

# RUSSIAN FEDERATION

## INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE (IIPA)

### 2022 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 2022.<sup>1</sup>

**Executive Summary:** The nature and scope of piracy in Russia has not changed in 2021, because of a lack of significant changes in legislation to deter infringement and a lack of enforcement by Russian authorities. However, in 2021, after several extensions of the anti-piracy Memorandum of Understanding (MOU) between key Russian Internet companies and rights holders, the regulatory bodies finalized the draft law that would work to convert this voluntary procedure into law. It is expected that the State Duma will adopt the bill in the spring session (January 2022 – July 2022). The draft has a high probability of adoption and will improve the legal framework to protect copyright online.

The bill provides for the obligation of search engines to remove links to pirated content at the request of copyright holders. Copyright holders will create special databases containing links to pirated content, which search engines must access to exclude links to pirated content from search results. Content owners will need to choose a model for the implementation of the law after its adoption.

In addition, at a meeting in Roskomnadzor<sup>2</sup> held on December 7, 2021, with the participation of parties to the MOU, an agreement was reached to sign a new version of the MOU—the MOU 2.0. The new version, which is subject to the adoption of the bill, provides for a number of new measures to stop search engines from providing easy access to infringing services. New measures in the updated version include removal of repeat offender sites from search results, removal of sites displaying over one hundred links to infringing content from search results, and measures to defeat “domain gluing.”<sup>3</sup> The deadlines for the removal of pirated links from search results by search engine operators will also be reduced.

This reform follows a recent trend in Russia to address online piracy with civil, not criminal, enforcement measures and streamlined processes to require websites, and now apps, with infringing content to comply with rights holders’ takedown notices. The reforms allow Russian courts (in particular, the Moscow City Court), to preclude access to infringing material, including clone, proxy, and mirror websites containing infringing content. The current laws and procedures also require online search services to exclude infringing websites identified in the court orders from search results.

Overall, the earlier civil and procedural reforms have precluded or slowed access to some major infringing sites and services. Unfortunately, American rights holders continue to report that these procedures are being directed predominantly against infringing activities of users in Russia and are not used against Russian sites and services catering to users outside the country and undermining foreign markets. The result is a substantial and persistent online piracy problem with no borders, as users in major markets outside of Russia access infringing content from Russian sites and services. Even the most effective takedown procedures and processes to disable access to infringing content on these websites can only slow piratical activities. These actions have little lasting deterrent effect without civil, and especially criminal, prosecutions directed at operators and owners of sites engaging in infringing content. One recommended legal reform is for Russia to clarify its Civil Code on the legal liability of Internet service providers (ISPs), including that any safe harbors apply to only passive and neutral intermediaries that do not contribute to infringing activities.

<sup>1</sup>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/2021/01/2021SPEC301HISTORICALCHART.pdf>.

<sup>2</sup>The Federal Service for Supervision in the Sphere of Telecom, Information Technologies (IT) and Mass Communications.

<sup>3</sup>“Domain gluing” is process used by operators of infringing services allowing them to return to the same search ranking from which they were removed by “gluing” pages together.



Two other industry-specific problems persist in Russia. One is the need to address the long-standing problems with collective management of music rights in Russia that have caused revenues to be a fraction of what they should be for a market the size of Russia. The state accredited Russian collecting societies are not currently operating with transparency or good governance rules consistent with international norms. The other enforcement priority is to address the camcording of motion pictures that results in many American feature films being illegally copied in theaters and migrating online worldwide.

## **PRIORITY ACTIONS REQUESTED IN 2022**

- Increase the number and effectiveness of criminal copyright digital piracy cases, especially deterrent criminal actions directed against organized criminal syndicates. Criminal actions should target those parties involved in piracy retail chains that continue to sell pirated entertainment software, music, and movies.
- Implement regulations on the operation of collective management organizations (CMOs) 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 CMO, and if so, which one, as well as 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
  - clarify the definition of the activities that qualify intermediaries to benefit from the safe harbors, to include only passive and neutral intermediaries that do not contribute to infringing activities.
- Enact the draft legislation to convert the MOU into law, making it applicable to all copyrighted works and all rights holders, with legally mandated obligations for ISPs and appropriate sanctions for non-compliance.
- Adopt a new text of the MOU that will regulate issues not included in the first memorandum and the bill.
- Amend the Civil Code in Article 1299 to provide civil liability for commercial trafficking in circumvention devices (including circumvention software), as well as for acts of circumvention.
- Amend the Civil Code, the Copyright Law, or other relevant law to address the issue of “domain hopping” that occurs after the Moscow City Court issues an initial content-removal order to expedite applications for additional relief against repeated copyright infringement.
- Amend the Criminal Code to establish criminal liability: (i) for the unauthorized camcording of motion pictures; and (ii) for the importation of and commercial trafficking (by distribution, making available, etc.) in circumvention devices (including circumvention software), as well as for acts of circumvention. Also, amend the Administrative Code to sanction camcording.
- Amend the Administrative Code by eliminating the for-profit requirement in Article 7.12 (Administrative Offenses), raise administrative penalties to deterrent levels by implementing higher fixed fines for violations by legal entities and individuals, and increase enforcement under this provision.

## **THE COPYRIGHT MARKETPLACE IN RUSSIA**

**Internet Use and Piracy:** The overall situation with online piracy remains the same when compared to last year. Russia remains host to several illicit sites that cater to English-speaking audiences, negatively impacting markets worldwide. Many pirate sites have moved to foreign hosting locations after several legal reforms that allow rights holders to seek injunctions through the Moscow City Court. However, the lack of explicit liability provisions for hosting providers creates a supportive environment for infringing services to use the infrastructure in Russia. Infringement on Russian social media and hosting platforms such as *VK*, *OK*, *Telegram*, and *DDoS-Guard* remains a significant concern for rights holders.

Internet access, including mobile phone access, has grown exponentially in Russia in recent years. Despite the civil law reforms intended to mitigate digital piracy, Russia remains home to many of the most popular illegal services in the world. These include commercial-scale infringing websites, such as web-based peer-to-peer (P2P) downloading and streaming sites, stream-ripping sites, linking sites, and cyberlockers, offering access to unauthorized music, film, video games, books, and journal articles. The other problem is significant moving of pirated content to mobile apps, such as

*Telegram*. Russia remains first globally when it comes to P2P piracy for the video game industry. 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. The development of technologically advanced pirate cloud systems (e.g., platforms as a service, often consisting of content delivery network based video providers that are accessible to only pirate streaming website operators), which provide Russian streaming websites with pirate video content, continues to grow.

Although the civil law reforms have improved enforcement by the courts, absent these court orders, most ISPs and website operators do not comply with takedown notices, instead merely forwarding notices to users without taking down material. Often, as a delaying tactic, the Russian websites insist on proof of copyright ownership before even considering compliance with takedown requests. The advertising agencies and payment processors that financially support infringing sites continue to resist cooperation with the copyright industries. The only alternative has been the voluntary MOU between some ISPs and certain local rights holders regarding delisting of infringing sites from search engines, which is why converting the MOU into legislation will help to improve the situation for rights holders, provided it is not limited to certain rights holders. The legislation should provide sanctions for non-compliance with takedown notices and should be applicable to all platforms and search engines and all copyrighted works.

Examples of the types of large-scale online piracy problems that persist are evident in the annual Notorious Markets List, and in the IIPA's past filings with the U.S. government. Many commercial-scale sites in Russia operate without deterrence, including those sites on the Notorious Markets List, offering free films, TV programs, music, books and journal articles, and video games. In January 2021, the U.S. government included six Russian online sites on its Notorious Markets List.<sup>4</sup> USTR retained *Sci-hub* (and its related sites), *VK.com* (*vkontakte*), and *MP3juices* on its list of Notorious Markets.

The motion picture and television industry is particularly concerned about *VK.com*, which is one of the most popular sites in the world and the most popular social network in Russia, along with *OK*, which is also an infringement hub. On these social media platforms, users illegally distribute thousands of unlicensed motion picture files (even though *VK.com* negotiated licenses a few years ago with some of the music companies for its use of music). *VK.com* limits access to third-party apps, making it more difficult for users to download content directly. It now 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. This means that *VK.com* is still 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 responds to notifications of infringement, piracy remains unabated given the ease with which the site's users can continuously upload and make available pirated e-books and audiobooks. In 2021, *VK.com* is still one of the main platforms for promoting video game pirate sites and marketplaces. Social networks have improved their responsiveness to take-down notices from the video game industry. These sites promptly remove any infringing material, including cheats and other unauthorized digital goods (UDGs).<sup>5</sup> However, video game piracy remains a significant problem in Russia and fuels piracy in other markets.

The video game industry reported that P2P websites remain the main search request and method of content distribution for video games for PCs and consoles. Mobile games are distributed mainly through forums, cyberlockers, and direct download sites. Since the 2018 anti-piracy MOU does not include the video game industry, links to pages with infringing content are available without the option of delisting, except through direct takedown notices. The video

---

<sup>4</sup>See

[https://ustr.gov/sites/default/files/files/Press/Releases/2020%20Review%20of%20Notorious%20Markets%20for%20Counterfeiting%20and%20Piracy%20\(final\).pdf](https://ustr.gov/sites/default/files/files/Press/Releases/2020%20Review%20of%20Notorious%20Markets%20for%20Counterfeiting%20and%20Piracy%20(final).pdf). The January 2021 report also included three physical markets in Russia, two of which are on the list for the prevalence of counterfeit (but not copyright- pirated) materials.

<sup>5</sup>Unauthorized digital goods (UDGs) are unauthorized sales of in-game digital items. They have become a growing concern for the video game industry. Closely related to these in-game items are software products (collectively known as "cheat software") that enable the unfair and rapid collection and aggregation of virtual goods, such as bots, hacks, and "cheats," or which otherwise tilt the scales in favor of one player over another. The rise of UDGs and cheat software have a negative impact on video game companies and consumers in the following ways: (1) sellers of unauthorized digital goods and cheat software divert significant revenue away from video game developers and publishers; (2) sales of digitally delivered items, like in-game digital items, have the potential for consumer fraud (such as stolen payment methods or compromised accounts) and the facilitation of money laundering schemes; (3) the unchecked sales of cheat software can threaten the integrity of game play, alienating and frustrating legitimate players; and (4) video game publishers and developers are forced into a perpetual virtual "arms race" to update their products and security technology before the sellers can update theirs.

game industry reports overall very weak compliance with takedown notices from these sites, and the very quick reposting of materials that are taken down. This industry further reports that in general, BitTorrent sites remain the main sources for downloading illegal copies of video games. However, action by the courts and injunctive relief related to mirror sites has reduced the traffic to these sites by at least 40%. In 2021, direct download sites, cyberlockers, and legitimate cloud storage services (such as *cloud.mail.ru* or *yadi.sk*) continue to be actively used primarily by pirate sites with a narrow audience. For example, pirate server sites use third-party sites for hosting their game and patch files. Wider audiences have direct download sites with mobile games, cheats, and other small gaming files. In 2021, more than 350 pirate video game sites were blocked, which consists of more video game sites blocked since the enactment of the anti-piracy law in 2013. One of the main drivers of piracy in Russia is the continued lack of a culture of legal video game consumption and an awareness regarding the threats of distributing unauthorized content, such as malware and phishing. In 2021, the compliance rate of hosting providers to takedown notices from video game providers is only approximately 41 percent.

The market for recorded music should be much stronger than it is for a country the size of Russia. According to a September 2021 industry report, the per capita spending on music in Russia is only US\$4.51 per year, compared with US\$23.91 per capita in the United States.<sup>6</sup> The most prominent forms of music piracy in Russia are the use of BitTorrent sites and stream ripping. The most popular BitTorrent site in Russia is *rutracker.org* (having received over 44 million visits from Russia in the three months between June and August 2021). Visits to the site remain high as Russian users are circumventing the permanent block imposed on the site to access the large amounts of both English and Russian content available on it. The continued popularity of the site is demonstrated in its position as the 123rd most visited site of any kind in Russia. The most popular stream-ripping sites in Russia are *savefrom.net* and *Y2Mate.com* (with the sites having received over 27.3 million and 6.9 million visits from Russia respectively during in the three months to August 2021, according to SimilarWeb.com). Russia remains home to many services supporting large-scale infringing websites, including web-based and P2P downloading and streaming sites, linking sites, stream-ripping sites, BitTorrent sites, and cyberlockers that operate globally. For example, *Newalbumreleases.net* is a popular linking site that has a large library of newly released popular music available, and *Music.Bazaar.com* and *mp3va.com* are sites that have the look and feel of legal music sites like Amazon or iTunes but sell downloads at a considerable discount. These sites undermine the sale of licensed music on legitimate platforms and remain targets for action.

Book and journal publishers report low compliance rates in response to rights holder notifications for links to infringing content, with many sites ignoring notices altogether. Most concerning to publishers is 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.is*). As of November 2021, *Sci-Hub* claimed its servers hold nearly 88 million copyright-protected journal articles, as well as millions of books found on *Libgen* and its mirror sites.<sup>7</sup> To further its infringing activities, *Sci-Hub* gains unauthorized access to university systems and publisher databases typically through compromised user credentials likely obtained through phishing schemes and uses the compromised credentials to illegally obtain copies of copyrighted journal articles, which it hosts on its own server network and cross-posts to *Libgen.io*.<sup>8</sup> Notwithstanding two injunctions against the site, *Sci-Hub* unfortunately remains accessible in the United States. The *Libgen* site encourages the creation of mirror sites of its content, and multiples of these mirror sites remain active.<sup>9</sup> 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

<sup>6</sup>International Federation of the Phonographic Industry (IFPI) Global Music Report 2021, p. 101, 158.

<sup>7</sup>*Sci-Hub* provides access to nearly all scholarly literature. See <https://www.insidehighered.com/news/2020/01/17/universities-ignore-growing-concern-over-sci-hub-cyber-risk>.

<sup>8</sup>*Id.*

<sup>9</sup>As of September 2021, there appear to be some 108 mirror sites associated with the Library Genesis Project. Of the active 108 mirror sites, the sites with the highest numbers in terms of global site traffic are: *book4you.org*; *1lib.us*; *1lib.domains*; *b-ok.cc*; *b-ok.africa*; *1lib.in*; *booksc.org*; *3lib.net*; *b-ok.asia*; and *b-ok.lat*. 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 (ISPs), 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.

several Sci-Hub mirrors in Russia took effect in 2020.

The independent segment of the film and television industry (IFTA) reports that online and physical piracy remain a significant export constraint for small- to medium-sized businesses that 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 that 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. Because 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 motion picture, music, video game, and book and journal publishing industries want Russia to take steps to keep infringing content on sites permanently down. Effective enforcement means focusing criminal enforcement actions against the owners and operators of sites engaged in large-scale infringing content, which is causing significant economic harm to all rights holders. The Government of Russia has outstanding commitments to take such action against digital piracy. In the 2006 U.S.-Russia Bilateral WTO Market Access Agreement Side Letter on Intellectual Property Rights (IPR) (2006 IPR Side Letter), 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.” When Russia joined the WTO in 2012, as part of its WTO accession, 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.”<sup>10</sup> Also in 2012, 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.<sup>11</sup>

The Government of Russia should fully and properly implement these obligations.

**Civil Enforcement Against Online Piracy:** As noted, civil judicial remedies have improved in recent years (with legal reforms in 2013, 2014, 2017, and 2020), along with administrative remedies. Although the civil injunctive relief mechanism continues to allow rights holders to enjoin notoriously infringing sites, enforcement issues still exist in Russia. The critical gap is the lack of relevant laws targeted at online piracy, “domain hopping” of pirate sites that occurs after the Moscow City Court issues an initial content-removal order, as well as the liability of hosting providers. Current regulations were designed in the offline environment, and some provisions are difficult to apply to diversified online piracy, specifically in terms of timelines, evidence fixation, and damages calculation.

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” (i.e. ISPs) that comply with all the requirements for those safe harbors. The changes did not provide clarity regarding the liability of online infringing websites and services, including that those safe harbors should apply to only passive and neutral intermediaries that do not contribute to infringing activities. Reforms in 2013 and 2014 included a set of amendments to the Civil Procedure Code (and corresponding amendments to the Arbitration

---

<sup>10</sup>WTO Working Party Report (paragraph 1339).

<sup>11</sup>U.S.–Russia IPR Action Plan (2012).

Procedure Code and the Federal Law on Information and Information Technologies (2006)) authorizing judicial injunctions after notice and takedown to enjoin access to infringing materials or websites.

The 2017 reform (Federal Law No. 157, in force October 1, 2017) addressed the problems of clone, proxy, and mirror sites by broadening the scope of court-ordered, civil injunctions to cover these sites, as well as the infringing site subject to the original order. 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, the administrative body sends notice to the hosting provider that it has enjoined the mirror site. The Ministry of DDCMM's decisions, which must be made within 24 hours of receipt of a rights holder's request, can be appealed to the courts. The 2017 legislation also required that search engines remove links to infringing content on sites that have been the subject of an order from the courts or the Ministry of DDCMM. An additional change was adopted in April 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. In 2020, the law was further amended (Federal Law No. 177, in force October 1, 2020) to apply the same civil injunctive relief procedures to mobile apps.

The pirates have found tools to navigate around these content protection tools. Part of the problem lies in how Yandex, the major search engine in Russia, indexes sites. Neither internal Yandex policy nor laws oblige Yandex to improve search and retrieval algorithms to reduce the number of pirate sites and links to infringing content. Yandex algorithms instantly or even automatically include updated mirror sites. Another tactic is to use an empty site with a relevant domain name for search engine results, which redirects to a site with infringing content. Significant changes and improvements in the piracy situation will require adoption of anti-piracy laws and policies that are relevant to the current issues affecting the creative industries.

Moreover, court practice related to title-specific civil injunctions has worsened. The Moscow City Court, under the influence of the first appellate court, changed its approach to decisions in title-specific civil injunction cases. Previously, the court prohibited a site from using the title on the site in general. Now, the court prohibits the use of the title on only the page on which it was captured. Any change of the URL allows the site to avoid enforcement under the court decision.

In June 2021, legislation was proposed in the Duma to convert the MOU with rights holders into legislation. The draft does not limit types of protected content as the MOU does. Therefore, the music and video game industries would receive the same benefits as all other rights holders, which is an improvement to the system. It is expected that the legislation likely will be adopted in 2022.

Overall, the results of the civil laws and procedures have been positive. Some sites have seen dramatic decreases in traffic right after such court orders, and some sites have even moved out of the country. Unfortunately, without the deterrence of criminal prosecutions against the owners and operators of notoriously infringing sites and services, many simply resurface in new guises. As noted, the MOU expires on January 31, 2021, and a legislative substitute is under consideration.

**Criminal Enforcement Against Online Piracy:** Russia needs to increase its enforcement activity beyond current levels to provide adequate and effective enforcement against IPR violations, including deterrent criminal penalties. A critical element of the 2006 U.S.-Russia IPR Side Letter is Russia's obligation to provide effective enforcement of IPR online. Currently, criminal cases for online piracy do not reach courts due to outdated provisions of the Criminal Code that are hard to enforce for online infringements, specifically, the definition of the "value of the crime" that sets the threshold for liability. The copyright industries continue to report high levels of piracy and declining levels of criminal enforcement, continuing a trend of the past several years. The criminal enforcement the Government of Russia has undertaken still is not focused enough on digital piracy.

To be effective, IPR enforcement in Russia needs a clear nationwide governmental directive 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. A coordinated

nationwide campaign should focus on *ex officio* criminal actions targeting large-scale commercial enterprises, improving investigations and digital tracking, as well as strengthening administrative penalties that to date have been largely ineffective. These steps 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. Because 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. Such coordination would help to increase the quality, effectiveness, and consistency of IPR enforcement activities. Work on a draft methodology was suspended years ago.

IIPA continues to recommend that the Government of Russia create a dedicated digital IPR enforcement unit to focus on online piracy. For example, combatting 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 acted on such cases in the past. 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 adequately staffed, equipped, and resourced, and other such units within the MVD should be formed to deal exclusively with intellectual property(P) 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 the enterprise does not charge a direct fee.

Changes to criminal procedure that placed copyright infringement cases into the category of serious crimes have enabled Russian law enforcement agencies to conduct thorough and comprehensive investigations against owners and operators of piratical operations, at least in theory. However, deterrent criminal penalties have rarely, if ever, been imposed against operators or 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 are 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 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 IP infringers in general has declined, especially against large-scale online infringers. The decline in police activity in general is the lingering result of the major reorganization of the police force in 2011 and the consequent drop in resources, as well as changes in government priorities and an unwillingness to pursue large-scale online infringers. Though rare, Russian courts have imposed some deterrent sentences, including a handful aimed at serious repeat offenders.

The Government of Russia should also examine and redress the lengthy criminal investigative process, particularly at the provincial level. As the government continues to rely on its own experts in investigating, examining, and prosecuting IP 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 seized products take months. The video game industry continues to report delays in examination reports from government experts, because of 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 law enforcement 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 Government of Russia should modernize the rules so that industry experts can be more effectively integrated into the judicial process. One way to accomplish this integration would be for the Supreme Court to issue new guidelines on the admissibility of the testimony of private experts. Some courts reportedly 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 to 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 these remedies and instead, treat these cases as civil law matters. 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 Article 146 of the Criminal Code, which increased such thresholds.

Another recommended measure to increase the efficiency of IP criminal investigations is the appointment of IP 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 aid in bringing more effective criminal investigations and trials leading to a successful conclusion. This cooperation 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 to establish 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 (an innovation center) was launched with 30 trained judges. This development 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.

Finally, Russia's Criminal Code should be amended to allow for corporate entities to be held criminally liable for infringement. At present, only a natural person (usually a corporate director) can be found criminally liable and only upon a showing that he or 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.

**Civil Enforcement in General:** While civil measures are not capable of providing the requisite level of deterrence against large-scale digital piracy, they can be a useful tool for some industries or in some instances. For independent creators, however, such as independent film and television producers, civil lawsuits are not viable because they are too time consuming and too costly to pursue. For those creators or producers who are able to pursue civil enforcement, many inadequacies remain. The list includes: (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 changes 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) the 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) the absence of the notion of clear contributory liability under the Russian civil law system dealing with copyright infringements; and (vii) the absence of judicial guidelines on civil search practices, including provisional measures consistent with the WTO TRIPS requirements.

There is a troubling, long-pending proposal to lower fines (i.e., statutory damages) from their current levels, below the minimum levels set in the Civil Code (approximately US\$140 per infringement). Awards imposed by the courts are already too low; further lowering the permissible levels would not be a deterrent. This proposal, which had a first reading in the Duma in 2017 and a second reading in 2018, remains under consideration for final passage to amend Article 1252 of the Civil Code. It should not be adopted, and instead, damage awards should be increased.

**Administrative Enforcement:** The Administrative Code (Article 7.12) provides a range of fines for infringement by natural persons (1,500 to 2000 rubles, US\$20 to US\$27), the owners or managers of legal entities (10,000 to 20,000



rubles, US\$133 to US\$266), and legal entities themselves (30,000 to 40,000 rubles, US\$400 to US\$533) and permits the confiscation and destruction of pirated products. The police or agencies file administrative cases, but the courts of general jurisdiction levy fines for natural persons and juridical entities, and arbitration courts levy fines 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, as well as the inability to reach commercial enterprises that distribute infringing content. Moreover, it has been an ineffective measure due to the lack of enforcement actions. In 2020, there were 711 cases under this article, in which only 429 cases included fines for a total of 4,520,000 rubles (approx. US\$63,163.95).

**Camcord Piracy:** A long-standing problem in Russia is the camcording of motion pictures, with many feature films being illegally copied in theaters and migrating online. To correct the camcording problem properly requires changes in the Russian legal framework, as well as dedicating sufficient resources and government willpower to engage in effective enforcement. 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.

Russia continues to be a significant source of illicit camcording. The total number of sourced audiovisual camcord copies from Russia decreased very slightly in 2019 to 45 (down from 48 in 2018). Numbers from 2020 are anomalous owing to COVID-19 cinema closures. However, once the theaters started to re-open, camcords started to appear immediately. 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 police are not interested in investigating such incidents because of the complex burden of proof procedure that current laws suggest. Further, enforcement action against unauthorized camcorders is complicated by the law's broad rules on evidence fixation that are impossible to implement. Separate provisions addressing illegal recording in theaters and tailored to that specific form of infringement, could enhance enforcement.

In August 2021, the Government adopted a Decree establishing the rules for film exhibition in theatres that cover the rights and obligations of both exhibitors and viewers. The Decree replaces the older document from 1994 and extends the exhibitors' rights to remove viewers who disregard the exhibition rules from the screening room, including attempting to record the film illicitly. In general, it improves the position of the exhibitors who now have a more explicit framework to interact with the viewers who attempt to record a film in the theater illicitly. However, this Decree does not resolve the issue of lack of liability for camcording. To adequately address the camcord problem, the Government of Russia should amend the Administrative Code to add liability for camcording to the general liability provisions on copyright infringements (Article 7.12) and to provide criminal law penalties as well. In 2020, the Government of Russia prepared changes to a new Administrative Code to address camcording; the Code will reportedly be completely overhauled, but the timing is unclear. The new rules, if adopted, would explicitly prohibit video or audio recordings of films in theaters and would allow theater owners to act to stop any such recordings, including removing the offending party from a theater. The proposed new law would also add administrative sanctions for camcording. While this is a step in the right direction, unfortunately, no proposals exist to amend the Criminal Code or to add any criminal sanctions for camcording pursuant to Russia's WTO and bilateral obligations. In addition to the legal reforms, IIPA recommends that the Government of Russia properly resource enforcement actions and undertake more effective enforcement against illegal camcording of motion pictures.

**Collective Management of Rights:** The long-standing problems concerning the collective management of music rights in Russia needs to be addressed properly. The ability to exercise one's rights through proper collective management is a WTO TRIPS obligation, and Russia made specific commitments on these issues as part of its accession to the WTO. In the Working Party Report, 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.<sup>12</sup> That commitment had a deadline of 2013. The 2006 IPR Side Letter

---

<sup>12</sup>WTO Working Party Report (Paragraph 1218).

had similar obligations to correct this problem.

After years of missed deadlines, Russia adopted new legislation in 2017 (in force, May 2018), that instead of fixing the collective management system in Russia, did not address key relevant issues and created even more problems. The new collective management system denies transparency to rights holders and good governance consistent with international norms, as well as best practices for CMOs as required by Russia's WTO accession obligations. The 2017 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 2017 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. Moreover, in terms of a lack of good governance, the law does not allow rights holders to control their RMOs.

The so-called "fiscal control improvements" in the new law, including regular audit reports, will not improve accountability, because the audit obligations are for reports only to the government for taxation purposes, not to rights holders. The new law creates "supervisory boards" for each of the various authors' CMOs (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 structure 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 of RMOs 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.

To develop properly functioning music broadcasting and public performance payment systems via collective management, the Government of Russia should re-visit the 2017 law to ensure that rights holders are able to control and manage their own RMOs or can effectively opt out of collective management. This change would result in fair representation characterized by direct representation of rights holders on the board in a manner that is proportionate to relevant market share and reflects commercial realities, with no conflicts of interest in the governance structures. Many models for proper governance of RMOs exist, including WIPO best practices, international rights holder group best practices, as well as U.S. and European Union (EU) existing practices. Instead, the existing regulations and state accreditations have institutionalized a system that is neither transparent, nor well governed with accountability for authors, record labels, and performers, who have no other option except for the state CMOs.

## **DEFICIENCIES IN THE RUSSIAN LEGAL REGIME**

Russia has made progress on legal reforms, but gaps remain, especially regarding effective Internet enforcement and implementation of the WIPO Internet treaties. IIPA and its members continue to note three major overarching concerns in the Civil Code, as amended: (a) a lack of clarity on numerous provisions, especially on exceptions and limitations; (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, as well as 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 civil injunctive relief that is quick and effective and applicable to all works.

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 should be expanded so that liability applies to the commercial trafficking in all variety of circumvention devices (including software) and services. In addition, commercial trafficking in circumvention devices, including by importation, should be criminalized. IIPA also recommends

improving Article 1252(5) of the Civil Code, which currently includes remedies for the seizure and destruction of materials and equipment used in infringements, by deleting the exception for the sale of materials by the state for “income,” and by parallel changes in the respective procedural codes.

## **MARKET ACCESS ISSUES**

In addition to the issues noted on copyright law and enforcement, significant market access issues exist in Russia that impact the motion picture and television industries. 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, contrary to standard international practice. Although modern-day digital transmissions mitigate the impact on film and audiovisual content, such assessments are a form of double taxation, because royalties are also subject to withholding, income, value-added, and remittance taxes.

The 1996 Law on State Support of Cinematography provided a VAT exemption for films granted a national film certificate. The government issued national film certificates only to Russian-made films. Therefore, any legal entity distributing a domestic film is exempt from VAT provided that such entity is a cinematography organization. As part of its accession to the WTO, Russia obligated itself to provide national treatment for taxes on similar products. The Government of Russia appears to violate this obligation as it is currently applying a VAT to non-Russian films and not to domestic films. Russia raised its VAT from 18 to 20 percent starting on January 1, 2019.

The Mass Media Law, as amended, prohibits non-Russians (including legal entities with foreign participants) from engaging in certain mass media activities, including broadcasting. The law limits foreign ownership to 20% of the capital of a covered entity, thus denying film producers and distributors access to the Russian market absent a joint venture partner. In 2020, a bill was submitted to the State Duma extending such requirements to online film websites, streaming platforms, and audiovisual services (AVS). The bill is now being discussed between online video services and the government as the bill reduces consumer choice and unreasonably favors domestic investors. In mid-2021, there was a suggestion (not yet formal legislation) to amend the Mass Media Law, replacing the 20% foreign ownership cap with restrictions on “foreign control” over AVS. A key concept is that foreign AVS would be allowed to “exercise ownership of a VOD service in Russia” through the special “international funds” established in “special administrative territories” in Russia. However, after the first draft was published, it received strong pushback from the market and was returned to the sponsors for rework. Further developments are expected on these draft amendments by the end of 2021.

Similar restrictions apply to over-the-top (OTT) services. Under the Law on Information, as amended on May 1, 2017, foreign ownership of audiovisual services shall be limited to 20 percent, provided that the number of Russian subscribers is less than 50 percent of that service’s total audience (i.e., the rule targets services with mostly non-Russian audiences). Foreign participation above the 20-percent threshold is subject to review and approval by the Government Commission on the coordination of ownership, management, or control concerning the audiovisual service owners.

In 2021, the Russian government began actively developing and implementing regulations for video-on-demand (VOD) services, including establishing audience measurement requirements. Although the initial reasoning behind the framework was audience research and creating an equal environment for linear and online distribution channels, the suggested amount of collected data exceeds the stated purposes. Moreover, the envisioned regulation includes a burdensome obligation to transmit said data on a twice-daily basis. In addition, some data items raise questions and concerns regarding data protection and privacy. Domestic VOD companies share these concerns and oppose implementation. Unfortunately, the government has not been responsive to expressed concerns.

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 it 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 has hindered the growth of the pay-TV industry in Russia.

Finally, market access issues in Russia affect the video game industry. As stated previously, the customs duties on the royalty value of some imported audiovisual materials rather than solely on the value of the physical

carrier medium applies to some video games. Moreover, on June 17, 2021, the State Duma adopted a law mandating foreign Information Technology (IT) companies with a daily audience over 500 thousand users to open a branch, a representative office, or an authorized legal entity in Russia, which could potentially affect the video game industry.