RUSSIAN FEDERATION

INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE (IIPA)
2020 SPECIAL 301 REPORT ON COPYRIGHT PROTECTION AND ENFORCEMENT

Special 301 Recommendation: IIPA recommends that the Russian Federation be retained on the Priority Watch List in 2020.[1]

Executive Summary: Russia, in recent years, has made significant reforms to its civil procedures and streamlined its processes, to require websites with infringing content to comply with rights holders' takedown notices. These reforms have allowed the Russian courts (in particular, the Moscow City Court), working with RosKomNadzor (the Federal Service on Communications and Mass Media) to disable access to infringing sites. Additionally, the court orders can extend—without reapplication to the court—to clone, proxy and mirror websites containing infringing content. Online search services are also required to exclude infringing websites (identified in the court orders) from search results. A Memorandum of Understanding (MOU) between key Russian Internet companies (Yandex, *Mail.ru* and Rambler) and rights holders—signed in November 2018—is now being re-worked into legislation for possible adoption by the Duma in 2020. The legislation would convert the MOU from a voluntary agreement to cooperate into an obligation for search engines to delist sites identified either by court order or on a registry of infringing sites, and will be broadened to cover all copyrighted works (not just audiovisual works as in the original MOU).

Overall, these reforms have blocked or slowed access to some major infringing sites and services. Unfortunately, American rights holders continue to report that these procedures are being directed only against the infringing activity of users within Russia, and are not being used against Russian sites and services catering to users outside the country. This has resulted in a substantial and persistent international copyright piracy problem, with users in major markets accessing infringing Russian sites and services. Even the most effective takedown procedures and processes to disable access to websites can only slow piratical activities. These actions have little lasting deterrent effect without civil, and especially criminal, prosecutions directed at commercial site operators and owners.

Two additional legal reforms are recommended: first, Russia should clarify its Civil Code on the legal liability of Internet Service Providers (ISPs), including that any safe harbors only apply to neutral and passive activities. Second, the takedown procedures should be expanded to cover mobile apps, now the most popular means of infringement. There are two other industry-specific priorities in Russia. One is to address long-standing problems concerning collective management of music rights in Russia that have resulted in revenues being a fraction of what they should be for a market the size of Russia. The state accredited Russian collecting societies are not operating with transparency or good governance rules consistent with international norms. The other priority is to address the camcording of motion pictures with many feature films being illegally copied in theaters and migrating online.

PRIORITY ACTIONS REQUESTED IN 2020

- Increase the number and effectiveness of criminal IPR cases focused against digital piracy, including a focus on deterrent criminal actions against organized criminal syndicates. Criminal actions should target those involved in piracy retail chains that continue to sell pirated entertainment software, music and movies.
- Increase the number of administrative actions (in addition to the criminal actions, noted above) against Internet piracy regardless of whether the servers or users are located in Russia.

[1]For more details on Russia's Special 301 history, see previous years' reports, at https://iipa.org/reports/reports-by-country/. For the history of Russia's Special 301 placement, see https://iipa.org/files/uploads/2020/02/2020SPEC301HISTORICALCHART.pdf.

- Implement regulations on the operation of collecting societies that confirm that rights holders have the legal and practical ability to determine how to exercise their rights, including whether to choose to entrust licensing to any collective, and if so, to choose that entity and to delineate the rights for such collections.
- Amend the Civil Code, Part IV, to:
  - clarify the basis for liability for providers of online services that induce or encourage the infringement of copyright and related rights, or that facilitate infringement and do not take reasonable steps to prevent such activities, to prevent knowing facilitators from enjoying these safe harbor benefits; and
  - provide additional legal norms that create incentives for ISPs to cooperate with rights holders in fighting infringement taking place over their networks. Article 1253.1 of the Civil Code provides that intermediary services facilitating the widespread dissemination of unauthorized content cannot benefit from the liability privileges if they know or should have known of an infringement.
- Amend the Civil Code in Article 1299 to provide civil liability for commercial trafficking in circumvention devices.
- Amend the Criminal Code to establish criminal liability: (i) for the unauthorized camcording of motion pictures; (ii) against principals in legal entities, including for IPR crimes (the Civil Code limits civil liability to the legal entities, not the principals of those entities); and (iii) for the importation of and commercial trafficking in circumvention devices.
- Amend the Administrative Code by eliminating the for-profit requirement in Article 7.12 (Administrative Offences), and raise administrative penalties to deterrent levels by implementing higher fixed fines for violations by legal entities and individuals.

THE COPYRIGHT MARKETPLACE IN RUSSIA

Internet Use and Piracy: Internet access has grown exponentially in the past few years—109.4 million Russians (of a total population of 144 million) have Internet access, and of those, 92 million are mobile Internet users. However, despite laudable legal reforms to mitigate digital piracy, Russia remains home to many of the most popular illegal services in the world, with commercial-scale infringing websites, including web-based (and peer-to-peer (P2P)) downloading and streaming sites, linking sites, and cyberlockers, offering access to unauthorized music, film, video games, books and journal articles. Many of these sites cater to English-speaking and other non-Russian users, resulting in financial harm to markets outside of Russia. Some BitTorrent and other pirate sites have reportedly moved their sites to foreign hosting locations in response to the new enforcement measures (or court-ordered injunctions) directed at sites within Russia.

While the new laws have helped, most ISPs and website owners do not comply with takedown notices, absent court orders, instead merely forwarding notices to users without taking down material. Often the Russian websites insist on proof of copyright ownership before even considering compliance with takedown requests. There are a few exceptions, with some industries reporting that a few sites do comply with takedown notices. The 2018, MOU signed by various rights holders and Internet platforms has facilitated cooperation with the platforms who signed the MOU. The MOU, which was set to expire in September 2019, was extended until January 31, 2021. Compliance would improve overall if the MOU obligations were to be enacted into law, and applicable to all Russian platforms and search engines. One set of actors who currently do not cooperate at all with the copyright industries are the advertising agencies and payment processors that financially support infringing sites.

In April 2019, the U.S. Government included several Russian online sites on its Notorious Markets List (the 2018 list, released in April).[2] In that report, USTR retained *rapidgator*, *rutracker*, *sci-hub* and *libgen.io* on its list of Notorious Markets—with the two former sites a perennial presence on the lists since 2012. As USTR noted, the cyberlocker *rapidgator* collects revenue through its premium membership and subscription plans and targets itself to users outside of Russia. The other site, *rutracker.org* (formerly *torrents.ru*) is a BitTorrent portal that first launched in 2010 in response to the takedown of *torrent.ru* by the Russian enforcement authorities; it has over 13 million registered users. It was subject to a blocking order (a permanent injunction) by the Moscow City Court, but then moved its

[2]See, https://ustr.gov/sites/default/files/2018_Notorious_Markets_List.pdf.

operations to several mirror sites. The third site mentioned by USTR is *seasonvar.ru*, based in St. Petersburg, which is a streaming website of television programs with over 15,000 TV series on the site. USTR also included *vk.com* (*vKontakte*) to the list which is one of the most popular sites in the world distributing thousands of unlicensed motion picture files (even though it negotiated licenses a few years ago with some of the music companies for its use of music).

Another problematic site is the Russian-hosted *firestorm-servers.com*. Rights holders have observed 6,400 active users on this site playing *World of Warcraft* without having to pay the monthly subscription fee established by the owners of the online video game. Additionally, Russia is a haven for the production of cloning software and the hacking of entertainment software programs. In 2019, the video game industry noted *rutracker.org*, *torrent-igruha.org* and *nyaa.si* (hosted by a Russian company) as particularly problematic, with the latter BitTorrent site, hosting 34 million visits a month, and very popular in Japan and the U.S. For the seventh consecutive year, Russia was first in the world in the number of connections by peers participating in the unauthorized file sharing of select video game titles on public P2P networks. Russia is first in the world when it comes to the unauthorized file sharing of video games on PCs with nearly six times as many illicit downloads to PCs in Russia compared to the second highest country, Ukraine. In 2019, users with Russian IP addresses accounted for approximately 32% of the global volume of detected infringements occurring on public P2P networks.

The market for recorded music should be much stronger than it is for a country the size of Russia. According to a September 2019 industry report, the per capita spending on music in Russia is only US$.68 per year, compared with US$20.26 per capita in the U.S. (IFPI Global Report 2019). The recording industry reports that paid download sites (e.g., *mp3va.com*) remain a source of piracy in Russia along with stream-ripping services, P2P services, linking sites and cyberlockers (e.g., *turbobit.net*), with some sites including pre-release music. The recording industry notes that some stream-ripping services are believed to be operating from Russia including *Flvto.biz, 2Conv.com* and *Flv2mp3.by* (all three offer essentially the same material operating from different domains). The sites provide downloads of converted YouTube videos to users as MP3 audio files (from servers in Germany). In Italy, in November 2018, AGCOM (the telecom regulator in Italy) ordered ISPs to block access to *Flvto* and *2Conv.com*, and in January 2019, it blocked *Flv2mp3.by*. In December 2018, a Danish Court also ordered ISPs there to block access to those sites. In April 2019, courts in Australia and Spain also blocked those sites. Examples of major stream-ripping sites are: *newalbumreleases.net*, a popular linking site which has a large library of newly-released popular music available, and *mp3va.com* which has the look and feel of a legal music site like Amazon or iTunes, but sells downloads of single tracks for less than 15 cents (and albums for US$1.50 or less). Some of the other unlicensed pay-per-download sites include: *mp3panda*, *mp3fiesta* (hosted in Russia) and *mp3eagle.com* (hosted in Russia with many of its users from the U.S.). In the past few years, access to illegal music via apps in Russia has grown exponentially, and major sources of these apps do not respond quickly (e.g., Apple), or, in some cases, at all, to takedown notices. The draft legislation that would block mobile apps (as the current law does for websites) would significantly improve this particular problem.

In 2016, *vKontakte* (*vk.com*), the most popular online social network in Russia, agreed to music licenses with several major record companies. In spite of these licensing agreements, the U.S. Government has retained *vKontakte* on the Notorious Markets List for the past three years. In its report in April 2019, the U.S. Government noted that despite the agreements with record labels, *vk.com* (now owned by *Mail.ru*) remains a source for thousands of infringing motion picture files. *vk.com* has a functionality specifically designed to enable its members to upload files, which includes hundreds of thousands of unlicensed copyrighted works, especially film materials available in many languages, including English. Beginning in 2016, *vk.com* limited access to third party apps, making it more difficult for users to download content directly, and it also has experimented with content recognition technologies. *Vk.com* also blocks infringing sites from accessing videos stored on its site, but third party pirate sites can still stream illegal content from another service operated by the same parent company. According to the motion picture industry, *vKontakte* is still serving as a major infringement hub for illegal film materials. The publishing industry (particularly trade book publishing), is similarly affected by e-book piracy on the site. Although the site is responsive to notifications of infringement, piracy remains a concern given the ease with which the site's users can upload and share pirated e-books and audiobooks. The video game industry reported that there has been a continuing decline in the distribution of video game items by groups distributing in-game items on *vk.com* for the past few years, and that the site has been generally responsive to takedown notices. However, in 2019 *vk.com* played a larger role in the distribution of illegal

copies of video games, including by users putting ready-to-download BitTorrent files on their social media pages on the platform.

In general, publishers report online enforcement is hampered by low compliance rates in response to rights holder notifications for links to infringing content, with many sites ignoring the notices altogether. P2P piracy providing free unauthorized access to e-books continues to be an issue as well. Book and journal publishers remain concerned by the prevalence of online book and journal piracy in Russia, particularly on hosted-content websites that are operated by Russian residents. The most egregious actor is the search engine/locker site *Sci-Hub.io* (formerly *Sci-Hub.org*) which appears to collaborate with a group of sites known as the "Library Genesis Project" (now *libgen.io*). Sci-Hub claims that as of October 2019, its servers hold some 79 million copyright-protected journal articles (more than 85% of articles published in toll access journals) and over 6 million books.[3] To further its infringing activities, *Sci-Hub* gains unauthorized access to university systems and publisher databases through compromised user credentials, obtaining the credentials through phishing schemes, and using the compromised credentials to harvest copies of copyrighted journal articles, which it then hosts on its own server network, as well as cross-posts to *libgen.io*. Notwithstanding two injunctions against the site, *Sci-Hub* unfortunately remains accessible in the U.S. The *Libgen* site encourages the creation of mirror sites of all of its content, and several such sites remain active.[4] In October 2018, publishers successfully sought an injunction to block the sites' primary domain in Russia. In 2019, a permanent block issued against *Libgen.org*, while a permanent injunction against the primary site's continued operation in Russia is expected to take effect this year. In December 2019, the Department of Justice (DOJ) confirmed that it is investigating the founder and operator of *Sci-Hub*, on suspicion this individual is working with Russian intelligence to steal U.S. military secrets from defense contractors.[5]

The independent segment of the film and television industry (IFTA) reports that online and physical piracy remain a significant export constraint for independent producers and distributors, the majority of which are small to medium-sized businesses and cannot engage in lengthy and expensive civil enforcement. Independent producers partner exclusively with authorized local distributors to finance and distribute films and television programming. As a result of the piracy, legitimate distributors cannot commit to distribution agreements, or alternatively, offer drastically reduced license fees which are inadequate to support the financing of independent productions. Revenue from legitimate distribution services, which are licensed country-by-country, is critical to financing the development of new creative works worldwide. Since Internet piracy in one territory affects other markets instantly, this type of infringement not only undercuts anticipated revenue from the distribution of a particular asset, it also harms the ability of independent producers to secure financing for future productions. The independent production sector cannot easily shift to new business practices that might otherwise limit piracy, such as worldwide same day release (referred to as "day-and-date" releases), since national distributors release films on their own schedules in synch with local release patterns that include compatibility with local holidays as well as investment in local marketing and advertising.

Civil Enforcement Against Online Piracy: As noted, civil judicial remedies have significantly improved in the recent years with the 2013, 2014 and 2017 reforms (as have administrative remedies). RosKomNadzor is the agency responsible for enforcement of these laws, and as noted, has been effective and cooperative with rights holders in implementing the new laws, in coordination with the Moscow City Court.

---

[3]"Sci-Hub provides access to nearly all scholarly literature." https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5832410/.

[4]Active mirror sites include: *b-ok.cc, b-ok.org, b-ok.xyz, b-ok2.org, bookfi.net, bookre.org, gen.lib.rus.ec (main site), lib.rus.ec (main site), libgen.is, libgen.lc, libgen.me, Libgen.org, libgen.pw, fiction.libgen.me, libgen.li, bookslabs.xyz, collegefun.org, booksdescr.xyz,* and *openlib.xyz*. In a 2015 case brought by an AAP member company, *Sci-hub.org*, the Library Genesis Project (*Libgen*), and its operators were found to have engaged in infringing activity by a court of the Southern District of New York, for the unauthorized reproduction and distribution of journal articles, and to have violated the Computer Fraud and Abuse Act, for Sci-Hub's intrusions into publisher databases. Damages in the amount of $15 million were awarded, and a permanent injunction issued. In November 2017, following another case brought by another AAP member company, a district court in Virginia issued a second default judgment against *Sci-Hub* (then at *Sci-Hub.io*) of $4.8 million, enjoining *Sci-Hub* and "those in active concert or participation with them" from infringing the publisher's copyright, and also ordered "any person or entity in privity with *Sci-Hub* and with notice of the injunction, including Internet search engines, web hosting and Internet service providers, domain name registrars, and domain name registries, cease facilitating access to any or all domain names and websites through which *Sci-Hub* engages in unlawful access to, use, reproduction, and distribution" of the publisher's trademarks or copyrighted works.

[5]For a newspaper account of this investigation, see: https://www.washingtonpost.com/national-security/justice-department-investigates-sci-hub-founder-on-suspicion-of-working-for-russian-intelligence/2019/12/19/9dbcb6e6-2277-11ea-a153-dce4b94e4249_story.html.

The 2013 legal reforms included two key civil law changes and procedures directed at online piracy. The first change amended the Civil Code, Part IV—in theory, to provide for third party liability, as well as safe harbors from such liability for "information brokers" (ISPs) that comply with all the requirements for those safe harbors. Unfortunately, the changes did not provide clarity regarding the liability of online infringing websites and services, so that safe harbors apply only to activities that are merely neutral or passive. The second 2013 reform included a set of amendments to the Civil Procedure Code (and corresponding amendments to the Arbitration Procedure Code and the Federal Law on Information and Information Technologies (2006)) authorizing judicial injunctions after notice and takedown to block access to infringing materials or websites. In 2014, amendments expanded the subject-matter scope of the 2013 changes (Federal Law No. 364, in force May 2015) and expanded the existing procedures for court ordered site-blocking against repeat infringers.

The 2017 reform (Federal Law No. 157, in force October 1, 2017) addressed the problems of clone, proxy and mirror sites by broadening the Russia court ordered (civil) injunctions to cover these sites as well as the original infringing site. Under the 2017 law, with an existing court order against an infringing website, a rights holder can submit a request to the Ministry of Digital Development, Communications and Mass Media (Ministry of DDCMM) identifying a mirror (or clone or proxy) site, and, after review by the ministry, RosKomNadzor issues instructions to block the mirror site; an administrative procedure is then used to block mirror site. No special request to a court is needed from a rights owner; rather, a list of qualified blocked websites is provided by rights holders via an online mechanism to the Ministry of DDCMM, although it is limited to 50 or 60 site blocks per day under regulations it adopted in October 2017. The ministry's decisions—which must be made within 24 hours of receipt of a rights holder's request—can be appealed in the courts. The 2017 legislation also required that search engines must remove links to infringing content on sites that have been the subject of an order from the courts or the Ministry of DDCMM. RosKomNadzor oversees compliance of both ISPs and search engines with this process. There are fines of up to 700,000 rubles (US$11,300) for search engines that do not comply with de-indexing orders. An additional change was adopted on April 23, 2019 in a Resolution of the Plenum of the Supreme Court (revising Chapter IV of the Civil Code), which amended existing practices to permit the use of screenshots of websites with unauthorized material on them to be treated as sufficient evidence to obtain a court order under the (2015, 2016 and 2017) laws.

A 2018 proposal before the Duma would apply the same website blocking procedures to mobile apps. There are two other pending proposals (recommended by the Ministry of Culture): one to block anonymous pirate websites without applying to a court; the other to accelerate enforcement of site blocking orders (from three days to one day). The Federal Tax Service (FTS) also has the authority to block the use of anonymizers and to create a list of banned resources to bypass blocked websites, but its jurisdiction is specifically limited to acting against illegal online gambling operations. The FTS can also request that RosKomNadzor block anonymizers, so there is in place effective authority to take action against online piracy if the Government of Russia chooses to apply it. Separately, a law was introduced in the Duma in 2017 to provide monetary penalties (up to 800,000 rubles; US$12,917), for attempts to bypass website blocking orders under the law applicable to anonymizers and virtual private network (VPN) services. The VPN law went into force in November 2017; the other law providing penalties has not yet been adopted.

The results of all of these new civil laws and procedures have been positive, with increasing numbers of injunctions, including permanent injunctions issuing against various infringing Russian websites. Overall, some sites have seen dramatic decreases in traffic right after such orders (and some sites have even moved out of the country). While these actions are commendable, without the deterrence of criminal prosecutions against the owners and operators of infringing sites and services, many simply resurface in new guises. The motion picture industry reports that in 2019, more than 2,500 domains of copyright infringing websites were blocked (15% the result of court orders and 85% the result of RosKomNadzor decisions against mirror sites, and that since 2015, the annual numbers of sites taken down or blocked have increased yearly. The music industry reports that, to date, over 2,000 music-related sites have been blocked.

The video game industry alone identified over 95 video game-oriented piracy websites blocked in 2018, and 42 sites blocked in 2019. There are many examples of injunctions against major infringing sites, including those against *rutracker.org* and *rutor.org*. However, workarounds still exist, and Internet users have obtained access via mirror sites

(and alternative DNS services) and VPNs, so sites such as *rutor.org* and *rutracker.org* retain millions of monthly users in spite of the laws.

As noted, there was a November 2018 MOU with rights holders (almost exclusively Russian), search engine operators and social networks for operators and networks to remove URLs to illegal content (i.e., audiovisual works), first set to expire in late 2019; it has now been extended until January 31, 2021. A legislative substitute is also under consideration to establish mandatory obligations for operators and networks, and make the current MOU terms applicable to all works, including books, music, and business and entertainment software (video games). In January 2020, RosKomNadzor reported that during the initial term of the MOU (November 2018 to the end of 2019), 2.1 million links were delisted.

Criminal Enforcement Including Against Online Piracy: According to the Ministry of Interior, the reported number of crimes related to copyright violations decreased by 22% from January to October 2019 from the same period in 2018. Since the copyright industries continue to report high levels of piracy, criminal enforcement appears to have declined in Russia, continuing the trend of the past several years. Criminal enforcement in Russia has unfortunately, not focused enough on digital piracy. A few industries, such as IFTA, report that physical piracy remains a problem for independent producers and distributors (although not as large a problem as digital piracy). High quality pirated DVDs and artwork are routinely sold in street markets or uploaded and offered for free online, destroying the legitimate market for these works.

To be effective, IPR enforcement in Russia needs a clear nationwide governmental directive on enforcement with a particular focus on online piracy. Without coordination and a high-level directive, criminal and administrative enforcement practices have varied considerably from region to region within Russia, and have had little deterrent effect. Any coordinated nationwide campaign should focus on *ex officio* criminal actions targeting large-scale commercial enterprises, as well as on taking administrative actions and strengthening administrative penalties. This would allow legitimate markets to develop and would also help support smaller independent rights holders who do not have the resources, and therefore must rely on the government for effective enforcement.

The agencies that can commence criminal cases—including the Investigative Committee of Russia, the Investigative Department of the Ministry of Internal Affairs (MVD), the Federal Security Service of the Russian Federation (FSB), and Customs—should coordinate their efforts with the police. Since the General Prosecutor's Office has supervisory authority over investigations and prosecutions, it should work with the Investigative Committee of Russia and the Investigative Department of MVD to develop an updated and detailed methodology for investigations of digital copyright infringements. This would help to increase the quality, effectiveness and consistency of IPR enforcement activities. Work on a draft methodology was suspended several years ago.

IIPA continues to recommend that there should be a dedicated digital IPR enforcement unit within the Government of Russia to focus on this problem. For example, combating copyright violations on the Internet, such as the dissemination of music through illegal pay-per-download sites and illegal P2P or streaming services, does not clearly fall within the current jurisdiction of the Computer Crimes Department (Department K) within the MVD, even though they have occasionally taken action in the past (at present, only the Economic Crime Police are doing this). Department K's authority and responsibility to act in all cases of online infringement should be clarified and strengthened. In addition, Department K should be properly staffed, equipped and resourced, and other such units within the MVD should be formed to deal exclusively with IPR Internet cases and to train officers on how to combat these copyright crimes, including the maintenance of evidence. It also should be clarified that actions can be brought under the Code of Administrative Offenses against commercial actors involved in the massive distribution of infringing material, even where there is no direct fee charged by the enterprise.

Changes to criminal procedure which placed copyright infringement cases into the category of serious crimes have enabled—at least in theory—Russian law enforcement agencies to conduct thorough and comprehensive investigations against owners and operators of piratical operations. However, deterrent criminal penalties have rarely, if ever, been imposed against owners of commercial Internet operations. In recent years, police and prosecutors have

had difficulty applying the criminal law thresholds to Internet crimes (and especially have had difficulty proving intent, or in identifying the individuals responsible for criminal activities). As a result, few such cases are ever brought and even fewer tried to a conclusion. The problem has been an inability to adopt a unified formulation by the police and prosecutors on how to apply the thresholds for online crimes. An intensification of criminal investigations and criminal convictions against principals of organized commercial pirate syndicates is sorely needed. The status quo only further corroborates the lack of political will or incentives by government agencies to act against large-scale copyright infringers. In addition to criminal enforcement, the relevant administrative agencies (e.g., the Federal Anti-Monopoly Service (FAS)) should target large illegal distribution enterprises, such as the large-scale unlicensed services responsible for most of the illegal distribution of music and film in Russia.

For the past several years, the quality and quantity of criminal raids and police activity against IPR infringers in general has declined, especially against large-scale online infringers. The decline in police activity in general is the lingering result of the 2011 major reorganization of the police force and the consequent drop in resources, as well as changes in government priorities and an unwillingness to take action against large-scale online infringers. As in recent years, there were some deterrent sentences and prison terms applied by the Russian courts, including a handful aimed at serious repeat offenders.

The lengthy criminal investigative process must also be examined and redressed, particularly at the provincial level. As the government continues to rely on its own experts in investigating, examining and prosecuting IPR violations, it should take measures to increase the number of experts and consider the appointment of a specialized unit of investigators and prosecutors, adequately trained and provisioned to effectively address IP crimes. Due to the lack of adequate staffing and the high volume of work, examinations of products seized take months. The video game industry continues to report delays in examination reports from government experts, due to a lack of technical expertise. For the video game industry, enforcement efforts are also complicated by other issues including new legislation, changes in jurisdiction or new personnel. Enforcement is also hampered, and trials delayed, by the requirement that exemplars be collected only with the participation of state officials, and by a statutory reliance on government expert reports. Delays also result from a lack of subject matter expertise in some cases as well as a reluctance to use or rely on rights holder expertise on forensic matters. Worse, some local authorities refuse to share any information on cases with rights holders at the investigative stage, making effective cooperation extremely difficult. The rules should be modernized so that industry experts can be more effectively integrated into the judicial process. One way to accomplish this would be for the Supreme Court to issue new guidelines on the admissibility of the testimony of private experts. It is reported that some courts will accept private expert testimony, but a uniform rule would be more effective.

Improvements should also be made with respect to court procedure. The criminal procedures generally permit a rights holder to request the destruction of the seized goods or move for recovery of damages in a separate proceeding before the Arbitration Court (a court of general jurisdiction). However, the criminal courts are reluctant to order this and treat these as civil law matters instead. The copyright industries recommend that the Supreme Court clarify guidelines on the destruction of goods and the calculation of damages in online cases for the purpose of meeting the minimal criminal damage thresholds established under the (revised and increased) Article 146 of the Criminal Code.

Another recommended measure to increase the efficiency of IPR criminal investigations is the appointment of IPR special prosecutors, investigators, and police officers at both the federal and regional levels throughout Russia. IIPA recommends that the Investigative Department of MVD and the Investigative Committee of Russia continue to work with IIPA members on future training programs, and that the General Prosecutor's Office (along with the MVD-IC) appoint a government liaison with IP rights holders to more effectively bring criminal investigations and trials to successful conclusion. This would also help to improve criminal enforcement nationwide, since expertise and enforcement practices vary widely throughout the country, especially with respect to digital piracy. A similar step to improve this problem would be the establishment of an official uniform methodology for the investigation and prosecution of copyright and related rights infringements, focused on digital enforcement. In 2013, a specialized IP court in Skolkovo (the innovation center) was launched with 30 trained judges. This was a positive step in IP enforcement, but is limited to patent cases. These courts should be created in other cities and regions across Russia and the jurisdiction broadened to handle copyright, as well as patent cases.

Russia's current Criminal Code does not allow for corporate entities to be held criminally liable for infringement; the Code should be amended. At present, only a natural person (usually a corporation director) can be found criminally liable, and only upon a showing that he/she had a direct intent to commit the infringement. It is extremely difficult to meet this burden of proof, so many cases are suspended without any penalty.

Camcord Piracy: Russia remains the home to some of the world's most prolific criminal release groups of motion pictures. Pirates obtain their source materials for infringing copies by camcording films at local theaters, and then upload these copies onto the Internet as well as sell illegal hard copies. In the past four years, 201 MPA-company films have been camcorded in Russia and, an additional 144 audio-only recordings were sourced from Russia. The total number of sourced audiovisual camcord copies from Russia decreased very slightly in 2019 to 45 (down from 48 in 2018); in 2019 there were 30 audio-only recordings sourced from Russia. Most of the Russian camcords come from Moscow, Kazan, Novosibirsk, Rostov-On-Don, Ekaterinburg, and Naberezhnye Chelny. The illicit camcords that are sourced from Russia are of fair quality, but they remain in high demand by international criminal syndicates. Copies of major film titles often appear online within a few days of theatrical release, damaging revenues worldwide and across the economic lifecycle of the film. The Russian-Anti Piracy Organization (RAPO) assists security personnel (trained by RAPO) whenever possible with interdictions. To address the camcord problem, the Government of Russia needs to amend Article 146 of the Administrative Code; it has been reported that this legislation may be delayed until 2021. The government should also properly resource and undertake more effective enforcement against illegal camcording of motion pictures.

Civil Enforcement in General: Civil measures are not capable of providing the requisite level of deterrence against this type of piracy. However, if, properly applied, civil enforcement can be a useful tool for some industries (as it has in the courts' actions against some websites), but this is not viable for all parties and especially independent creators, such as independent film and television producers. For those who are able to pursue civil enforcement, there remain many inadequacies, including: (i) remedies limited to the seizure of specific copies of works that are the object of a lawsuit; (ii) failure to award preliminary injunctions (although 2013 amendments made some improvements), or to freeze assets and evidence; (iii) low damages awards, which, like all awards, are also very difficult to enforce; (iv) burdensome evidentiary requirements, including rights ownership information; (v) absence of personal liability for the directors of infringing companies or enterprises (the only way to bring proceedings in cases where bogus companies operate); (vi) absence of the notion of clear contributory liability under the Russian civil law system dealing with copyright infringements; and (vii) absence of judicial guidelines on civil search practices, including provisional measures consistent with the WTO TRIPS requirements.

One very troubling development is a proposal to lower fines (statutory damages) from their current levels, below the minimum levels set in the Civil Code (currently US$170) per infringement. Awards imposed by the courts are already too low; further lowering the permissible levels will not be a deterrent. This proposal, adopted at a first reading in the Duma in October 2017, remains under consideration for final passage (Amendments to Article 1252 of the Civil Code). It should not be adopted.

Administrative Enforcement: The Administrative Code (Article 7.12) provides a range of fines on natural persons (1,500 to 2000 rubles, US$24 to US$32), the owners or managers of legal entities (10,000 to 20,000 rubles, US$148 to US$296), and on legal entitles themselves (30,000 to 40,000 rubles, US$485 to US$646), as well as permits the confiscation and destruction of pirated product. Administrative cases are filed by the police or by agencies, but the levying of fines is done by courts of general jurisdiction for natural persons and juridical entities, and arbitration courts for legal entities. Imposing significant administrative fines on legal entities would have a deterrent effect, especially in instances when criminal cases are terminated for failing to meet the high evidentiary burdens. Unfortunately, current administrative procedures are inadequate because of the very low level of fines imposed and the inability to reach commercial enterprises that distribute infringing content.

Collective Administration: In 2017, legislation was enacted (in force, May 2018), to purportedly address the problems of the state accreditation system and the governance of collecting societies. Unfortunately, the new law falls far short of either providing transparency to rights holders or good governance consistent with international norms and

best practices for collecting societies. The new law amended the Civil Code and the Administrative Code to revise the make-up and activities of collective rights management organizations (RMOs). One obvious failure of the new law regarding transparency is that it neither allows rights holders to see how much money their RMOs collect, nor how much they distribute to their members.

The new law creates "supervisory boards" for each of the various authors' collection societies (the Russian Authors Society, the Russian Union of Right Holders and the All-Russian Intellectual Property Organization) consisting of members of each RMO, but also including government representatives and "user" group representatives. This does not allow rights holders to be involved in the selection and management of the organizations that purport to manage their rights. Proper management would allow for a supervisory board of rights holders to oversee the internal management of the RMO, and would include international rights holders with local representatives on the board. Instead, partial control by the Government of Russia deprives rights holders of their ability to control the licensing and collection of monies for their works and recordings, and is resulting in less, not more, money flowing to authors and producers (and certainly less money than should be collected for a market the size of Russia). Lastly, the so-called fiscal control improvements, including regular audit reports, will not improve accountability, because the audit obligations are only to the government (for taxation purposes), not to those rights holders. There are many models for proper governance of RMOs, including WIPO best practices, international rights holder group best practices, as well as U.S. and European Union existing practices.

COMPLIANCE WITH EXISTING OBLIGATIONS TO THE UNITED STATES

In three separate bilateral and multilateral agreements, the Government of Russia made commitments to take effective action against Internet piracy. First, in the 2006 U.S.-Russia IPR Agreement, Russia agreed to combat the growing threat of Internet piracy "with the objective of shutting down websites that permit illegal distribution of content protected by copyright or related rights" (and especially for websites registered in Russia's .ru domain name, or whose servers are situated in Russia), and "to investigate and prosecute companies that illegally distribute objects of copyright or related rights on the Internet."

Second, when Russia joined the WTO in 2012, as part of its WTO accession, in the Working Party Report (paragraph 1339), the Government of Russia pledged that it would "continue to take actions against the operation of websites with servers located in the Russian Federation that promote illegal distribution of content protected by copyright or related rights, such as phonograms (sound recordings), and investigate and prosecute companies that illegally distribute objects of copyright or related rights on the Internet."[6] Last, in 2012, in the U.S.–Russia IPR Action Plan, the Government of Russia agreed it would take "enforcement actions targeting piracy over the Internet" and more specifically it would, *inter alia*: "Take measures in order to disrupt the functioning of websites that facilitate criminal copyright infringement, and provide for takedown of infringing content….Take actions against the creators and administrators of websites through which intellectual property crimes are committed….Conduct meaningful consultations with rights holders to target and to take action against high-priority infringing websites." The Government of Russia has not fully implemented these obligations.

With regard to collective administration, existing regulations and state accreditations have institutionalized a system that is not transparent and lacks good governance or accountability for authors, record labels and performers—who have no other option except the state collective management organizations. Correcting this problem is also a treaty obligation. During WTO accession (in the Working Party Report, paragraph 1218), Russia assured its trading partners it would "review its system of collective management of rights in order to eliminate non-contractual management of rights within five years after Part IV of the Civil Code entered into effect," to bring the management societies in line with international standards on governance, transparency and accountability. That commitment was due in 2013. Instead, the 2017 legislative reforms (in place as of May 2018) set any progress backwards to phase out non-contractual license management schemes—now five years after Russia was obligated to fix this problem. To

[6]The U.S. Government last detailed all the intellectual property WTO commitments of Russia in its "2018 Report on the Implementation and Enforcement of Russia's WTO Commitments" (December 2018), available at https://ustr.gov/sites/default/files/Russia-2018-WTO-Report.pdf.

develop properly functioning music broadcasting and public performance payment systems, the Government of Russia must fulfill its WTO Working Party Report and U.S.-Russia IPR Agreement obligations. This would entail proper state accreditation of collecting societies in a manner that ensures that rights holders are able to control and manage their own societies, so they are fairly represented and there are no conflicts of interest in the governance structures. Fair representation in these societies includes direct representation of rights holders on the board in a manner that is proportionate to relevant market share and that reflects commercial realities.

DEFICIENCIES IN THE RUSSIAN LEGAL REGIME

Russia has made progress on legal reforms but gaps remain, especially with regard to effective Internet enforcement and implementation of the digital treaties.

IIPA and its members have in the past, commented on three major overarching concerns in the Civil Code, as amended: (a) a lack of clarity on numerous provisions, especially exceptions; (b) administrative law principles throughout the Civil Code that likely cannot be enforced by civil or criminal procedures; and (c) the absence of clear liability rules for online websites and services that induce or encourage infringement (and the applicability of safe harbors for such services). Even after the recent amendments, the law does not define ISPs and the various services they provide, nor does it link liability and safe harbors in a manner that will encourage cooperation with rights holders to effectively deal with Internet piracy. Lastly, it does not define secondary liability. If Russia is to foster legitimate electronic commerce and if the rule of law is to apply to the online world, Russia needs to develop a balanced system of liability provisions that incentivizes ISPs to cooperate in addressing Internet piracy, and one that does not provide cover for services that induce or promote infringement (or that directly infringe). Further, it is critical that Russia amend its regime to allow for injunctive relief that is quick and effective and applicable to all works, especially for Internet matters.

Other existing hurdles to effective civil and criminal enforcement are: (a) the failure of courts and police to apply statutory presumptions of copyright ownership; (b) overly burdensome evidentiary requirements to prove title; and (c) the lack of criminal liability for corporate enterprises or the principals of such enterprises. To require a "full" chain of title for each recording in every investigation is especially problematic for foreign rights holders with translation, notarization and other costs and delays. Similarly, the procedures for obtaining injunctions tied to notice and takedown (and proposals for further changes), have been criticized as being overly burdensome in requiring "proof" of ownership.[7]

Article 1299 of the Civil Code prohibits the commercial distribution (i.e., trafficking) in circumvention devices and services that circumvent technological protection measures (TPMs). The law needs to be expanded so that liability applies to the commercial trafficking in all variety of circumvention devices and services. In addition, commercial trafficking in circumvention devices–including by importation–should also be criminalized. IIPA also recommends that Article 1252(5) of the Civil Code, which currently includes remedies for the seizure and destruction of materials and equipment used in infringements, be improved by deleting the exception for the sale of materials by the state for "income," and by parallel changes in the respective procedural codes.

[7]For a detailed list of IIPA's prior comments, specifically on the Civil Code (and some of the related laws), see https://iipa.org/files/uploads/2017/12/2010SPEC301RUSSIA.pdf at page 138.

MARKET ACCESS ISSUES

There are four existing laws harming the marketplace for audiovisual content in Russia.

In 2015, a law went into force banning advertisements on pay cable and encrypted satellite channels. The law does not affect state-owned television channels because they do not rely on advertising revenue, and exempts terrestrial broadcasters who are heavily dependent on ad revenue. As a result, the law significantly impacts the market for cable and on-demand services, including those services operated by foreign companies, and hinders the growth of the pay-TV industry in Russia.

In 2017, a Mass Media Law amendment was adopted which regulates and licenses online film websites, including streaming platforms, and which limits foreign ownership of such sites to 20%. The law applies to operators of all online audiovisual services if their Russian audiences are below 50% of their total users (and, if Russian users are below 100,000/month). The usage calculation is very unclear, with severe consequences for violations, including barring a foreign entity or individual from owning or participating in these businesses entirely. The law was opposed by Russian and foreign film distributors (as a violation of international treaties) and website owners fearing that, upon adoption, it would become a tool to limit legal websites while alternatively resulting in more, not fewer, piratical film sites. Although it was initially thought to be a law aimed at preventing the expansion of foreign businesses into the local market, it is now clear the law was part of an overall scheme to control all media sectors.

Further, Russia imposes customs duties on the royalty value of some imported audiovisual materials (which include video games), rather than solely on the value of the physical carrier medium. In practice, however, digital distribution has mitigated its impact, and there have been few reported disputes with the customs authorities on this matter in the past two years. The Value Added Tax (VAT) remains very problematic and has been imposed in a discriminatory manner: only Russian-made films are given national certifications that exempt them from the VAT (which was raised to 20% on January 1, 2019). This is a WTO violation because it denies national treatment for taxes on identical foreign products.

There have been several proposals to limit the percentage of screens that can be taken by any single film. One proposal would limit the number of foreign film screenings in multiplexes or monoplexes to 35% of the total number of screenings in those theaters. If enacted, these proposals would harm the distribution and exhibition of foreign films in Russia. Another proposal would place a 3% tax on theatrical box office revenue. None of these proposals have been implemented, nor should they be implemented, as they violate Russia's WTO obligations.

In December 2019, a new law was enacted requiring manufacturers of electronic devices to install Russian software on all smartphones, computers and other devices (by July 1, 2020). The practical implication of this new law remains to be seen and also depends on the software required to be installed. The copyright industries urge the government to ensure that no unlicensed content distribution apps are installed.