfeits, have not been effective.

In addition to the foregoing markets, the following markets also exemplify the problem of widespread counterfeiting of consumer products:

- **Jinlongpan Foreign Trade Garment Market, Guangzhou, Guangdong Province**
- **Zhanxi Lu Garment Wholesale Market, Guangzhou, Guangdong Province**
- **Yulong Garment Wholesale Market, Guangzhou, Guangdong Province**
- **Wu'ai Market, Shenyang, Liaoning Province**

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

ARGENTINA

La Salada, Buenos Aires

While Argentina conducted raids and other significant enforcement actions related to counterfeiting or piracy in La Salada in 2017, the sale of counterfeit goods has reportedly continued. La Salada remains on the List as it will take sustained enforcement action and stronger legal tools to reverse the long-standing reputation of La Salada as one of the largest black markets for IP-infringing goods. Considerable quantities of a wide variety of counterfeit goods are reportedly still sold at the market and re-sold throughout the city, country, and region. Most goods appear to be imported from China, but some local assembly and finishing may also take place in and around La Salada.

BRAZIL

Rua 25 de Marco, Sao Paulo

Rua 25 de Marco in Sao Paulo is notorious for hosting shopping malls that sell counterfeit and pirated goods, including Galeria Pagé and Shopping 25 de Marco. The center of Sao Paulo city is reportedly the epicenter of counterfeits and piracy in the state and one of the

most notorious examples of counterfeit markets in the country. According to the Sao Paulo Federation of Industries, contraband, pirated, counterfeit, and stolen goods cost the state of Sao Paulo approximately $4.4 billion and 111,500 formal sector jobs in 2015. Since the 2015 List, police have conducted at least three significant operations, including dismantling a large center of pirated CD and DVD production. However, after the successful September 2017 action that temporarily closed Shopping 25 de Marco, counterfeit sales unfortunately resumed in bulk as local political pressure to reopen the market sapped the will to continue enforcement. USTR encourages the newly elected state and city governments to combat counterfeits and piracy through strong enforcement actions.

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 reportedly conduct 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 these markets.

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 List in 2018. Vendors reportedly sell counterfeit products in open view of the public and largely with impunity. Occasional enforcement efforts have been insufficient to address the overall problem. 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 List in 2018. Stakeholders confirm that it remains a market selling counterfeit products, including apparel and footwear. Counterfeit products from Tank

Road wholesalers are also reportedly supplied to other Indian markets, including Gaffar Market and Ajmal Khan Road. These wholesalers appear to operate freely, allowing them to build well-established businesses over many years. USTR encourages India to take sustained and coordinated enforcement action at the Tank Road market, previously-listed markets, and numerous other non-listed markets in its territory.

INDONESIA

Mangga Dua Market

Mangga Dua is a popular market in Jakarta selling a variety of counterfeit goods, including handbags, wallets, clothing, and fashion accessories, with reportedly minimal enforcement by the government 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 Lists.

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 urges Malaysia to launch a sustained, coordinated, and effective effort to tackle widespread counterfeiting and piracy at markets throughout Malaysia, including the Petaling Street Market.

MEXICO

El Tepito, Mexico City

Significant levels of piracy and counterfeiting reportedly continue in El Tepito, an open-air 80 square block market in the middle of Mexico City. Stakeholders are concerned that El Tepito market has become increasingly dangerous, even for local police, making it nearly impossible for right holders to enforce their rights. Infringing items sold at El Tepito include video games, modified consoles and devices that enable the circumvention of technological protection measures, and counterfeit apparel. 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, remains on the List in 2018. With approximately 3,000 vendors, Mercado San Juan de Dios is the largest indoor market in Latin America, attracting a significant number of Mexican and foreign visitors. Amongst a plethora of pirated and counterfeit goods sold in the market, roughly one third of vendors allegedly sell devices that enable the circumvention of technological protection measures. Stakeholders have continued to raise concerns with the Mexican practice that requires each infringing game disc to be accompanied in the prosecution files by a copy of a legitimate original for comparison by experts in order for legitimate videogame right holders to enforce their rights. This requirement can be burdensome when there are multiple infringing copies of the same game disc under consideration. USTR encourages Mexico to address this issue to ensure that legitimate right holders are able to adequately and effectively enforce their rights.

PARAGUAY

Ciudad del Este

Ciudad del Este has been named in the List and/or the Special 301 Report for over 16 years. The border crossing at Ciudad del Este and the city itself have long been known as a regional hub for the distribution of counterfeit and pirated products in the Brazil-Argentina-Paraguay 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. Despite Paraguay's stated goal to transform Ciudad del Este into a legitimate marketplace, including commitments to take specific steps to improve IP protection and enforcement, effective seizures at Ciudad del Este remain inadequate to stem the tide of counterfeit products. USTR commends the recent efforts by the Attorney General to increase IP prosecutors in the city. While Paraguayan authorities, including the National Directorate of Intellectual Property

(DINAPI), continued enforcement actions in 2018, including conducting raids, seizing merchandise from vendors, and interdicting cargo, seizures and raids in Ciudad del Este remained relatively low due in part to weak coordination between authorities. USTR urges effective coordination and information sharing between the DINAPI and the Attorney General.

PERU

Polvos Azules, Lima

Polvos Azules is a popular shopping center located in the heart of Lima. Its stores sell a broad range of illicit goods, including counterfeit consumer goods, clothing, shoes, appliances, toys, and electronics. In July 2018, according to local media, officers from the Fiscal Police unit of the National Police seized 17,000 pirated CDs, DVDs, and Blu-ray discs in a basement at Polvos Azules where they were allegedly being produced. This raid illustrates the scale of the problem and the need for sustained enforcement leading to successful criminal prosecution. Stakeholders are concerned that due to the strong influence of business interests benefiting from the illicit trade, local authorities may be reluctant to commit resources to IP enforcement at Polvos Azules.

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. Large volumes of counterfeit handbags and shoes are reported to be sold openly to the public. Other counterfeit products said to be sold are clothing, toys and games, computer and phone accessories, household goods, jewelry, watches, and electronics. Stakeholders note that more counterfeit products are offered for sale than genuine products. USTR urges the Philippines to enhance and sustain enforcement actions to deter sales of counterfeit goods at this market.

RUSSIA

Sadovod Market, Moscow

A new entrant to the List this year, the Sadovod Market is reportedly the largest trading center for consumer goods in Russia, with over 8,000 stores frequented by approximately 36 million people a year. In addition, representatives of businesses from across Russia and Central Asia allegedly use the market to make wholesale purchases for their business operations. Unfortunately, reports indicate that a variety of counterfeit apparel, accessories, and toys 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.

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 at this market, despite enforcement efforts by the Spanish National Police and Civil Guard in 2016 and 2018. 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. There has been a lack of sustained local enforcement efforts. In addition to Els Limits de La Jonquera, some stakeholders reported a sharp increase in street sales of counterfeit products across the cities of Barcelona and Madrid, particularly in tourism centers. USTR notes that authorities are reportedly unwilling to address the problem, despite awareness of it. USTR urges Spain to work with landowners, 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, 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, Turkey is among the largest and oldest markets in the world and a top tourist attraction in Turkey. The market's 61 covered streets include over 4,000 shops that reportedly sell counterfeit jewelry, watches, perfumes, cosmetics, wallets, handbags, and other leather goods. Right holders report that periodic raids by Turkish police have been insufficient to overcome the scale of the problem.

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. Commentators have estimated that the market has an estimated 150,000 customers per day. Vendors sell large volumes of counterfeit goods, reportedly sourced from China, including clothing, jewelry, luxury goods, and perfume. According to stakeholders and local media, the market operates according to its own laws 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.

UNITED ARAB EMIRATES

DragonMart and Ajman China Mall

DragonMart and the Ajman China Mall serve as important markets for China-sourced counterfeit goods, and both remain on the List in 2018. Together, these two markets host over 5,000 stores selling a broad range of goods, including appliances, stationery, communication and acoustic equipment, lamps, household items, building materials, furniture, toys, machinery, garments, textiles, footwear, handbags, and watches. In addition to serving the UAE market, these two marketplaces also serve as gateways to distribute counterfeit goods to foreign markets, particularly in the Middle East, North Africa, and Europe. An estimated 80 percent of the companies operating in the Ajman China Mall are Chinese, and China supports the project as part of the China Council for the Promotion of International Trade's 2010 "Going Out" strategy paper.

VIETNAM

Ben Thanh Market, Ho Chi Minh City, and Dong Xuan Market, Hanoi

Ben Thanh Market in Ho Chi Minh City and Dong Xuan Market in Hanoi are two of the most well-known retail markets in Vietnam. At Ben Thanh Market, industry estimates that the quantity of counterfeit items exceeds one million units per marketplace and that this causes harm to right holders of roughly $50 million. At Dong Xuang Market, sellers offer a wide range of counterfeit goods, including cosmetics, apparel, footwear, handbags, and phones. Although some markets in Vietnam have been the target of raids and seizures of both counterfeit goods and labels—and many vendors have also made written commitments to refrain from selling counterfeit and contraband goods—penalties are reportedly not strong enough to deter violations. 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.

Public Information

The 2018 Notorious Markets List is the result of the ninth OCR of Notorious Markets, which USTR initiated on Aug 16, 2018, through a Federal Register Request for Public Comments. The request and responses are available at WWW.REGULATIONS.GOV, Docket Number USTR-2018-0027. USTR developed the 2018 List in coordination with the federal agencies represented on the Special 301 Subcommittee of the Trade Policy Staff Committee (TPSC). Information about Special 301, the TPSC, and other intellectual property rights-related processes and issues is available at HTTPS://USTR.GOV/ISSUE-AREAS/INTELLECTUAL-PROPERTY.

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