IP HOUSE

A Report by IP House

OVERSEAS AND OUT OF REACH

International Video Piracy and U.S. Options to Combat It

September 2024

Commissioned by Digital Citizens Alliance

Table of Contents

Foreword by the Digital Citizens Alliance

As a non-profit dedicated to educating Internet users about—and protecting them from—online risks, the Digital Citizens Alliance has published dozens of investigative reports over the last twelve years. We often raise issues that haven't yet hit the mainstream, guided by the mantra, "We can't protect against what we don't know." While the subject matter of these reports varies widely, they generally share three key attributes.

> ***First,*** *Digital Citizens, often in partnership with leading experts in the field, conducts research and issues reports on the vast array of ways that criminals and other bad actors scheme to rip off and otherwise endanger Internet users.*
>
> ***Second,*** *these reports highlight the legitimate businesses that, by failing to police their platforms and services adequately, have created an environment that enables scammers to thrive.*
>
> ***Third,*** *these reports provide a roadmap for how private entities and governments can do better, suggesting specific technologically feasible and economically reasonable steps to counter the threats that scammers pose.*

While the full list of reports can be found on our website, a few recent examples represent the range of revelations in the Digital Citizens' reports include[1]:

- Scammers dangling the prospect of acquiring online hard-to-get weight loss drugs such as Ozempic to steal consumers' money while platforms turn a blind eye.
- Illegal products, including opioids, steroids, and malware, are being promoted on popular social media sites like YouTube, Instagram, and Facebook despite having the problem repeatedly brought to the attention of these platforms.
- Jihadists leveraging social media platforms such as Google+ and Facebook to recruit new members, spread propaganda, and publish gruesome and violent content.

While Digital Citizens has uncovered and warned of many online dangers, it has repeatedly turned its attention to global piracy: the organized theft and illegal distribution of copyrighted content. This research started when Digital Citizens found that the piracy websites systematically targeted their users for harm.

Perhaps that should not have been surprising. Piracy is the original online grift; theft is the very premise of criminal piracy websites and apps. The criminal organizations that engage in piracy steal movies and television shows, which have taken many people massive amounts of time, effort, and talent to create. And, as our studies have shown, piracy operators annually make billions of dollars through content theft and by exposing their customers to malware and credit card fraud.

[1] https://www.digitalcitizensalliance.org/get-informed/digital-citizens-investigative-reports/

Digital Citizens published *Good Money Gone Bad* a decade ago, revealing that, in 2014, just a sampling of piracy websites raked in nearly a quarter of a billion dollars annually in ad revenue. The report showed piracy websites could profit to this extent due to a lack of controls that online advertisers and ad networks could have instituted.[2]

Based on what was learned from that first report, it was obvious there was a need to dig deeper. Since then, reports have looked at the staggering profitability—measuring in the tens or even hundreds of millions—of various forms of professional piracy. These include "cyberlockers" (where stolen copyrighted works are stored and accessed)[3] and "IPTV services" (illicit cable-like systems offering live programming from around the world).[4]

Digital Citizens' focus has been piracy's harm to individuals, small businesses, corporations, and even governments. For example, Digital Citizens' reports have spotlighted how criminal piracy organizations often use the bait of free content to trick their users into downloading dangerous malware that can expose them to identity theft and jeopardize their cyber- and financial security. The victims rarely know how—or even that—they've been infected and that hackers can now capture their every keystroke. Also, unsurprisingly, users who provide these criminal organizations with their credit cards can find that their trust was misplaced, with their cards used to make unauthorized purchases. [5]

Global piracy has quietly become a massive $2 billion-plus illegal industry that works in concert with other criminal entities, creating a substantial risk to Americans. Yet the technology platforms that enable these criminals to find and fleece U.S. victims don't care enough to stop assisting them, and many consumers still don't know that the piracy sites they visit are designed to do them harm. Most importantly, the operators are largely out of the reach of U.S. civil and criminal enforcement.

It's said that the definition of insanity is doing the same thing repeatedly and expecting a different result. It's time to consider other options to combat the dangers of an industry that preys on Americans from the comforts of overseas villas.

One of the most potentially promising ideas to combat piracy is called "site-blocking," a procedure that is used in more than 50 countries but not yet tried in the piracy context in the United States.[6] Site-blocking usually involves a rigorous court process to identify websites that deal exclusively in illegal products and services (such as piracy), but are out of reach of domestic civil or criminal enforcement. Once the website is found to be infringing, an order is served upon relevant intermediaries, such as Internet Service Providers (ISPs), to stop these criminal websites from being readily accessible in that country.

Site-blocking has powerful advantages—overcoming jurisdictional obstacles and allowing courts to issue effective, enforceable orders that empower innocent local intermediaries to stop their networks and infrastructure from being used by foreign actors for harm, while also providing due process and transparency. The intermediaries are protected from liability for actions taken pursuant to these court orders, keeping the focus properly on the foreign websites responsible for the harm.

---

[2] https://www.marketingdive.com/news/piracy-sites-raked-in-227m-in-ad-revenue-in-2013/228793/
[3] https://variety.com/2014/biz/news/credit-card-companies-enable-piracy-study-claims-1201308836/
[4] https://www.forbes.com/sites/augustinefou/2020/09/02/ad-supported-piracy-is-thriving-thanks-to-programmatic-ad-tech/
[5] https://www.wpxi.com/news/local/report-finds-12-ads-piracy-websites-involve-malware-target-users/H5WZ75KY6BDPPB7FUQOWFW6L4Q/
[6] https://www.americanactionforum.org/insight/primer-site-blocking-and-online-piracy

A decade ago, there was a heated policy debate in the United States over an anti-piracy proposal to create several remedies similar to site-blocking—but one that went much further and included non-judicial processes and addressed a range of online harms beyond digital piracy. This proposal died under the weight of claims that such a process would "break the Internet" and result in users losing access to their favorite websites.

The debate was largely theoretical because site-blocking didn't exist in many countries at that point. Today, however, with so many countries having adopted variations of site-blocking, there is data that be evaluated to determine if site-blocking is effective and whether the claims of "breaking the Internet" or causing other harmful unintended consequences are valid.

To conduct that evaluation, Digital Citizens asked experts in the field to investigate. IP House, with profound knowledge of precisely how organized piracy operates, was commissioned to produce a report that would describe, in non-technical terms, how organized piracy works, looking at both video-on-demand (VOD) and live-streaming piracy. It was also asked to examine how widespread piracy is, who the pirates are, and what harm they cause. Finally, IP House was tasked with looking at the body of evidence about site-blocking, including its effectiveness in combating piracy and any harmful consequences it has caused.

The report that follows is the result of IP House's research. Given IP House's compelling findings that site-blocking is successful, proportionate, and does not injure Internet safety, it is time for policymakers to consider adopting site-blocking as the most effective strategy to deter overseas criminals from using pirated content to target and harm U.S. citizens.

The other option is to do nothing and enable overseas criminal operators to continue to target Americans for harm and to foil U.S. law enforcement's efforts to protect consumers, small businesses, and corporations—all while these overseas criminal operators enjoying their riches.

To go that route would truly be the definition of insanity.

Executive Summary

As experts in the field of intellectual property theft and methods to combat it, IP House was commissioned to explain how video piracy—the international illegal distribution of movies and television shows—works. As part of that report, we were asked to determine how popular video piracy is and to analyze who the piracy are and the harm they cause. Finally, we have been asked to assess the benefits and drawbacks of "site-blocking," which many governments and courts around the world have implemented over the last decade to protect consumers and combat video piracy.

While large-scale online video piracy dates back only twenty years, the problem of intellectual property theft has a much longer timeline.[7] For as long as brilliant minds have come up with new inventions, works of art, trade secrets, or iconic symbols, unscrupulous operators have tried to profit off the intellectual property of others. Governments have tried to discourage these types of theft for centuries, enacting new laws when the old ones proved inadequate.

Almost as soon as pictures were put in motion in the United States, operators seized the opportunity to make copies and sell them without permission. Thomas Edison tried to stop a rival from making copies of his movies by filing the country's first copyright infringement case in 1903.[8] As the generations passed, the formats have changed, but the process of stealing creators' content has followed a time-proven principle: it's easy to make a profit when you sell the work of others and keep the income.

While digital piracy was once viewed as an activity of amateurs, the last two decades have spurred an exponential growth of organized large-scale content theft conducted by savvy criminal enterprises operating from around the globe. Content theft is now a big business, generating an estimated $2.3 billion yearly from the theft of movies and TV shows.[9]

Over 15 years ago, the Rand Corporation found that organized crime syndicates count on piracy as a revenue stream to augment their profits from drug smuggling, counterfeiting, and racketeering.[10] But even putting aside the capacity of piracy to support other organized crime activities, video piracy's harms are widespread. In the digital era, the creator of the infringed work is no longer the sole victim. Instead, the harms of pirated content include Internet users, businesses, and governments.

Cyber-criminals have been quick to recognize that the temptation of instant, online access to cheap or free movies and TV shows makes piracy an excellent mechanism to deliver dangerous malware to Internet users, subjecting them to the risk of ransomware and identity theft, along with other threats.[11] Subscribers to piracy streaming sites have been shown to fall victim to credit card fraud disproportionally.[12] And governments lose hundreds of millions of dollars in tax revenues due to content piracy: Pirates typically don't pay taxes on their ill-gotten gains.[13]

7 https://www.hudson.org/intellectual-property/what-online-piracy-data-tells-us-about-copyright-policymaking
8 https://unwritten-record.blogs.archives.gov/2020/02/12/pioneers-of-movie-piracy-and-the-expansion-of-copyright-law/
9 https://piracymonitor.org/dca-ad-supported-pirate-streaming-2021-08/
10 https://www.rand.org/pubs/research_briefs/RB9417.html
11 https://www.yahoo.com/news/report-finds-12-percent-ads-202717500.html
12 https://www.mediapost.com/publications/article/386562/piracy-subscription-purchases-often-lead-to-additi.html
13 https://www.uschamber.com/assets/documents/Digital_Video_Piracy_June_2019.pdf

These piracy operators are often talented imitators. They create professional-looking services that entice users to access a virtual universe of content at a low price—typically $10 to $15 a month—or for free if users are willing to view advertising. Because these operators don't pay the main cost borne by all legitimate streaming services—licensing movies and TV shows—these illicit services enjoy profit margins of up to 85 percent.[14]

Typically, these illicit actors operate under the radar to avoid attention. But some can't help but flaunt their wealth. Kim Schmitz began his career as a hacker and peddler of stolen phone calling cards in Germany before proclaiming himself "Kim Dotcom" and becoming the world's most flamboyant supplier of pirated content. At the time of his 2012 arrest in New Zealand, police seized eighteen luxury cars, works of art, and $175 million in assets.[15] While he claimed he had no control over what his users uploaded to his site, his case underscores not only the riches piracy can bring but also the challenge of bringing these operators to justice: It has taken a dozen years for the New Zealand government to finally order him extradited to the United States to face trial.

Whether they choose to operate in the shadows or revel in their notoriety, piracy moguls have much in common. They steal content. They build multi-million-dollar technical networks to handle immense traffic. They specifically target wealthy countries with a high demand for content—focusing especially on movie and TV lovers in the United States.

And they have one more critical commonality: for the most part, they operate outside the reach of U.S. law. Since Kim Dotcom's arrest, piracy operators have tended to establish their operations in regions such as Southeast Asia and remote corners of Eastern Europe that have less strict laws against piracy, are lax in their enforcement, are unwilling to extradite these criminals to the United States, or all three.[16]

Domestic piracy in the United States remains a problem. Nevertheless, there are civil and criminal laws that can be used to reach the perpetrators when they can be located within U.S. jurisdiction. And Congress has given federal prosecutors more tools to go after domestic piracy operators by making piracy streaming a felony. Piracy kingpins operating overseas, by contrast, can still act with relative impunity, resting comfortably in the knowledge that it is highly unlikely they'll ever be held accountable for their criminal actions.

Over a decade ago, U.S. policymakers grappled with the challenge of overseas piracy organizations. One of the proposed solutions at the time was called "site-blocking." At a high level, site-blocking impedes the operator of a banned website from reaching consumers in a particular locality.

Site-blocking was not enacted in the United States at the time. However, since 2011, when the United Kingdom became the first country to allow rights holders to apply to courts for blocking orders,[17] many other countries have established procedures for judicial or administrative site-blocking injunctions against commercial piracy sites. Such countries include much of the European Union, as well as Canada, Australia, India, Brazil, South Korea, and Singapore.

[14] https://dtv.nagra.com/pirate-subscription-services-now-billion-dollar-us-industry-joint-digital-citizens-alliance-nagra
[15] https://www.theguardian.com/technology/2012/jan/20/megaupload-shutdown-guns-cars-cash-seized
[16] https://asiaiplaw.com/section/in-depth/enforcement-amid-digital-piracy-and-organized-crime-in-vietnam
[17] https://www.bbc.com/news/technology-14322957

IP House has been asked to review the evidence amassed about site-blocking in those countries. This includes whether it is effective in diminishing piracy and in promoting legitimate distribution of content.

The evidence we've reviewed shows significant results. Three separate studies—focused on the United Kingdom, Portugal, and Australia—found that when sites were blocked, traffic decreased to those sites. The decrease was substantial; traffic decreased by 89 percent in the United Kingdom, 70 percent in Portugal, and 69 percent in Australia.[18,19,20]

On the other side of the equation, site-blocking remedies appear to help build secure and trustworthy digital markets where more people use legitimate streaming services. A recent study found that site-blocking in India resulted in a one-year 8 percent increase in lawful streaming in 2019 and boosted lawful streaming by 5 percent in Brazil in 2021.[21]

IP House was also asked to review whether any harm has been caused by site-blocking in the jurisdictions that have adopted this remedy. Our review of the experiences of these countries suggests that the harms that some originally feared have not come to pass. Specifically, there has been no discernible harm done to the workings of the Internet, no impact on legitimate websites, and no impingement on legitimate speech.

[18] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2766795
[9] https://www.incoproip.com/wp-content/uploads/2020/02/Site-Blocking-and-Piracy-Landscape-in-Portugal-May-2017.pdf
[20] https://creativecontentaustralia.org.au/wp-content/uploads/2021/03/INCOPROAustralianSiteBlockingEfficacyReport-KeyFindingsJuly2018FINAL.pdf
[21] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723522

International Content Piracy: How it Works

Simply put, online piracy involves distributing and making available copyrighted content digitally, typically via websites or apps, without the permission of the rights holder. According to numerous surveys, at least 1 in 3 Americans say they have visited a piracy website or app in the last year.[22] It's fair to surmise that others have done so as well, without realizing it was an illicit site because of its slick features and layout.

Almost any type of work that can be distributed digitally can be pirated. Those rights holders affected by piracy include movie studios, record labels, independent creators, book publishers, gaming companies, and software publishers.

Image 1 (right) from MUSO, a piracy-tracking data company, details visits to piracy sites by category.

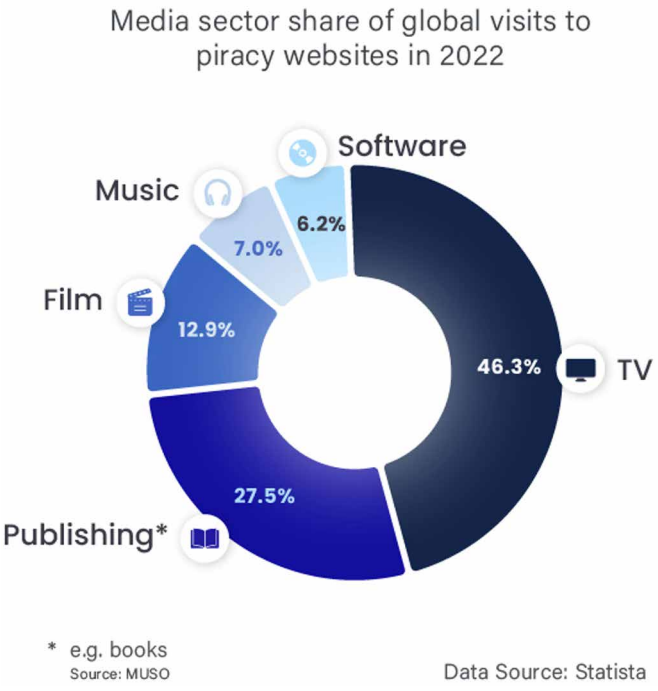
This report focuses on the business models for video piracy. It's a diversified and dynamic industry, but generally can be broken down into two types:

- Pirated *recorded* content (movies and TV shows) through Video-on-Demand (VOD) Piracy Services.
- Pirated *live* content (programming, including sports, special events, and other live-streaming content) through illicit streaming services.

Video-on-Demand (VOD) Piracy Services

VOD piracy services provide access to a catalog of recorded movies and TV shows through an Internet connection. In many respects, they mirror how legitimate services operate. Like on Apple TV+ or Freevee, subscribers generally pay a monthly or annual fee and/or agree to view advertising in return for free or reduced-price service. In return, subscribers can access a vast collection of recorded content that can be streamed to a computer, tablet, phone, or TV.

Image 1: The Media Industries Most Affected by Piracy



[22] https://piracymonitor.org/dca-78-risk-of-fraud-if-you-used-a-credit-card-to-subscribe-to-a-piracy-service/

Surveys have shown that Internet users are sometimes duped into thinking these websites and apps are legitimate. The reason is simple: these VOD piracy apps and websites can look almost identical to legitimate streaming services, with professional, user-friendly interfaces, including many features found in legitimate services. These features include links to trailers, IMDb ratings, synopses, and cover art. Users can quickly search for content, click on their desired selection, and start watching. Furthermore, many apps allow users to download content for offline viewing.

Piracy operators go to great lengths to mimic legitimate services. The following images compare how the legitimate streaming website *Paramount+* (Image 2) looks compared to an illegal VOD piracy website called *123 Movies*. (Image 3)

IMAGE 2: *Paramount+*

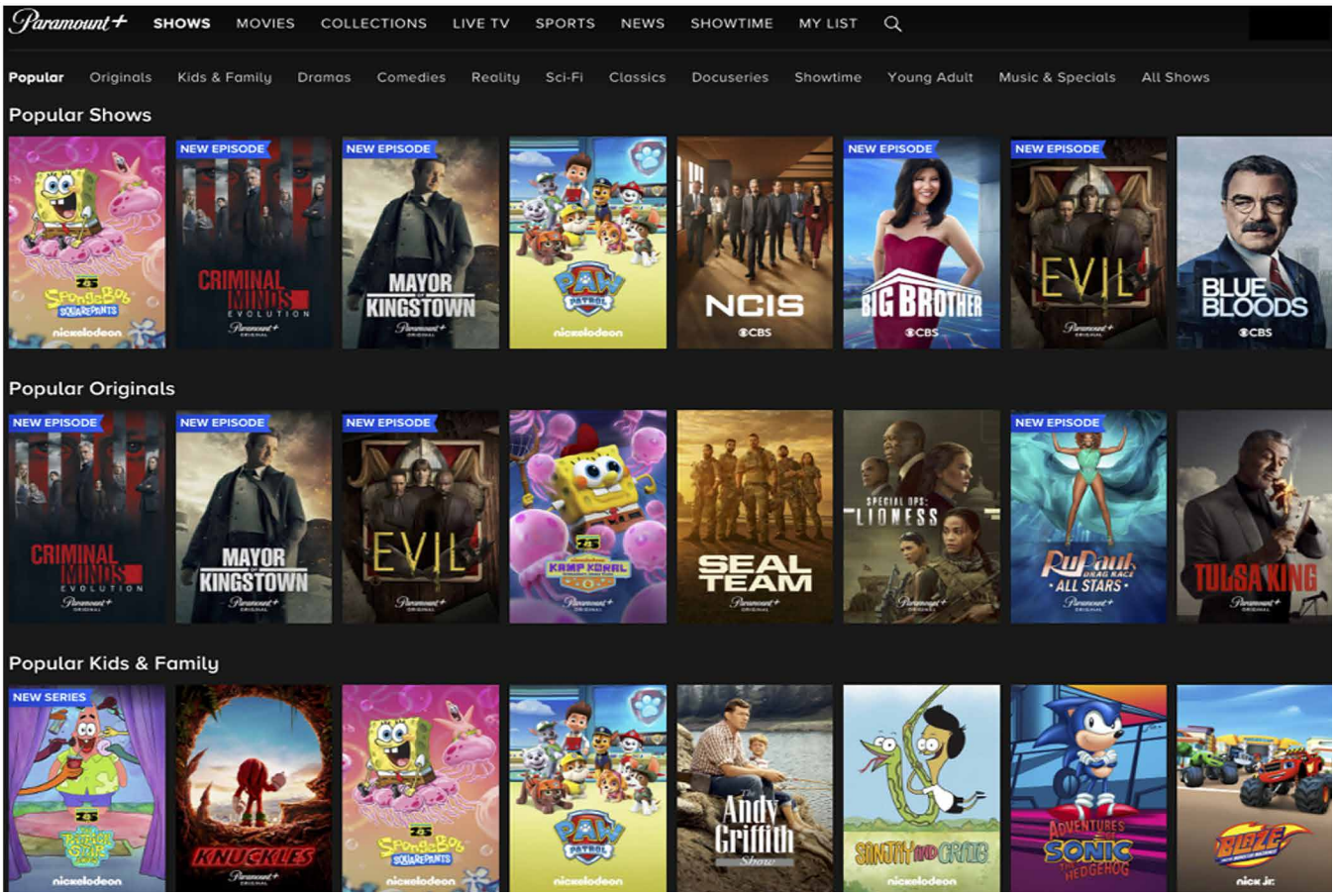
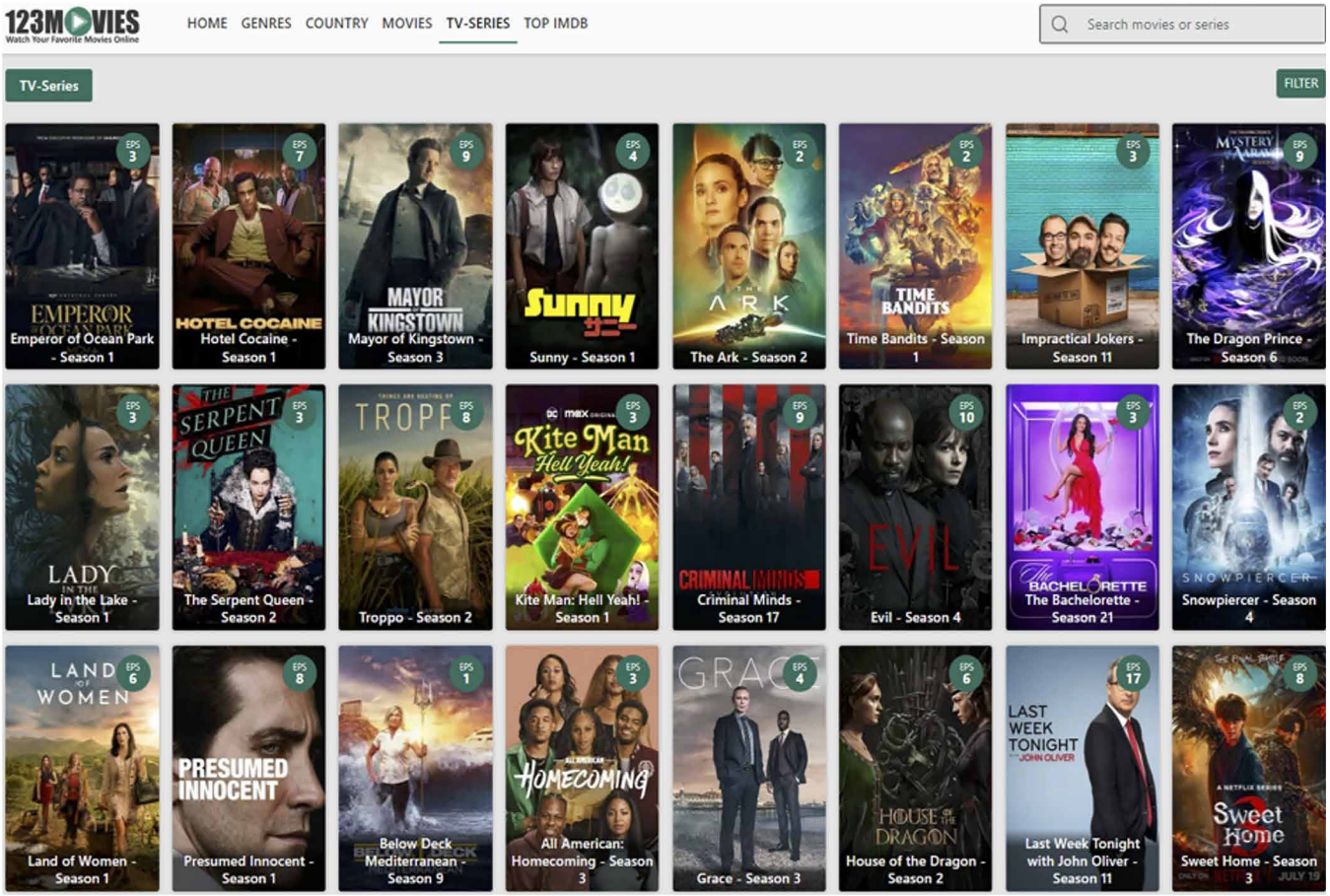


IMAGE 3: VOD Piracy Website *123movies*



VOD piracy services like *123movies* typically provide access to tens of thousands of movies and TV episodes, including content that is only legitimately available on specific streaming services. The content offered is often in the form of high-quality streams like those provided by legitimate services.

These piracy services can offer immediate access to movies that are currently in theaters when no legitimate service is permitted to make them available. For example, below is a screenshot from the piracy app called *Flix Vision*. Clicking on the image for *Deadpool & Wolverine* in the top left corner (Image 4) calls up the movie, as seen in the screenshot immediately below (Image 5). The movie was available on *Flix Vision* in late July 2024, contemporaneous with the film's theatrical release and long before it would be available on any legitimate service. With technological advances in recent years, even movies illegally recorded in movie theaters are rarely shaky or blurry.

IMAGE 4: ***Flix Vision***

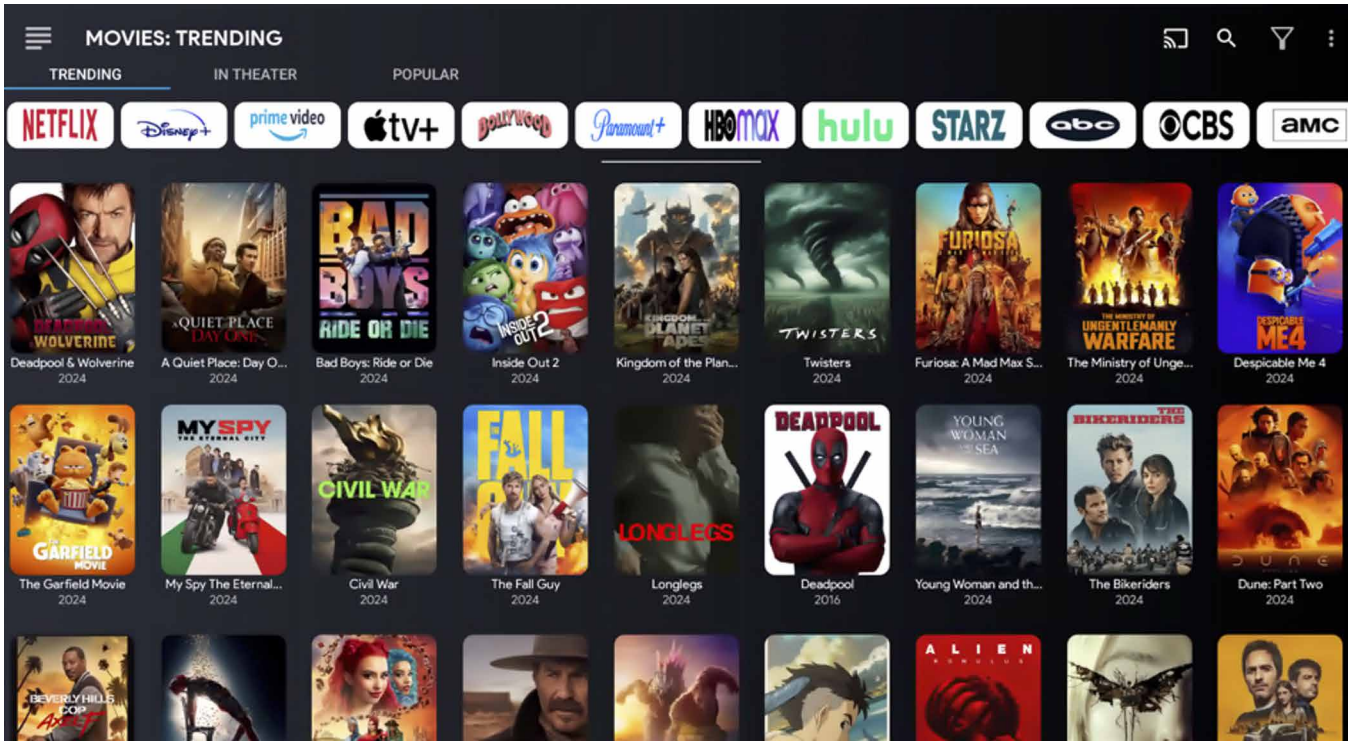
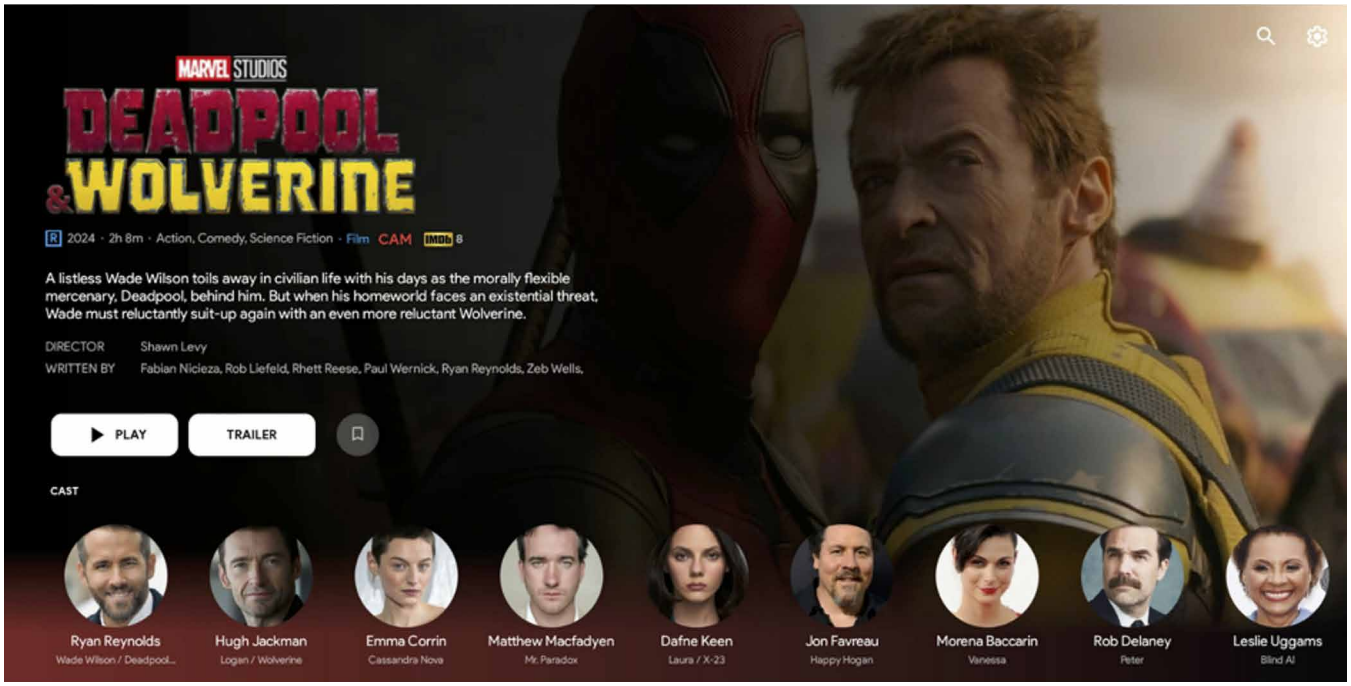


IMAGE 5: ***Flix Vision***



These VOD piracy services can make available any content from anywhere in the world because they pay nothing for the movies and TV shows they offer. Legitimate services, by contrast, must negotiate licensing agreements with the owners of the content that allow them to stream specific content only in specific jurisdictions.

Advertising-supported VOD piracy apps and websites typically don't have any (or very low) subscription fees but instead bombard the user with advertising—often containing hidden malware, as discussed in detail later in the report.[23]

The players that drive the VOD piracy market are generally sophisticated criminals who have created piracy syndicates, structured like multinational enterprises, requiring employees with a range of talents to operate savvy and technically robust multi-million-dollar operations. Piracy VOD services employ skilled tech teams that design attractive websites and apps, marketing and customer support teams to attract and retain customers, and security teams to implement countermeasures to protect the site from being shut down by authorities.

How VOD Piracy Services Obtain and Store Content.

VOD piracy services acquire content in a combination of ways. Sometimes, they make an illegal copy directly from the source by, for example, downloading or recording content from legitimate streaming services using screen recording or digital rights management circumvention software. They also obtain physical copies (DVDs/Blu-rays) and convert them to digital formats. If their users accept the marginally lower quality in exchange for movies not available through any legitimate means, they can use recordings created illegally from within movie theaters.

Some VOD piracy organizations prefer to rely on the collections of others, downloading from what are called "torrent sites" content that other people previously uploaded or outsourcing completely the task of accumulating libraries by paying illegal content suppliers to gain access to their content library.

One notorious content supplier is *VidSrc*, a source used by dozens of VOD piracy websites. The supplier offers over 76,000 movies, 15,000 TV series, and almost 370,000 TV show episodes. It offers high-quality streams and caters to English-speaking audiences. The content comes replete with advertising, and its operators make it free for any would-be VOD piracy website owner to use. It also offers an option to stream content without advertising for a fee. *VidSrc* refuses to comply with copyright owners' demands under U.S. law to remove the illegal content.[24] It received over 4.2 million visits in 3 months, of which over 30 percent came from the United States. The operators of this library are suspected to be in Vietnam. The *VidSrc* brand is so well-known that imitators have established services of their own using similar names; one such service was recently the subject of a takedown by the Hanoi Police, but the original *VidSrc* is still thriving.

[23] https://www.mynewstouse.com/stories/avoid-malicious-online-advertisements,36719

[24] Digital Millennium Copyright Act (DMCA) notices, 17 U.S.C. 512(c)(3)

VOD piracy operators often utilize the hosting services of so-called "cyberlockers" to store their content. Cyberlockers are online storage facilities that turn a blind eye to the nature of what is uploaded onto their platform and often profit from constant downloads of popular material—like copyrighted content.

India-based *Doodstream* is the largest video hosting site (cyberlocker) in the world, with 898 million visits in the first quarter of 2024, a large percentage of which originated from the United States. *Doodstream* is also used as a content source for more than 660 popular VOD piracy services (many of which target U.S. consumers).[25] The VOD piracy service embeds the *Doodstream* link on its website or app, and with a single click, users can load the desired video of choice. As of the publication of this report, the site has been blocked in France and is currently in litigation in the High Court of Delhi, but is still accessible from the United States.[26]

Piracy operators utilize sophisticated strategies to stay under the radar of law enforcement. Because websites that receive many visitors can attract the attention of copyright enforcement organizations, these syndicates often run multiple websites or apps using a variety of well-known "piracy brands," such as *Fmovies* or *123Movies*. These sites appear to be less popular individually, but combined, they can attract millions of monthly visits. Like a grocery store chain that operates under different names in different states, the common ownership is not transparent.

As mentioned, these VOD enterprises typically operate from abroad and across multiple jurisdictions, but they target consumers in countries with a high demand for pirated content, such as the United States. The countries from which they operate often have less strict copyright laws—or they don't enforce them—making it difficult or impossible to catch the infringers and bring them to justice.

Live-Streaming Piracy

VOD piracy services make up only part of the online piracy puzzle. A growing component of international piracy consists of live-streaming piracy services that let viewers watch real-time programming and pay-per-view ("PPV") events using illicit websites and apps.

There are two basic types of live piracy streaming services: *subscription* services accessible to subscribers only, generally for a fee, and *streaming portals*, websites available to anyone and typically supported by ads.

Piracy subscription services (sometimes called "illicit IPTV services"—Internet Protocol (IP) TV services) are digital streaming services delivered to customers over the Internet through an app, without the need for a cable box or satellite dish. Viewers can watch the programming on a computer, TV, or mobile device. Subscribers pay a subscription fee to the piracy operators—typically between $10 and $15 a month.[27] They can offer their services at a fraction of the cost of their legitimate counterparts because they pay nothing for the programming.

[25] https://www.iipa.org/files/uploads/2023/01/2023SPECIAL301FILING_WEBSITE-1.pdf

[26] Warner Bros. Entertainment Inc. v. Doodstream.com, Case No. CS(COMM) 234/2024

[27] https://www.cdsaonline.org/2021/03/30/me-journal-an-insiders-look-at-the-billion-dollar-pirate-subscription-iptv-business/

IMAGE 6: Price Sheet for a Popular Illicit IPTV Service

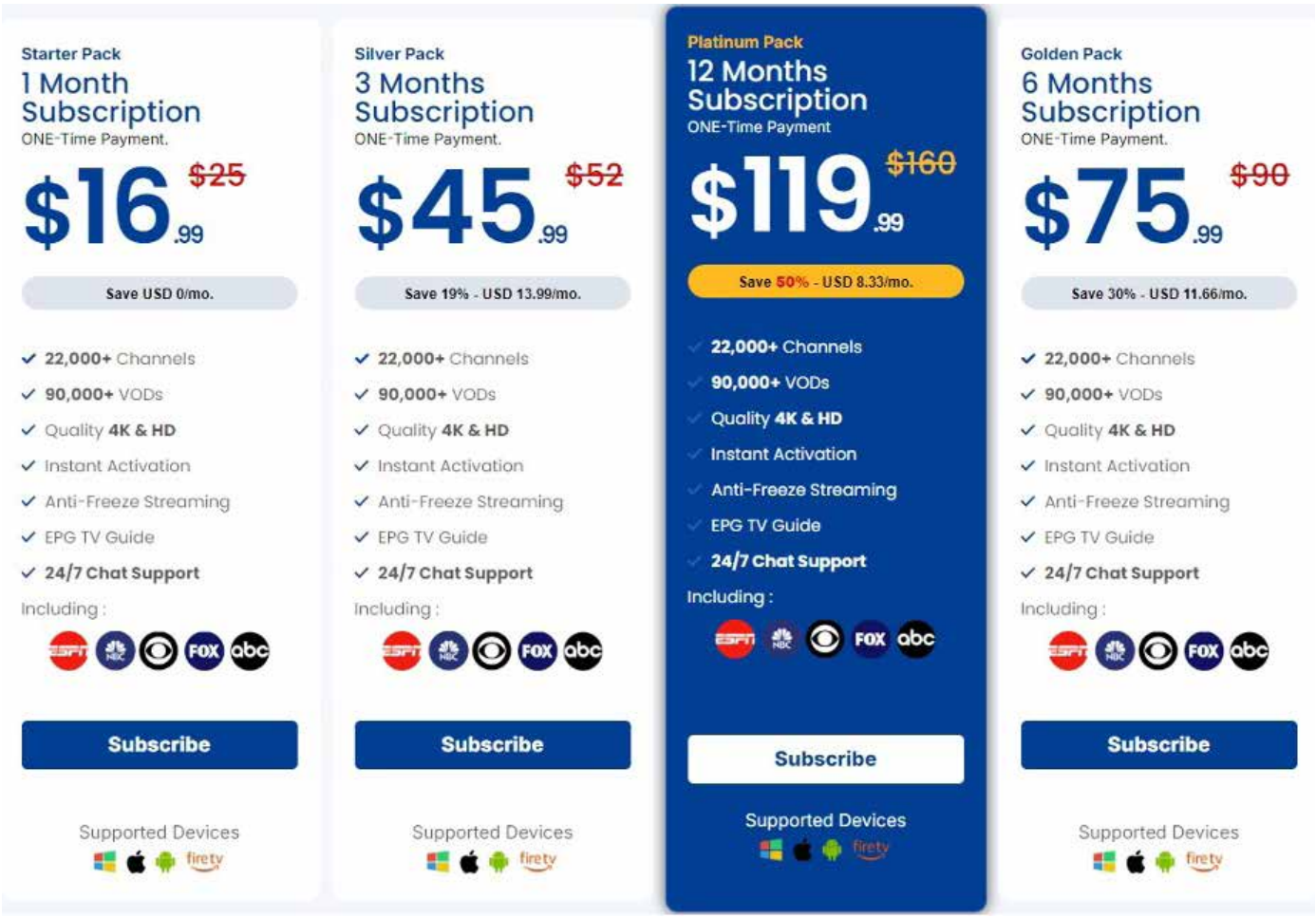


Image 6 is the price sheet for a popular illicit IPTV service, offering over 22,000 channels and 90,000 VODs for only $119 per year.

For their fee, subscribers gain access to live programming from the United States and often from all over the world. This usually includes not only basic broadcast and cable channels but also premium channels like HBO and Showtime. In addition, for the same or sometimes an additional fee, users gain access to pay-per-view special events, like UFC fights.

The images below show the legitimate streaming service ESPN+ (Image 7) next to an illicit one (Image 8); they appear almost indistinguishable.

IMAGE 7: Legitimate Streaming Service *ESPN+*

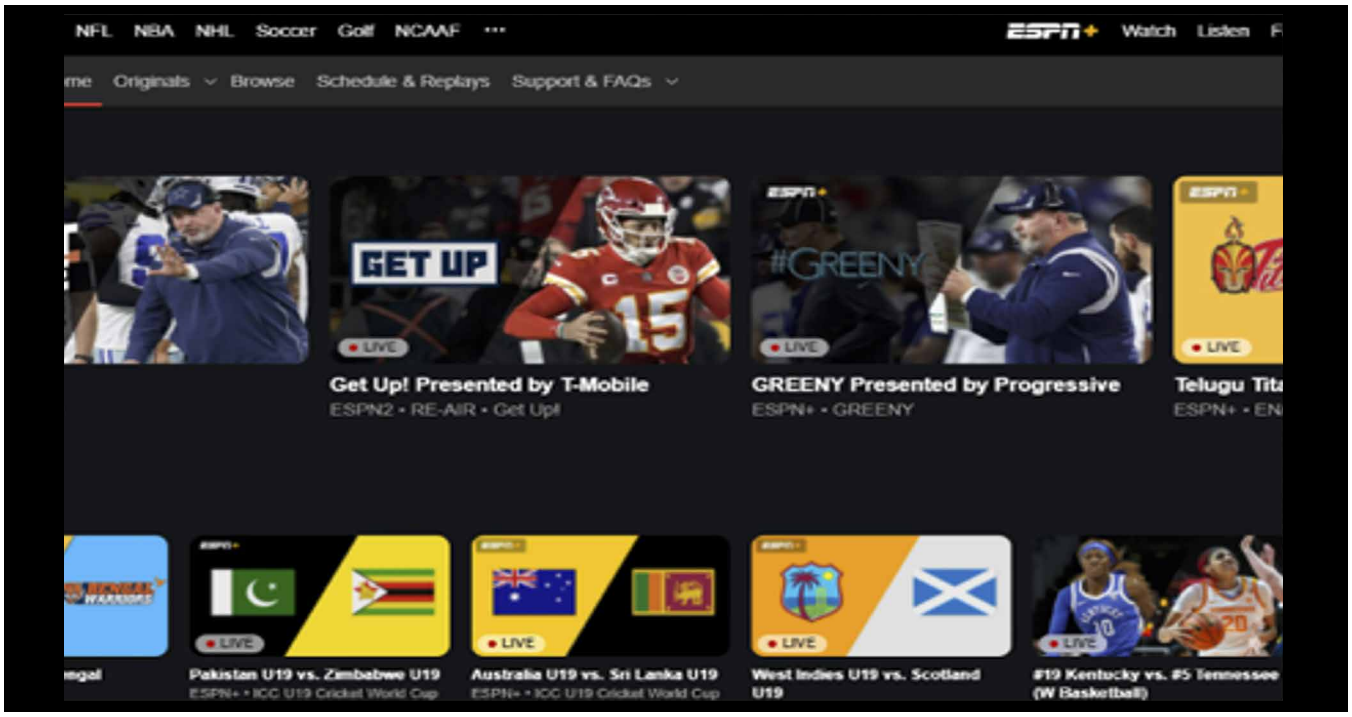
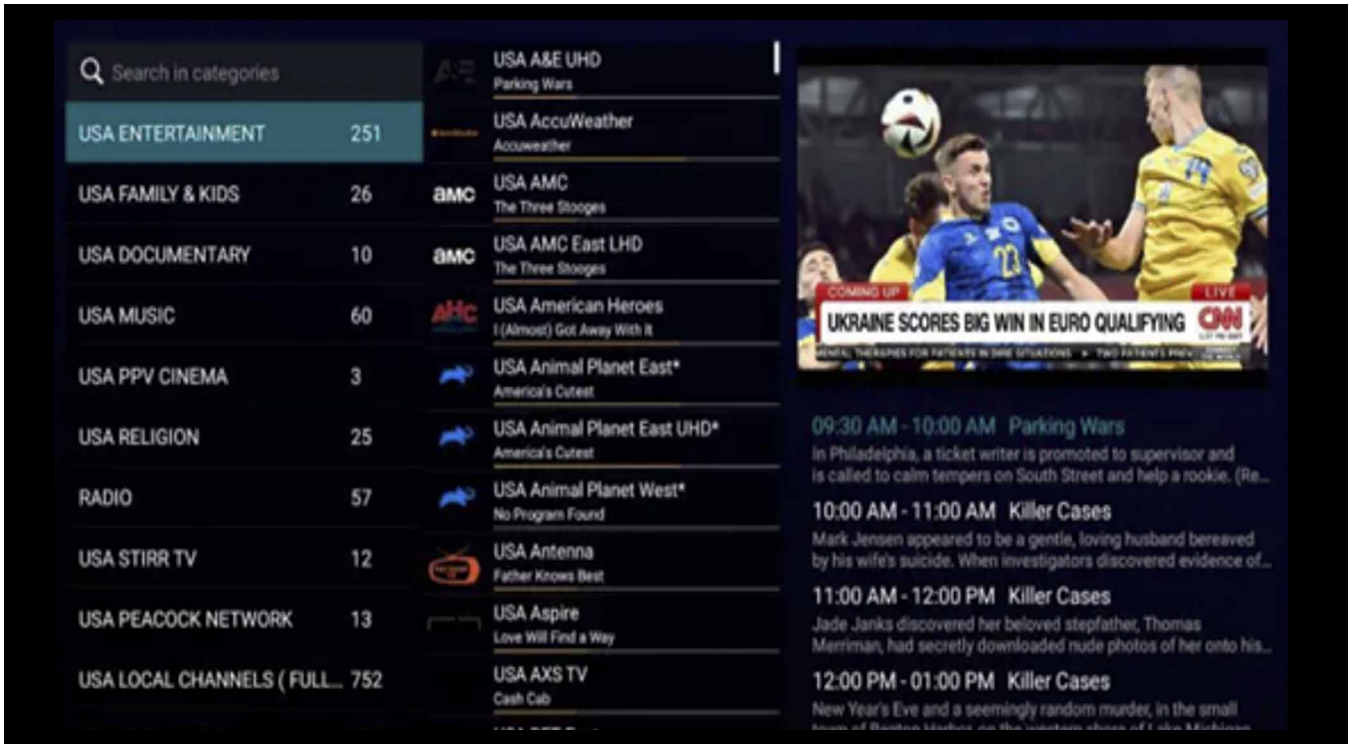


IMAGE 8: Illicit Streaming Service



Because IPTV services have customers to please, the operators require a strong technical infrastructure to operate.[28] They must invest in high-capacity servers and bandwidth to offer a broad range of channels and PPV events to a large subscriber base. They also require special software that allows them to operate like a cable company.

Oftentimes, the operators of the public-facing IPTV services outsource the technical aspects of the business to others, paying them a hefty percentage of the subscription fees for that service and freeing them to focus on recruiting new customers. These wholesalers generally don't have a consumer-facing presence, making it harder for content owners or law enforcement to identify or bring legal action against them. In addition, some IPTV services operate like multi-level marketing companies, recruiting resellers and taking a slice of their revenue. This creates a chain where many people make money (except the content creators and tax authorities).[29]

Globe IPTV is one particularly infamous illicit IPTV wholesaler. The Office of the U.S. Trade Representative described it in 2022 as "one of the largest wholesalers of content to piracy services globally," and rights holders reported that "attempts to engage with the site, including through notice-and-takedown requests, have been ignored."[30] Investigations by the Premier League determined that *Globe IPTV* is operated out of Lebanon.[31]

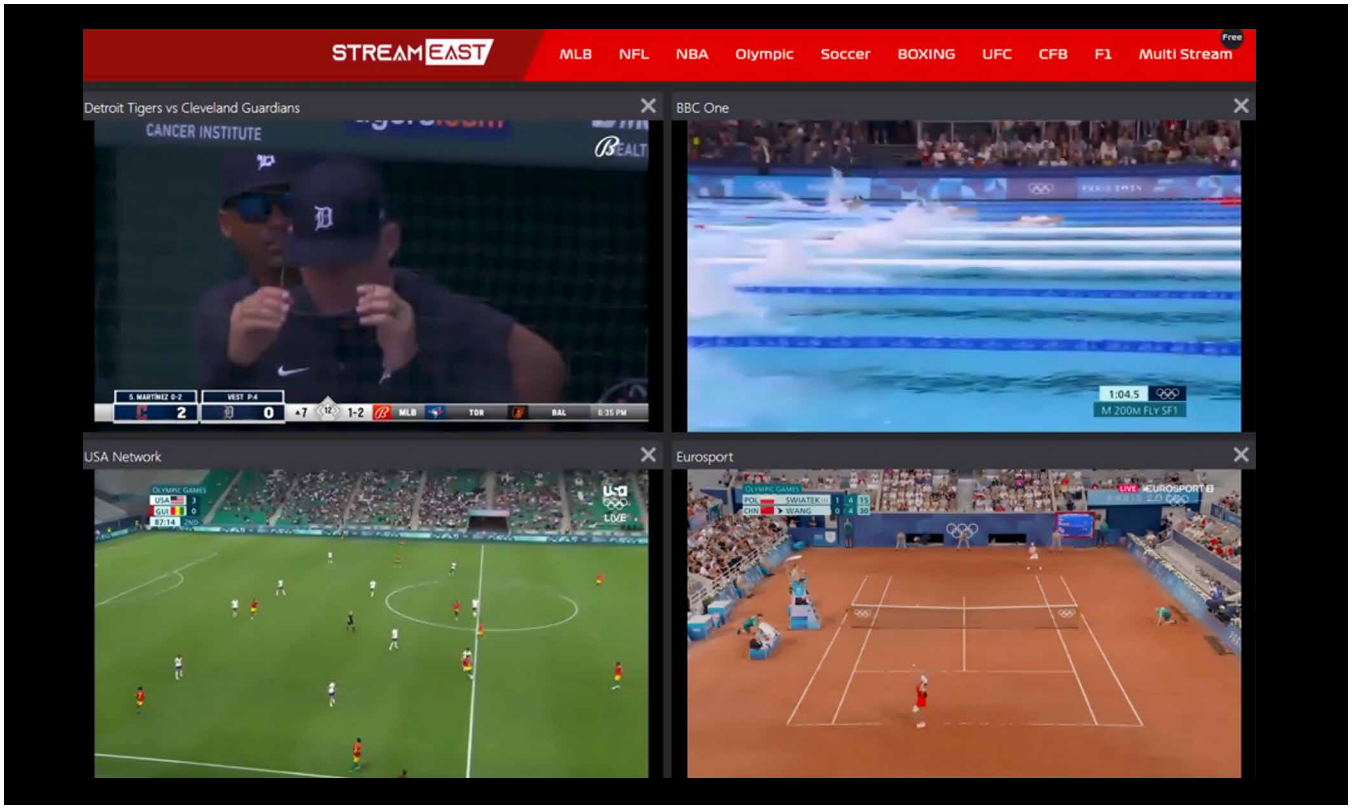
IPTV services, or their wholesalers, procure live streams from various sources, with the more established services ensuring that they have multiple sources for programming in case one becomes unavailable. One of the ways the operators obtain the programming is referred to as "Rip and Restream," whereby content is illegally obtained directly from legitimate cable boxes or streaming service subscriptions, essentially stealing ("ripping") the signal and sharing ("restreaming") it with their customers. A streaming piracy operator, with the assistance of collaborators, may take out many cable subscriptions under different names and addresses, ripping different channels from each. Another way they obtain the content is by simply stealing it from other piracy operators, using automated tools to lift links to live streams from other, equally illegal, IPTV services and streaming portals.

The second type of live-streaming piracy services are websites, sometimes called "streaming portals," that are available to anyone and are generally ad-supported. One example is the popular streaming portal *StreamEast*. It received almost 60 million visits between April and June of 2024, of which more than 80 percent originated from the United States. It is currently the 675th most popular website in the United States. *StreamEast* boasts an interface that allows consumers to access unauthorized streams of all major sports leagues, including the MLB, NBA, WNBA, NHL, NFL, CFB, F1, boxing, and UFC. The website requires its users to watch numerous ads before they can watch a game.

As a demonstration of the persistence of well-known piracy brands like *StreamEast* (Image 9), recent efforts by law enforcement to shut down the sites by seizing the associated domain names resulted only in temporary shutdowns of the service, whose operators quickly pivoted to alternative domains they had procured in advance.[32]

[28] https://damonmccoy.com/papers/IPTV.pdf
[29] https://knowledge.everc.com/blog/illicit-iptv-small-screen-big-risks
[30] https://ustr.gov/sites/default/files/2023-01/2022%20Notorious%20Markets%20List%20(final).pdf
[31] https://www.regulations.gov/comment/USTR-2022-0010-0021 and https://www.regulations.gov/comment/USTR-2023-0009-0011
[32] https://torrentfreak.com/feds-seize-domain-names-of-sports-streaming-site-streameast-240819/

IMAGE 9: *StreamEast*



Some streaming portals use affiliate marketing, providing a finder's fee or kickback to entice users to click on a link or banner for a product. Some Virtual Private Network ("VPN") services appear to intentionally use illegal streaming portals to market their products. Piracy streaming portals often try to use scare tactics to frighten users to click on ads for VPNs, making money per click or when the user signs up for the VPN's service. Ironically, the ads sometimes emphasize the illegal nature of the site and the danger of criminal or civil liability to drive the user to purchase the VPN.

Streaming portals also make money from advertising legitimate products. Advertisers often don't know that their ads are shown on piracy services because they pay an advertising network to distribute them. Many legitimate advertisers have banded together through an organization called the Trustworthy Accountability Group, or TAG, to stop ads from appearing on piracy and other sites that are not "brand-safe"; their efforts appear to be working and resulted in a significant reduction of ads for well-known brands on streaming portals and other ad-supported piracy sites.[33]

Like large-scale VOD piracy operators, operators of IPTV services and streaming portals generally operate from countries that make enforcement difficult or impossible due to a lack of copyright laws or a lax approach to enforcing them.

[33] https://www.tagtoday.net/news/torrentfreak-pirate-sites-with-malicious-ads-face-restrictions-under-new-initiative

Piracy by the Numbers

As a part of this report, IP House was asked to review the data regarding how widespread and profitable piracy is. We appreciate the relevance of this assessment: if VOD and live-streaming piracy are relatively rare, the issue may not warrant much attention from policymakers and law enforcement. If, by contrast, piracy is more prevalent, it may require new laws and additional resources devoted to combating it.

In general, there have been three types of reports about piracy. Some reflect how often piracy websites are visited; some analyze consumer surveys conducted about piracy; and the third estimates the profitability of piracy.

We look at the most current and comprehensive of those studies in turn.

Visits to Piracy Sites

The available published data suggest that piracy is significant, with no evidence that it is trending downward. One of the most comprehensive reports was issued in 2022 by MUSO, a well-known antipiracy firm. Their report, *The Film and TV Piracy Report 2022*, analyzed how often piracy websites are visited.[34]

The report found that there were approximately 215 billion visits to piracy websites worldwide in 2022 for all media sectors. MUSO found that video piracy was on the rise: comparing 2021 to 2022, visits to piracy websites for film content grew by 36 percent, and visits to piracy websites for TV content grew by 9 percent. The United States accounted for a large share of this piracy, with U.S. visitors responsible for over 13.5 billion visits to film and TV piracy websites.[35]

Other studies have reached similar conclusions. In its 2021 *Movie & TV Piracy Trends*,[36] the Alliance for Creativity and Entertainment—which focuses on combating online video piracy—determined that there were:

- 159.6 billion visits to film and TV piracy sites globally in 2021;
- 16.0 billion downloads globally of pirated wide-release movies, primetime TV, and VOD shows in 2021 using peer-to-peer protocols alone; and
- 14.9 billion visits to film and TV piracy sites in 2021 from the United States.[37]

Drilling down on just a single piracy operation called *Fmovies* shows what a challenging problem piracy can be. This operation thrived for years while operating out of Vietnam, with its flagship site providing illicit access to tens of thousands of movies and TV shows, with a focus on shows from the United States and Europe. Over 18 months, from January 2023 to June 2024, the site had 6.7 billion visits.[38]

---

[34] https://www.ctam.com/wp-content/uploads/MUSO-2022-Film-And-TV-Piracy-Report.pdf
[35] *Ibid*
[36] https://www.alliance4creativity.com/wp-content/uploads/2022/11/ACE-Piracy-infographic-2021_final.pdf
[37] *Ibid*
[38] https://www.latimes.com/entertainment-arts/business/story/2024-08-29/anti-piracy-coalition-and-vietnamese-police-shut-down-major-pirate-streaming-business.

While the Government of Vietnam finally took steps to close down *Fmovies*, the harms inflicted over the years on legitimate sites, while difficult to quantify with precision, are enormous.[39] And there are always new sites ready to take their place, suggesting that a "whack-a-mole" strategy of trying to investigate and prosecute foreign sites one by one is doomed to fail.

Piracy from the Consumer Perspective

Viewed from the U.S. consumer angle, piracy is an enticing activity. A consumer survey report from April of 2024 by CordCutting called *The State of Content Piracy* revealed that:

- 1 in 3 American adults pirated shows or movies in the past year, and almost half the population have pirated at some point in their lives;
- The practice of piracy is particularly prevalent in younger Americans, with over 75 percent of people born after 1997 admitting that they have pirated content;
- 11 percent of people who recently pirated content said they do it now more frequently than a year ago; and
- 11 percent of people who do not pirate say they would if they knew how.[40]

How Profitable is Piracy?

Another way of assessing the problems posed by piracy is by estimating its profitability. The more profitable piracy is, the more likely organized criminals are or will become involved in it.

The evidence suggests that piracy is hugely profitable. One study from August 2020 estimated that global piracy operators offering illicit IPTV subscription services generate an estimated $1 billion a year by providing content to 9 million U.S. subscribers, enjoying robust profit margins of up to 85 percent.[41] These operators provide this content through at least 3,500 U.S.-facing storefront websites, apps, and social media pages.

On the VOD side, a report from August 2021 found that piracy operators that offer "free access" to movies and TV shows generate $1.3 billion in revenues from advertising.[42] This model is highly lucrative, with the top operators raking in between $18 million and $27 million a year.

Looking at the wealth accumulated by some of the relatively few U.S.-based piracy operators who have been prosecuted for their crimes affords another perspective on the profitability of piracy. For example, a self-proclaimed former drug dealer from New Jersey named Bill Omar Carrasquillo operated an illegal streaming service in the Philadelphia area. He became a millionaire within a year and was soon making $100,000 a day.[43] In the three years he operated his piracy scheme, he earned over $30 million, using his ill-gotten gains to purchase over 55 cars, motorcycles, ATVs, and other luxury vehicles, real estate, and a collection of diamond-studded jewelry.[44,45]

[39] https://www.msn.com/en-us/money/other/antipiracy-coalition-and-vietnamese-police-shut-down-major-pirate-streaming-business/ar-AA1pEfr8?ocid=BingNewsSerp
[40] https://cordcutting.com/research/content-piracy-study/
[41] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA-Money-for-Nothing-Report.pdf
[42] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/Breaking-Bads-Report.pdf
[43] https://www.youtube.com/watch?v=_e08DLdZSGA&ab_channel=SAYCHEESE%21
[44] https://appletowing.hibid.com/catalog/483697/-u-s--marshals-webcast-auction-baltimore--md-10-13-2023
[45] https://www.txauction.com/auctions/29776/lot/12423-lot-27

Another example is the operator of the immensely popular illegal sports streaming subscription service *Hehestreams*. That operator, Joshua Streit (not the basketball player of the same name), was ordered to pay almost $3 million in restitution at his sentencing in 2023 after the *Hehestreams* service was shut down in 2021.[46] Similarly, in a civil action, Florida-based Jason Labossiere and Nelson Johnson, operators of the illicit IPTV subscription service *Set TV Now*, were ordered to pay over $90 million in statutory damages after the operators were sued for copyright infringement.[47] The service had 180,000 subscribers before it was shut down.[48]

The amount of money illicitly earned by U.S. piracy operators that have been prosecuted criminally or sued civilly suggests that foreign piracy operators comparably accumulate great wealth from their illegal activities. The profitability of piracy, in combination with the relative lack of danger from prosecution in many jurisdictions, makes piracy a tempting lure for organized crime.

[46] https://www.justice.gov/usao-sdny/pr/minnesota-man-sentenced-three-years-prison-scheme-commit-computer-intrusion-and

[47] https://www.lightreading.com/video-broadcast/set-tv-is-now-really-really-dead

[48] Dish Network L.L.C. v. Johnson, Case No. 8:18-cv-1332-T-33AAS (M.D. Fla. Jul. 2, 2018)

International Piracy Players & the Harms They Cause

Who are the International Piracy Operators?

Because piracy is an illicit online activity, it is often difficult or impossible to discern where its operators are physically located. When a significant piracy operator can be identified as being in the United States, they are reachable by criminal prosecutions and subject to civil suits. When they are not, they can be difficult or impossible to reach.

We know little about most international piracy operators because they generally operate in secret, with their location hidden. What we know about the international piracy kingpins can be inferred from the few instances where they were identified and caught.

For example, Kim Dotcom's *Megaupload* piracy empire enabled him to live in luxury for years, residing in the most expensive home in New Zealand, sleeping in a $103,000 custom bed, and buying cars worth $4.8 million with vanity license plates ("Guilty," "Evil," and "Mafia") that celebrated his infamy.[49]

IMAGE 10: Kim Dotcom's Home in New Zealand

[49] https://archive.curbed.com/2012/10/18/10316438/its-said-to-be-the

At his height, Kim Dotcom was reportedly earning $150,000 a day in profits[50]—until he left his piracy operation vulnerable to action by U.S. law enforcement by establishing a *Megaupload* server in the United States. Although indicted in the United States, he has remained elusive, with the New Zealand government only recently ordering his extradition to the United States to face trial after a dozen years of legal proceedings.

Another glimpse into the profitability of piracy occurred when operators of the Polish piracy site *Ogladaj* were arrested.[51] Police reported seizing "various currencies, funds in accounts, luxury cars, as well as high-quality sports equipment, silver bars, and gold collector coins."[52] As a reminder that criminals such as piracy operators are often involved with other criminal activity, police also accused the *Ogladaj* operators of "deriving financial benefits from prostitution."

Another piracy operator who had been arrested in Poland, Artem Vaulin, has been evading a U.S. criminal indictment after vanishing in 2016 when he was released on bail.[53,54] Prosecutors claimed his site, *Kickass Torrents*, made $12 million a year from illegal piracy.

Even when prosecuted, international piracy operators often receive minimal sentences. For example, Fredrik Neij, a co-founder of the infamous *The Pirate Bay* piracy site, served only two-thirds of his 10-month sentence in a Swedish prison before being set free.[55]

In some instances, the location of the operators of major piracy sites may be known, but they remain out of reach of U.S. civil and/or criminal enforcement. For example, *Vegamovies* is known to be operated by an Indian national located in Western India. The site is in English and makes tens of thousands of U.S. and international movies and TV shows available. It receives over 180 million monthly visits.[56]

Another such service is *TeaTV*, which is operated from Vietnam and is one of the most popular VOD piracy apps in the United States. *Kemo IPTV* is another popular piracy subscription and VOD service operating in the United States, offering over 16,000 live channels and a VOD catalog with over 10,000 titles. *Kemo* is distributed under a number of alternative names and is operated by a Malaysian national currently living in the UAE.

[50] https://www.celebritynetworth.com/richest-businessmen/ceos/kim-dotcom-aka-kim-schmitz-net-worth/
[51] https://malopolska.policja.gov.pl/krk/aktualnosci/aktualnosci/40007,Co-najmniej-15-mln-zlotych-strat-i-3-osoby-z-zarzutami-za-nielegalne-rozpowszech.html
[52] https://sygnal.org.pl/en/three-people-detained-for-their-pirate-services/
[53] https://cyberscoop.com/kickasstorrents-artem-vaulin-poland/
[54] https://www.justice.gov/usao-ndil/pr/owner-most-visited-illegal-file-sharing-website-charged-criminal-copyright-infringement
[55] https://www.theguardian.com/technology/2015/jun/02/last-remaining-pirate-bay-founder-freed-from-jail-fredrik-neij
[56] https://ustr.gov/sites/default/files/2023_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy_Notorious_Markets_List_final.pdf

"Unfortunately, many of these websites like Fmovies are hosted on servers that exist outside the United States, currently outside our ability to take them down..."[57]

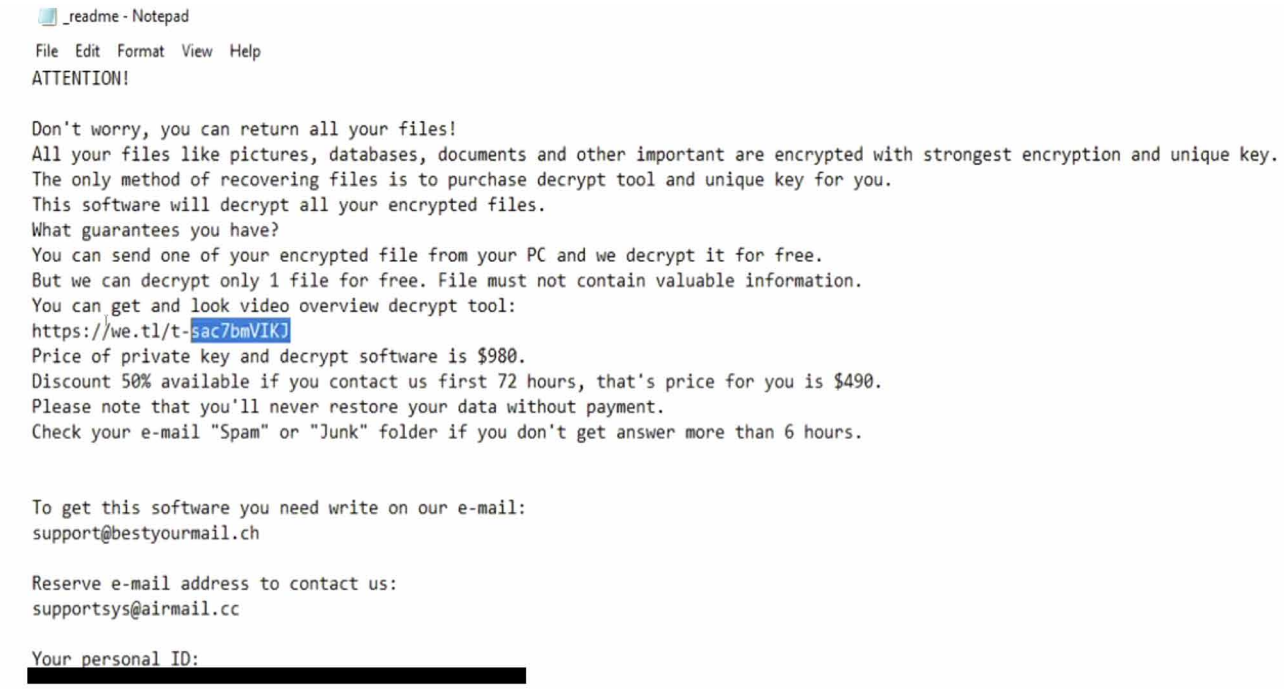
—Chairman Rep Darrell Issa (R-Ca.),
House Judiciary Subcommittee on Digital Copyright Piracy in December 2023

Harms from Piracy

While many piracy kingpins operating overseas work hard to keep their identities secret, the harms they cause are well-known. One of the most disturbing harms of piracy is its established link with malware. Piracy operators target the very people who make them money: their customers. Over the last decade, investigations have shown how piracy operators team up with malware-distributing cyber-criminals to infect the devices of the visitors and users of piracy websites and apps.

One stark example occurred during an investigation in 2022 that recorded a ransomware attack in real-time as a user clicked on an ad on a piracy website. After clicking on an ad, the user found their files locked up, followed by a demand to make a payment to regain access: "*All your files like pictures, databases, documents, and other important [*sic*]are encrypted with [*sic*]strongest encryption and unique key....Please note that you will never restore your data without payment.*" (Image 11)

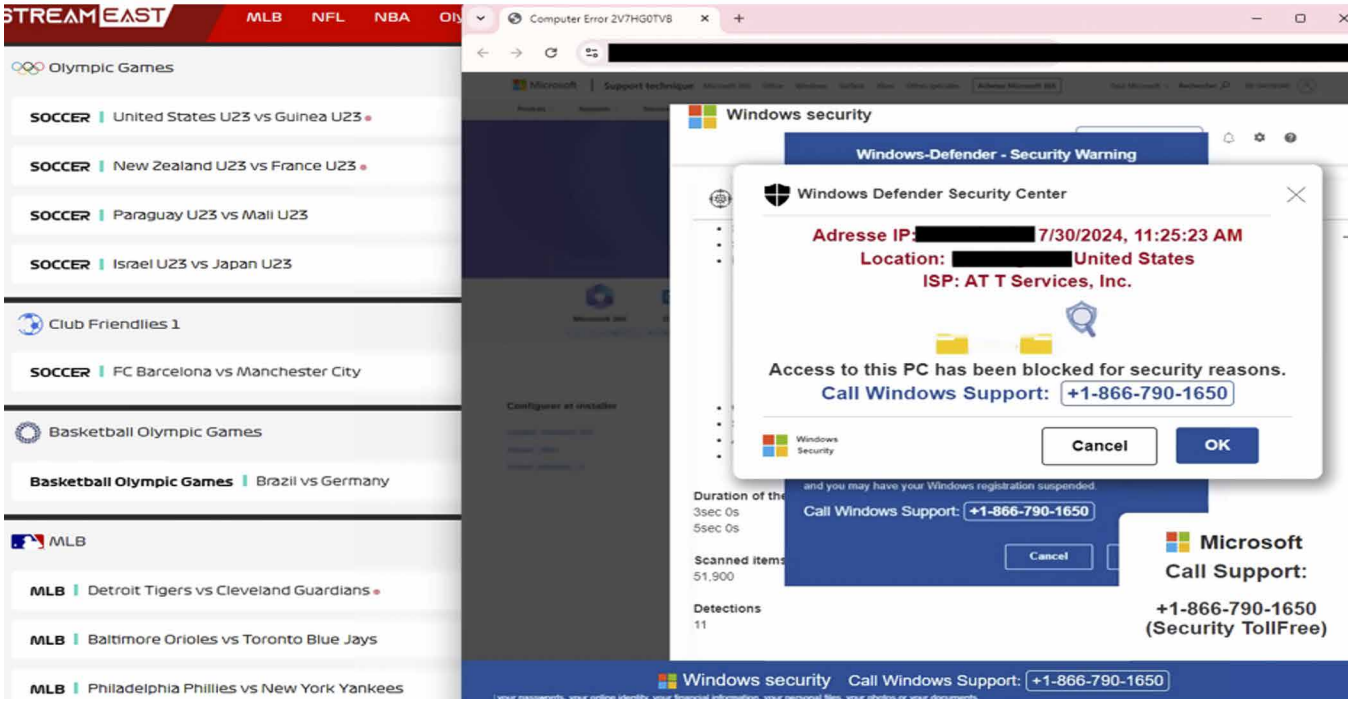
IMAGE 11: Ransomware Attack



[57] https://judiciary.house.gov/committee-activity/hearings/digital-copyright-piracy-protecting-american-consumers-workers-and

Another example of the link between piracy and malware is the fake security warning below on an ad on the illicit streaming service *StreamEast* (Image 12). Clicking the link to "resolve the issue" would result in the installation of malware, unwanted programs, or the user being scammed.

IMAGE 12: *StreamEast*



Piracy operators allow ransomware and other types of malware to pervade their sites for a simple reason: money. Nearly 80 percent of piracy sites served up malware-ridden ads to their users during the 2022 investigation referenced above. More than half of the $121 million generated ($68.3 million) from malvertising came from U.S. visits to these sites.[58] The sites investigated were overseas, outside the reach of U.S. law enforcement.

Sometimes malware is not contained in an ad but instead embedded directly into a piracy file, ready to infect the computers of the unwary downloader. Although the most basic tenet of cyber safety is not to download attachments from strangers, many people seem to suspend sensible caution in order to obtain desired pirated content. For example, just a few weeks prior to this report's publication, an infected file purporting to be a bonus episode of the popular TV show *House of the Dragon* was released to torrent sites. The file contained a "trojan horse" that is used to spread malware. According to *TorrentFreak*, the file was downloaded "many hundreds, or even thousands of times."[59]

[58] https://www.techradar.com/news/piracy-sites-are-bombarding-users-with-malicious-ads-to-download-actual-malware

[59] https://torrentfreak.com/bonus-episode-of-house-of-the-dragon-comes-with-a-nasty-surprise-for-pirates-240825/

The close nexus between piracy sites and services and malware propagation has been recognized by Interpol, the world's preeminent international law enforcement agency. In a 2023 report, Interpol warned that: "Many websites and peer-to-peer networks that offer pirated material may contain malware or viruses, which can harm the user's device or steal personal information. This malware can also spread in parallel within a home or corporate network, potentially affecting critical business operations, or used as the launchpad for identity theft and identity fraud."[60]

Academia has also noted the link between piracy and malware. For example, the Indian School of Business (ISB), in its 2024 report, *The Piracy-Malware Nexus in India*, concluded: "A nationally representative Perceptions and Experience study reveals that Indian consumers ranked their relative risk of downloading malware from piracy sites at 2.03 times greater than from mainstream websites. Piracy websites presented the highest risk for Indian consumers of malware infection (59 percent) followed by accessing adult industry ads (57 percent) and accessing gambling ads (53 percent)."[61]

These types of malware risks led the Federal Trade Commission in the United States to warn consumers to use only legitimate apps and stay away from apps that allow access to illegal pirated content: "Devices let you stream video through popular apps like *Hulu*, *Netflix*, *SlingTV*, *Amazon Prime Video*, and *YouTube TV*. *Unfortunately, there are other apps that allow you to watch illegal pirated content. And hackers are using those apps to spread malware.*"[62]

In addition to being fertile breeding grounds for malware, piracy also wreaks economic damage on the creative industries and on governments that rely upon the tax revenues that the legitimate industry generates.

The creative community is an important sector within the U.S. economy. Film and television production supports 2.74 million American jobs and comprises over 122,000 businesses while generating $229 billion in annual revenue.[63] When film and television shows are pirated, workers are not paid for their labor, distorting the market by understating the demand for the product, thus making them less profitable and less likely to draw capital.

Consumers lose too, as legitimate streaming services and filmmakers struggle to "compete with free." Small and independent streaming services offering diverse and less commercial programming face the greatest risks, and this illegal competition can drive them out of business altogether, depriving consumers and under-served audiences of creative options.

Independent filmmakers also must find a way to absorb losses from pirated views of their work. When a Philadelphia producer learned that her movie had been illegally downloaded 160,000 times, she wrote: "I spent over $20,000 self-funding *Love You Right*, and the film still is not paid off. If just a tenth of these hundreds of thousands of [pirated] views of my film paid just a dime to watch, it would be in the black. If just those 160,000 downloads paid a market rate of $4 per rental, the film would have earned more than half a million dollars."[64]

[60] https://www.interpol.int/en/Crimes/Illicit-goods/Shop-safely/Digital-piracy
[61] https://www.isb.edu/content/dam/sites/isb/India-Piracy-and-Cyber-Threats-Report-DM.pdf
[62] https://consumer.ftc.gov/consumer-alerts/2019/05/malware-illegal-video-streaming-apps-what-know (emphasis added)
[63] https://www.motionpictures.org/wp-content/uploads/2024/03/MPA_Economic_contribution_US_infographic-1.pdf
[64] https://www.inquirer.com/opinion/commentary/illegal-download-movie-piracy-filmmaker-20220228.html

In addition to industry and consumer losses, digital piracy also causes substantial taxation and other economic losses. According to the U.S. Chamber of Commerce's Global Innovation Policy Center (GIPC), digital piracy results in the loss of between 230,000 and 560,000 jobs and costs the U.S. GDP between $47.5-$115.5 billion annually.[65] And when members of the American creative community don't get paid for their work, the government loses tax revenue at all levels, including income taxes and corporate taxes. Of course, crime syndicates operating piracy sites and services don't pay taxes on their illicit earnings.

There is also a troubling correlation between paid subscriptions to piracy sites and credit card fraud. According to a 2023 investigation, Internet users who signed up for a piracy subscription service were four times more likely to report credit card fraud than those who don't visit such piracy websites and apps.[66]

Malware and credit card fraud are not the only harms caused by international organized piracy; it has also been found to thwart law enforcement and threaten national security. In 2020, NAGRA Kudelski, a company that specializes in digital security and media technologies, uncovered a troubling scheme where the residential Internet connections of piracy IPTV customers were provided to other users—who could potentially use them for illegal activities.[67] Access to these types of connections is especially attractive to criminals because, unlike IP addresses from data centers, residential Internet connections often fly under the radar of law enforcement or Internet security experts.

That poses a serious challenge for law enforcement and a major risk for the actual owner of the residential Internet connection. When crimes are committed using a residential Internet connection, they are harder for authorities to detect. But if they do detect illegal activities, it is the unsuspecting owner of the Internet connection who will appear to be the perpetrator.

NAGRA also found that pirated IPTV services can be a means for overseas terrorists to operate in the United States. Al-Manar is a Lebanese television outlet operated by the extremist political party Hezbollah and is banned from operating in the United States after the U.S. government labeled it a "Specially Designated Global Terrorist entity."[68] Nevertheless, Al-Manar was offered on at least half of the piracy IPTV services that NAGRA monitors, including a number of services available in the United States.

[65] https://alec.org/article/the-global-innovation-policy-center-releases-impacts-of-digital-piracy-on-the-u-s-economy/
[66] https://piracymonitor.org/dca-78-risk-of-fraud-if-you-used-a-credit-card-to-subscribe-to-a-piracy-service/
[67] https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA-Money-for-Nothing-Report.pdf
[68] https://dtv.nagra.com/pirate-subscription-services-now-billion-dollar-us-industry-joint-digital-citizens-alliance-nagra

Exploring Preventative Measures: Site-Blocking Around the World

The last section demonstrated that online piracy operators run a multi-billion illegal market, causing significant harm to the U.S. economy, to individuals who are targeted for malware or credit card fraud just by visiting an illicit site, and to creators who have their content stolen. The perpetrators of these harms often have little to fear because they are beyond the reach of U.S. law enforcement. So, the question becomes: If they remain beyond reach personally, can they at least be restricted in the United States from running their illegal business and targeting U.S. consumers for harm?

A growing number of countries have found a mechanism to stymie piracy organizations from preying on their citizens and disrupting their economies. The solution they have gravitated to is called "site-blocking." Whenever a piracy site is blocked in a particular jurisdiction, a user in that jurisdiction who types the name of the site in his or her web browser is not taken to the site. Instead, they may be met by an error message or redirected to a site explaining why the piracy site is not available in the country. Site-blocking is used to blunt many types of illegal acts. In addition to copyright theft, site-blocking orders have been issued to prevent access to sites that promote and facilitate prostitution, online gambling, and child pornography.[69]

In the United States, a legislative debate about site-blocking and other anti-piracy measures took place over a decade ago. That process did not result in Congress enacting a law, in part because some groups raised concerns that instituting site-blocking could disrupt the technical workings of the Internet.

Since then, however, many other countries have adopted some form of site-blocking. The United Kingdom was the first country to allow rights holders to apply for blocking order injunctions, resulting in ISPs in the United Kingdom blocking access to commercially infringing piracy websites.[70] Now, more than 50 countries across the globe have followed suit and allowed for judicial or administrative site-blocking injunctions against commercial piracy sites.

In this section, we:

- Explain what site-blocking is and how it works in practice;
- Review the evidence on site-blocking effectiveness; and
- Review the evidence on whether site-blocking has caused other types of harm, including interference with the technological operations of the Internet, violations of due process and free speech, and over-blocking innocent sites.

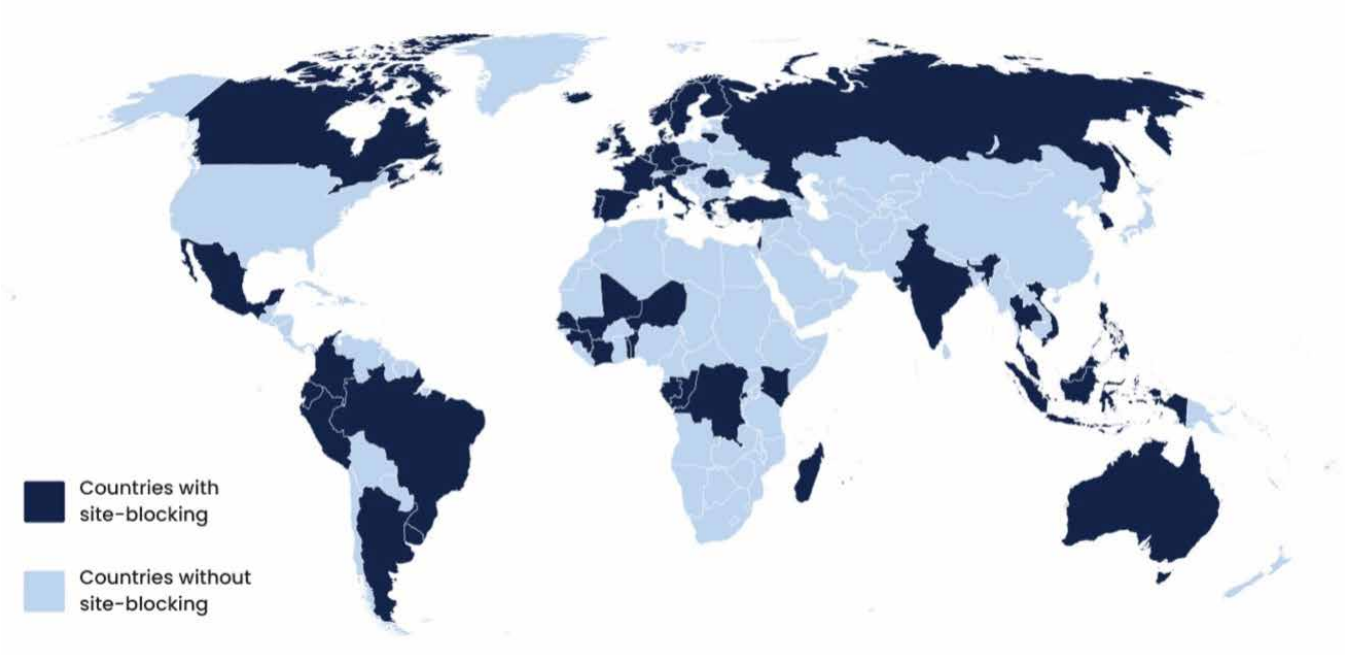
[69] https://www2.itif.org/2016-website-blocking.pdf

[70] https://www.reuters.com/article/world/british-court-orders-isp-to-block-piracy-site-newzbin-idUS1053241400/

What is Site-Blocking?

As the Information Technology and Innovation Foundation (ITIF) has noted, several dozen countries have adopted some form of site-blocking. These include much of the European Union, Canada, Australia, India, Brazil, South Korea, and Singapore (Image 13).[71]

IMAGE 13: Site-Blocking is Used in Over 50 Countries Around the World.



In each of these countries, there are slightly different methods for obtaining a site-blocking order and slightly different effects given to such orders. However, the process for obtaining a site-blocking order has far more commonalities than differences.

In general, a party seeking to obtain a site-blocking order (usually a rights-holder or organization acting on behalf of a group of rights-holders) has a high burden of proof to show that the site in question is either exclusively or substantially devoted to piracy and that a blocking order is justified. Due process is a key component of site-blocking procedures around the world, with the owners of sites targeted for blocking provided the opportunity to oppose the proposed orders. Although some jurisdictions allow an administrative agency to determine whether to grant a site-blocking order, in many countries that decision is entrusted to a court after it has had a full opportunity to consider the evidence.

As a technical matter, if an order is issued to block the site, it is generally served upon the leading Internet Service Providers in that jurisdiction. Those ISPs usually have discretion on how to implement these orders.

[71] https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online/

A common method is "Domain Name System (DNS)" blocking. A DNS request is how computers translate the name of a website (e.g., piracy-site.com) to the numerical address of the server (12.34.56.78) where the website is hosted. When a blocking order is implemented via DNS blocking, the user's DNS request no longer returns the numerical address. Instead, it returns either an error message or redirects the user to a site explaining why the DNS request wasn't resolved on the piracy site.

IMAGE 14: Before DNS Blocking is Implemented:

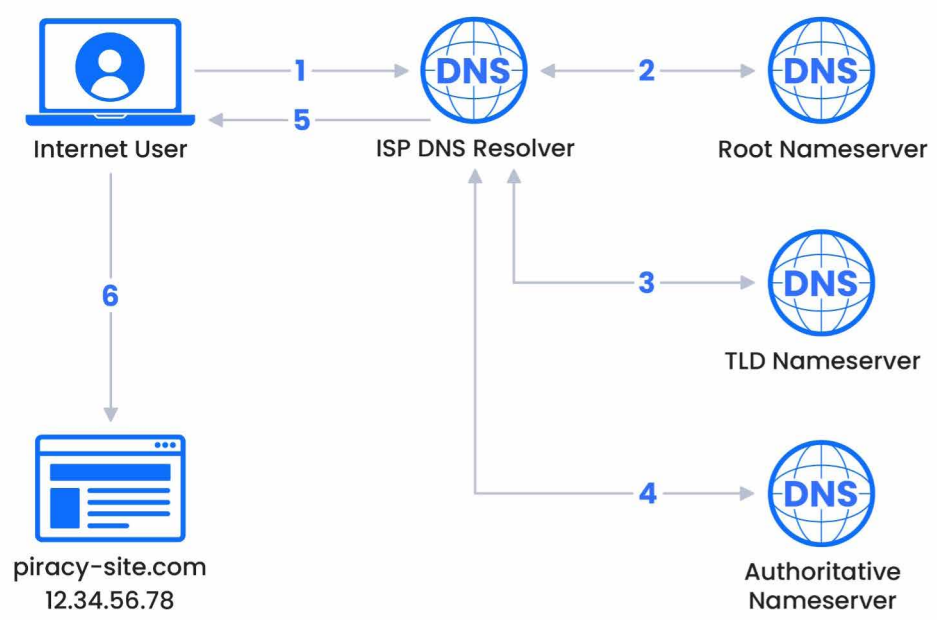
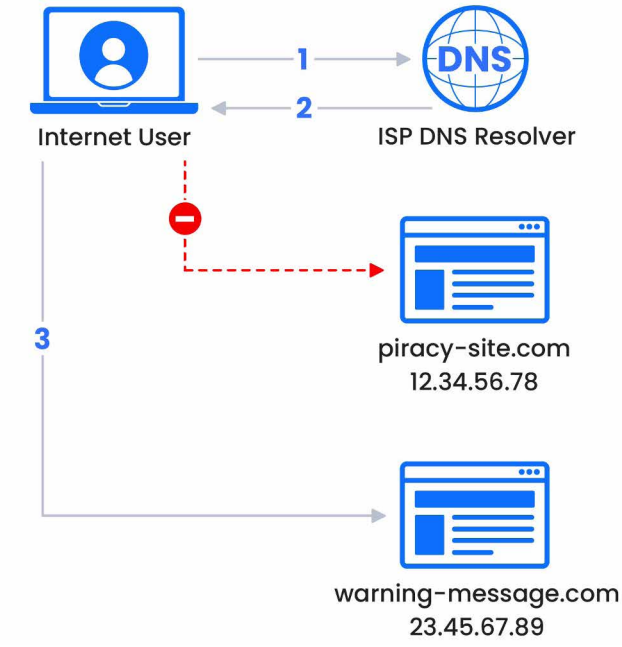


IMAGE 15: After DNS Blocking is Implemented:



Other types of blocks have also been utilized to prevent piracy operators from easily accessing users in countries that have adopted site-blocking. One such method is IP blocking. When it can be established that only infringing sites use a particular IP address, the ISPs in the jurisdiction can block any effort to reach that address. A schematic explaining the process of IP blocking can be found below:

IMAGE 16: Without IP Blocking:

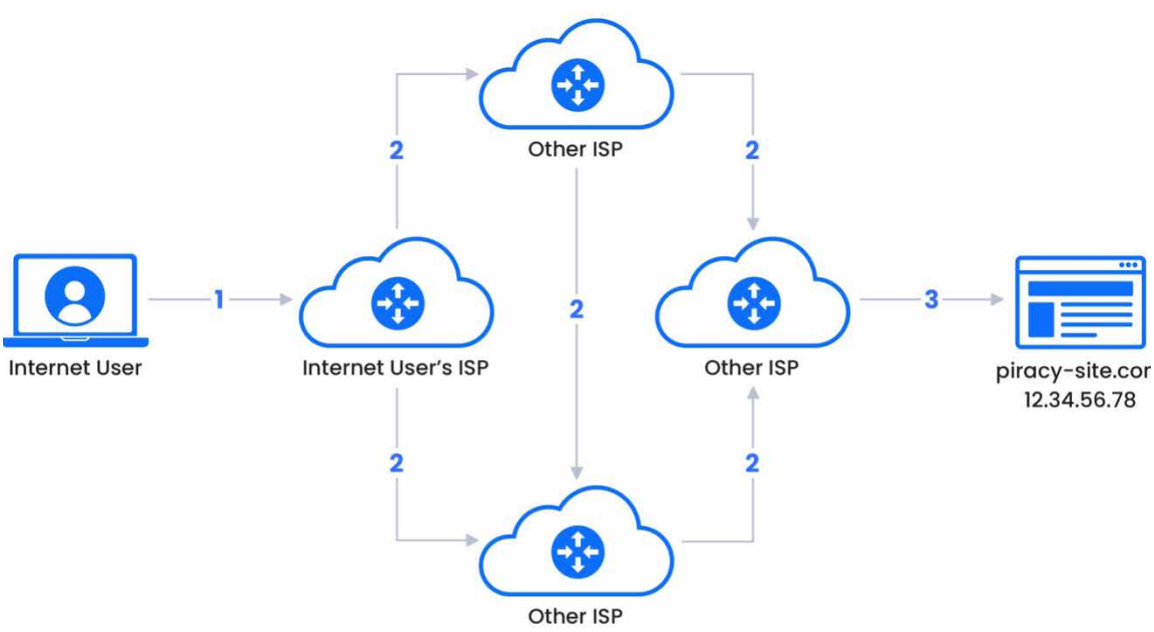
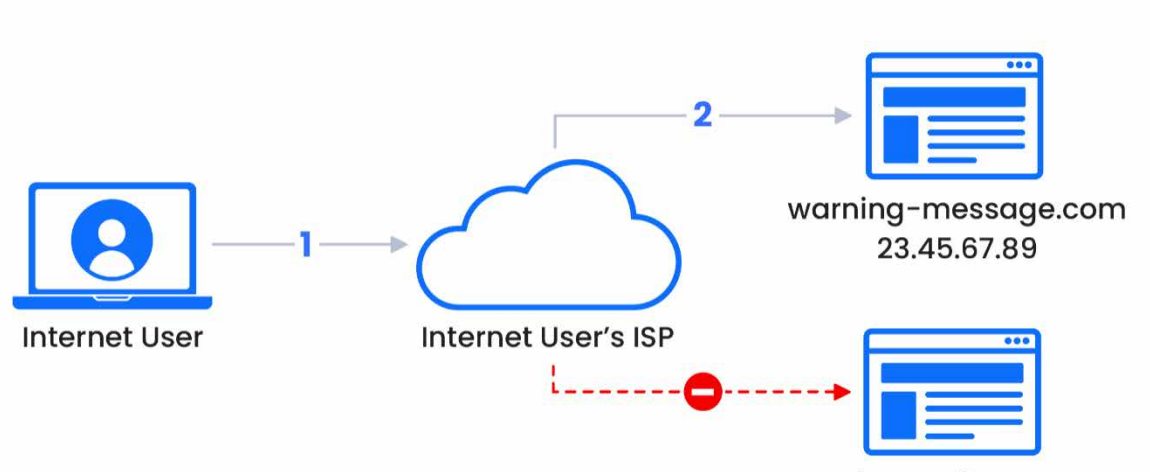


IMAGE 17: With IP Blocking



The Effectiveness of Site-Blocking

As noted above, site-blocking has been adopted in a number of countries around the world. All told, courts and administrative agencies have disabled access to more than 90,000 domains used by over 27,000 piracy sites.[72]

Scholarly studies have concluded that site-blocking has had a real and lasting impact, reducing visits to piracy sites and often spurring more visits to legitimate sites. The most recent study, *The Impact of Online Piracy Website-blocking on Legal Media Consumption,* published in early 2024, looked at the effects of site-blocking in India and Brazil.[73] It determined that "website-blocking in India in 2019 and 2020 caused an 8 percent and 3 percent increase in legal consumption, respectively, and website-blocking in Brazil in 2021 caused a 5 percent increase in legal consumption."

These findings were consistent with earlier studies looking at the impact of site-blocking in the United Kingdom. There, visits to those piracy sites that were subject to a blocking order decreased by an average of 89 percent between June 2021 and May 2022. Importantly, site-blocking resulted in an overall 24 percent reduction in piracy traffic.

Other countries have seen similar results:

The UK is not the only country where you can see a change in behavior because of site blocking. In Portugal, site-blocking reduced traffic to adjudicated piracy websites by 70 percent.[74] Meanwhile in Australia, site-blocking regulations resulted in a 69 percent drop in traffic to blocked sites and a 25 percent reduction in traffic to the top 250 piracy sites that had not been blocked.[75]

In the last few years, some countries have made their site-blocking processes even more effective by introducing "dynamic site-blocking orders." Such orders include a process to quickly obtain a new site-blocking order against a redirect, proxy, or mirror site to an already blocked domain. A "brand order" is another type of dynamic blocking order currently being issued in courts in Australia, India, and the United Kingdom. Brand orders are used against copycat sites that intentionally use domain names similar to popular piracy sites in order to encourage user traffic. Significantly, new dynamic orders recently issued by the Delhi High Court in India now include not only brand orders but also separate orders to domain name registrars associated with the identified piracy domains, requiring them to "lock and suspend" the blocked domain name and provide the rights owners with registrant details.

[72] https://judiciary.house.gov/committee-activity/hearings/digital-copyright-piracy-protecting-american-consumers-workers-and
[73] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4723522
[74] https://www.telecompaper.com/news/portuguese-report-finds-drop-in-use-of-pirate-websites--1205893
[75] https://creativecontentaustralia.org.au/wp-content/uploads/2021/03/INCOPROAustralianSiteBlockingEfficacyReport-KeyFindingsJuly2018FINAL.pdf

Site-blocking is not a perfect remedy. Intrepid consumers of pirated content may well be able to find ways to evade a site-block. Nevertheless, blocking effectively sends the message to the average consumer that piracy is illegal and dangerous—and the evidence indicates that the message helps educate consumers about the risks so they can make their own viewing decisions.

For a comprehensive review of the data about site-blocking around the world, it is worthwhile to review *Congress Should Protect the Rights of American Creators with Site-Blocking Legislation* by Adam Mossoff.[76]

Perceived Dangers of Site-Blocking

The evidence set forth above suggests that site-blocking—while not a silver bullet to the total problem of online piracy—is effective. At the same time, it is important to consider in any public policy debate whether any potential "side effects" of site-blocking outweigh the benefits. There have been three basic arguments leveled against site-blocking in the United States and jurisdictions that have later adopted the practice. These are that site-blocking:

- Endangers the technical working of the Internet;
- Lacks due process stifles legitimate speech; and
- Sweeps up innocent sites by "over-blocking."

The concern that site-blocking would interfere with the technical workings of the Internet was first voiced during the 2012 debate about adopting site-blocking in the United States. Colloquially, this was expressed as a fear that site-blocking would "break the Internet," resulting in a lack of access to the legitimate websites citizens of the U.S. and people around the world have come to depend upon.[77]

The simple answer to this concern can be gleaned from the experience of the more than 50 countries that have adopted site-blocking. None of those countries have reported any discernible effect on the technical working of the Internet.

A 2016 paper titled *How Website-blocking Is Curbing Digital Piracy Without "Breaking the Internet"* by the Information Technology & Innovation Foundation was among the first to evaluate whether these claims came to pass in countries that adopted site-blocking:

"The growing use of website-blocking…shows that these claims were not based in reality and that website-blocking did not 'break the Internet,' nor lead to a multitude of other predicted dire outcomes, such as the widespread circumvention of blocking orders, the fragmentation of the global DNS namespace for the Internet, an alternative DNS system for the Internet, nor contribute to a breakdown in user trust and an exodus of users from the Internet." [78]

[76] https://www.hudson.org/intellectual-property/congress-should-protect-rights-american-creators-site-blocking-legislation-ad-am-mossoff
[77] https://itif.org/publications/2015/10/12/oops-dns-blocking-did-not-break-internet/
[78] https://itif.org/publications/2016/08/22/how-website-blocking-curbing-digital-piracy-without-breaking-internet/

Concerns have also been raised that site-blocking lacks due process and stifles free speech. A review of the practices in countries that have adopted site-blocking, however, shows that, especially in those jurisdictions that require court approval, there are rigorous due process protections and procedures set in place to ensure that site-blocking is used appropriately and only against egregious sites that are essentially dedicated to piracy. Our review found no instance in which a site was ordered blocked pursuant to such a process and later proven to not be a piracy site—suggesting that the measures in place are working well.

In addition, we found no evidence that legitimate speech has been wrongly stymied by site-blocking orders. Sites that distribute content that belongs to others without permission are not engaged in speech; they are engaged in theft, and the fact that the stolen goods are digital is of no consequence.

Our review also investigated claims that site-blocking would lead to so-called "over-blocking," where legitimate sites are swept up along with illicit sites. There are scant instances in which a legitimate site was blocked as part of an effort to impede a piracy site, especially where the blocks are court-ordered. In those few cases, over-blocking has generally occurred because an ISP implements the order without sufficient due diligence and checking, and any inadvertent errors were quickly rectified.

Conclusion

Much has changed in the last decade. Digital piracy has exploded into a $2 billion-plus illicit enterprise.[79] Savvy criminals have exploited piracy to spread malware and engage in credit card fraud. The secondary effects of piracy have, at times, jeopardized law enforcement's ability to protect America's economic and national security.

At the same time, the last decade has created an opportunity to assess the efficacy of site-blocking based on the evidence. Thousands of blocking orders have been executed in more than 50 countries, so any real shortcoming or defect in the process would have clearly surfaced and resulted in concrete examples of failed or inappropriate blocks. Indeed, there is a highly motivated and well-funded cadre of site-blocking critics scouring the record and scrutinizing these cases for any hint of a problem. But no such obvious examples exist.

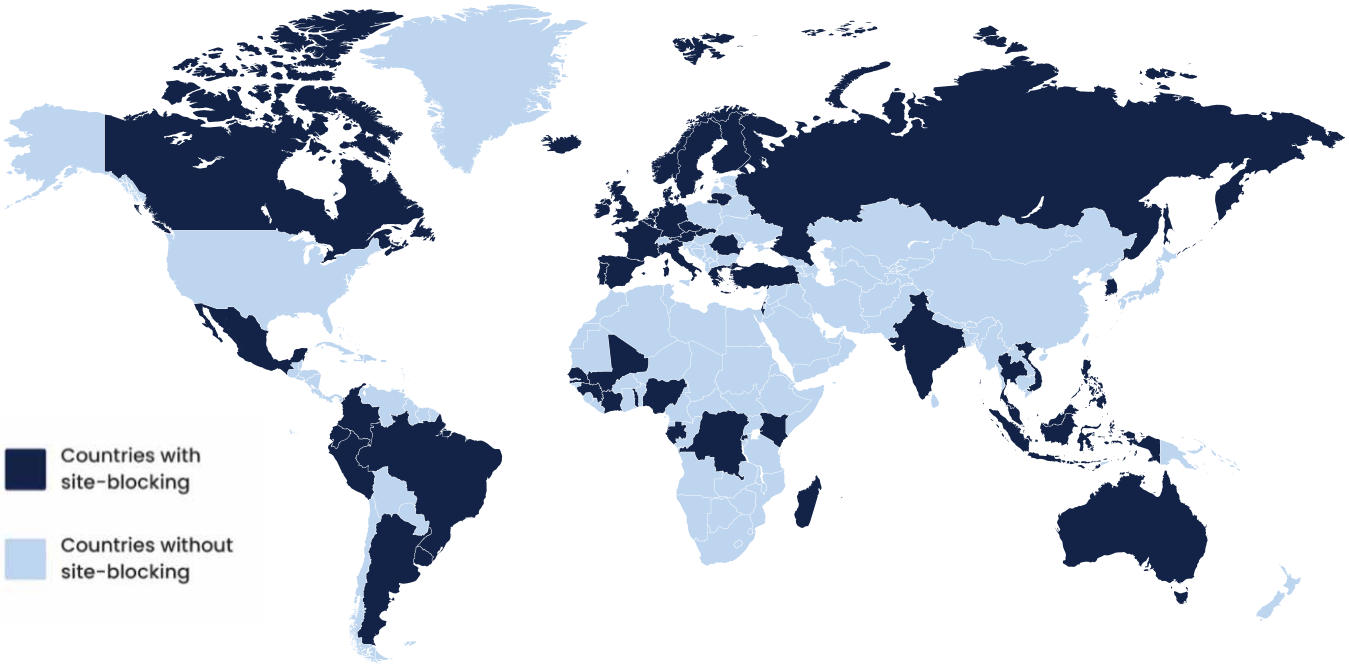
The lack of evidence of abuse suggests that site-blocking orders are fair, rigorous, and issued only in legitimate cases of large-scale piracy.

While site-blocking is relied upon across the globe, it has not been authorized in anti-piracy cases in the United States—the home to not only the world's creative center but also perhaps the world's preeminent and most rigorous judicial system. U.S. policymakers who may be concerned about the possibility of over-blocking or other abuse should have great confidence in the ability of U.S. federal courts to deliver procedural fairness and issue blocking orders only where appropriate—and are free to design robust processes and guardrails to govern the issuance of such orders. The global track record on site-blocking is strong, but the United States has the ability to set the bar even higher.

Taken as a whole, the IP House review of site-blocking measures employed by other countries found they did not cause the types of harm that critics claimed they would during the last Congressional debate in 2012. Given that, it is IP House's viewpoint that it would be appropriate for the U.S. Congress to once again explore the feasibility of legislation to enact site-blocking in the United States.

[79] https://www.uschamber.com/technology/data-privacy/impacts-of-digital-piracy-on-the-u-s-economy

Countries That Have Implemented Site-Blocking



North America
Canada
Mexico

Latin America
Argentina
Brazil
Colombia
Ecuador
Peru
Uruguay

Asia Pacific
Australia
India
Indonesia
Malaysia
Philippines
Singapore
South Korea
Thailand
Vietnam

Europe, Middle East, and Africa
Austria
Benin
Belgium
Czech Republic
Democratic Republic of Congo (DRC)
Denmark
Finland
France
Gabon
Germany
Greece
Guinea
Iceland
Ireland
Israel
Italy
Ivory Coast
Kenya
Lithuania
Madagascar
Mali
Mauritius
Netherlands
Niger
Norway
Portugal
Republic of Congo
Romania
Russia
Rwanda
Senegal
Slovakia
Spain
Sweden
Togo
Turkey
United Kingdom

About IP House

IP House was founded by two professionals dedicated to combating illicit trade. Steve Francis, with 25 years in federal law enforcement leadership roles and most recently as Executive Associate Director for Homeland Security Investigations (HSI), has directed IP responses across the U.S. government. He recognized the need for a more proactive approach, combining awareness, education, and risk management with prioritized enforcement rather than relying solely on fragmented vendor efforts and government response.

Jan van Voorn, who launched and led the Alliance for Creativity and Entertainment at the Motion Picture Association, saw similar challenges. He noted the inefficiencies and high costs of fragmented private sector responses and the benefits of coordinated efforts across organizations.

Together, they envisioned IP House as the provider of world-class IP protection services across all industries, combining human intelligence, cutting-edge technology, and a truly global footprint.

IP House has a rapidly growing team of over 250 professional investigators, analysts, and IP law counsels and specialists, each skilled in a wide range of effective countermeasures against IP crimes, from litigation to site-blocking and criminal enforcement. With such a depth of knowledge comes an understanding of the most effective solutions to different types of IP violations, including patent infringements, counterfeiting, and digital piracy. IP House adopts a holistic view and considers all possible angles and impacts to provide comprehensive solutions to these harmful criminal acts.

Relentless attacks from counterfeiting, piracy, and other intellectual property (IP) infringements drain $2.5 trillion annually from the global economy. Across digital and physical realms, threats to IP often dwell in the shadows, masked by anonymity and sophisticated operations. IP House provides end-to-end proactive solutions to protect IP rights and unmask the operators behind these crimes anywhere in the world. Its cyclical approach gathers intelligence on infringements at every stage to fuel new investigations, disrupt activities, and launch civil or criminal actions. With innovative strategies and unparalleled industry expertise, IP House ensures that business threats are neutralized at their source and critical distribution points around the world.

ip-house.com

digitalcitizensalliance.org