Contribution Stichting BREIN on the EU Counterfeit and Piracy Watch List for 2025

The BREIN foundation (Stichting BREIN or "BREIN") is the Dutch joint content protection program of authors, artists, publishers, producers and distributors of music, film, games, TV, interactive software, books and images. BREIN represents various Dutch national and international branch organizations and collecting societies representing producers, publishers, composers, text writers, writers, photographers, directors and all kinds of performing artists such as musicians and actors.[1]

BREIN would like to address some of the issues, developments and services it encounters in its daily business of combating online piracy, that fit the purpose of a contribution to the Counterfeit and Piracy Watch List for 2025.

Intermediaries

All stakeholders in the internet ecosystem, including hosting providers, DNS providers, cloud services (including reverse-proxy and anonymization services), advertising networks, payment processors, social media platforms, and search engines, should proactively work towards reducing support for well-known infringing sites. Voluntary initiatives aimed at combating online content theft should be embraced. It is important to note that categorizing a service as an infrastructure service does not absolve it from duties of care and responsibilities.

Also, in general, intermediaries should know who their customers are. We call this the "Know Your Customer" (KYC) principle. This of course has been incorporated in the Digital Services Act for online marketplaces[2], but this obligation should not be limited to these services only. For VAT purposes such a broader obligation already exists in the international context if for example a customer wishes that the 0%VAT tariff is applied. In such case a customer must prove its address outside the EU to qualify for the reduced VAT rate. Illegal actors often operate anonymously and can continue their illegal business elsewhere if their website is taken offline. If they can be identified, they can be held liable. To do so more efficiently it also should be possible to obtain cross-border injunctions more easily.

At the moment, data privacy is the main obstacle to the right of information, even if the infringing party apparently qualifies as a legal entity providing an information society service, which already has the obligation to publish its true identity and address under EU law. Even in such cases often unjustly a court order is demanded (for instance by the internet service provider) to obtain identifying information. In most other cases a claim for a court order is not justified either, because the information can be shared without a court order on the basis of general tort law.[3]

[1] For more information please visit www.stichtingbrein.nl
[2] Article 30 DSA
[3] Dutch Supreme Court 25 November 2005, ECLI:NL:HR:2005:AU4019

For several years now, the hosting landscape has dramatically changed. Most major Dutch hosting providers no longer see themselves as hosting providers but try to position themselves as 'mere conduit' or 'internet access providers': they argue that they only offer internet connectivity. They point to their resellers (usually located abroad and often even outside the EU) who would be the real hosting providers. These resellers are often however not cooperative or not even responsive. And even if they are responsive and willing to provide information, the information is usually not verified. BREIN has thought of a way to tackle this development, which is to ask of the Dutch (or EU) internet service providers to implement in their contractual relationships with non-Dutch (or non-EU) parties, what we under Dutch law describe as a 'chain clause' ensuring that KYC obligations are also implemented by their resellers. An alternative solution would be that all intermediaries from outside the EU which *host data at datacenters within the EU*, should have a point of contact within the EU, also if they offer their services to customers outside of the EU.

BREIN would like to draw the attention to the below listed companies that BREIN encountered in the past years and that – in BREIN's experience – can be labeled as 'not responsive' or 'not cooperative':

- *Amarutu Technology Ltd,* also trading under the name "*Koddos*"
  Website: koddos.net.

  Koddos is a Hong Kong based hosting provider that uses several different Dutch datacenters. They have not been responsive to BREIN's takedown and/or information requests in relation to evidently illegal websites hosted in their network in the past. If BREIN succeeds in getting her requests handled correctly by Koddos, this is due to the mediation of the Dutch datacenter that Koddos uses in that particular case, but this cannot always be established.

- *Private Layer Inc.*
  Website: privatelayer.com

  A hosting provider based in Panama, using datacenters in Panama and Switzerland. They are known as a bulletproof hosting provider, not responding to any takedown- and information requests. They don't display their company details on their website.

- *Alexhost SRL*
  Website: alexhost.com

  Hosting provider based in Moldova. It i.a. uses servers in Dutch datacenters and does not respond to BREIN's requests in relation to evidently illegal websites hosted in their network.

- *Virtual Systems LLC*
  Website: vsys.host.

Virtual Systems is based in the Ukraine and uses i.a. servers in Dutch datacenters. They do not respond to BREIN's requests in relation to evidently illegal websites hosted in their network. In the past BREIN established that Virtual Systems applies masking techniques to hide the origin of the (Dutch?) data.

- *SERVERS TECH FZCO*, also trading under the name "*Vdsina"*
  Website: vdsina.com

  Located in the United Arab Emirates. This hosting provider does not respond to BREIN's requests in relation to evidently illegal websites hosted in their network.

- *Packet Exchange Limited*
  Website: packetexchange.eu

  Packet Exchange is a hosting provider located in the United Kingdom. BREIN has established several times that this hosting provider does not respond to requests.

- *Sarek Oy* and *1337 Services LLC*, the latter also trading under the name "*Njalla"*
  Website Sarek: sarek.fi
  Website Njalla: njal.la

  Sarek (based in Finland) and Njalla (based in Saint Kitts and Nevis) act as intermediaries for domain name registration purposes, procuring and 'owning' the domain names on behalf of others to provide them with full anonymity. Peter Sunde, co-founder of the notorious The Pirate Bay, is involved in both companies. Sarek and Njalla are prominent among pirate sites, as BREIN has also discovered in preparing its blocking cases (see below). Neither of these intermediaries responds to any of the requests BREIN has made until now. In light of this, BREIN is supporting the decision of the Dutch domain registry, Stichting Internet Domeinregistratie Nederland (SIDN), to prohibit third-party registration of .nl domain name holders and registrars as of October 2023.[4]

- *Namecheap, Inc*
  Website: namecheap.com

  Namecheap is a prominent domain name registrar and hosting provider based in the United States but with customers from all over the world. BREIN has contacted Namecheap multiple times over the past years, including in relation to the blocking cases. BREIN has requested Namecheap in several instances to cease providing their services to these evidently illegal websites that are now blocked in The Netherlands, as well as to provide BREIN with the customer details. Namecheap has never complied with these

[4] https://www.sidn.nl/en/news-and-blogs/privacy-and-proxy-services-prohibited-from-nl-after-1-october

requests and always insists on a US court order and is therefore willfully uncooperative as these cases clearly concern evidently illegal websites.

Blocking Targets

Neutral intermediaries have an obligation to help prevent abuse of their services for illegal use or failing that to at least help mitigate the negative effects thereof. Most significant in this respect is the dynamic blocking by internet access providers (IAPs) of popular illegal sites. By now BREIN has expanded the blocking measures applied by Dutch IAPs (laid down in a blocking court order requested by BREIN) to:

Popular illegal Bittorrent sites:

- The Pirate Bay (main domain: thepiratebay.org)
- Limetorrents (main domain: www.limetorrents.lol)
- 1337x (main domains: 1337x.to, 1337x.st, x1337x.ws, x1337x.se, x1337x.eu and x1337x.cc)
- EZTV (main domains: eztvx.to, eztv.yt and eztv.wf)
- Kickasstorrents (main domains: kickasstorrents.to, kickasstorrents.cr, kickasstorrent.cr and katcr.to)
- YTS (main domain: yts.mx)

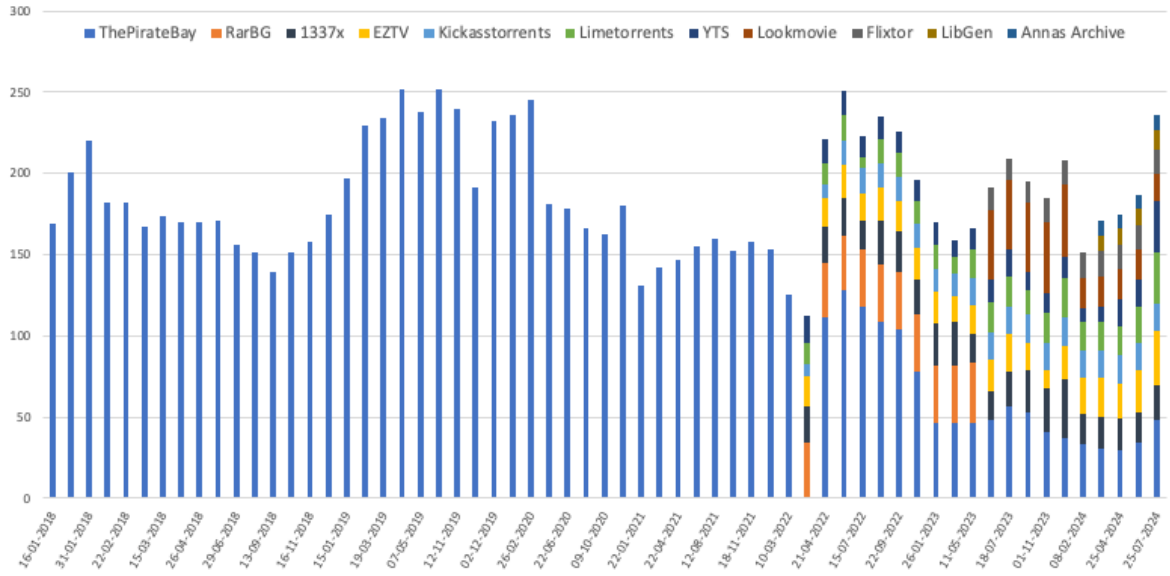
Video streaming sites:

- Flixtor (main domains: flixtor.vc, flixtor.to, flixtor.tk, flixtor.sx, flixtor.se, flixtor.nu, flixtor.li, flixtor.la, flixtor.fi, flixtor.ch and flixtor.bz)
- Lookmovie (main domains: lookmovie2.to, lookmovie2.la, lookmovie.buzz, lookmovie.clinic, lookmovie.digital, lookmovie.download, lookmovie.foundation, lookmovie.fun, lookmovie.fyi, lookmovie.guru, lookmovie.media, lookmovie.mobi and lookmovie.site)

Clusters of illegal download sites specialising in ebooks, articles and audiobooks

- Anna's Archive (main domains: annas-archive.org, annas-archive.se and annas-archive.li)
- Library Genesis (main domains: libgen.st, libgen.rs, libgen.rocks, libgen.li, libgen.is and libgen.gs)

As well as the main proxies and mirrors for all of the above illegal services, which concerns a dynamic group of sites, fluctuating but at all times resulting in around 200 domains. BREIN keeps track of this and periodically sends updates to the access providers (see also below). It is clear that these proxy services are a business model as such, part of a commercial activity that relies on copyright theft. In the near future BREIN will continue to expand the list of blocked illegal services.



The chart above shows all the updates BREIN has sent to Dutch IAPs regarding websites to be blocked. It shows that the numbers of domains fluctuate monthly. A total of 1,770 unique domains have been blocked by IAPs since the beginning of 2018 through 61 updates requested by BREIN. Of these, a total of 1,534 domains have also been unblocked again. Currently, 236 domains providing access to clearly infringing websites are blocked. In addition to the main domains, this number includes the proxies and mirrors of the aforementioned illegal platforms. It is also striking that over time the average number of proxies and mirror websites per platform decreases so that the total number of blocked sites has not increased. Apparently, many proxy sites give up if they are blocked long enough.

Trends

IPTV

Illegal IPTV is the most serious threat for the audiovisual rights holders. A study by Bournemouth University from 2022[5] concludes that in 2018 8.2% of the Dutch population used illegal IPTV for an average price of 5,35 euro per month. A EUIPO report from September 2023 concludes that 58% of online piracy is streaming (IPTV) and 32% downloading.[6] We see sales of illegal IPTV online through sites and ads but also neighbourhood satellite/electronics shops and market halls. The producers, broadcasters and all of the copyright and neighbouring rights holders involved in TV channels, movies and series and live sports broadcasts suffer great damage from illegal IPTV. In May 2023, the European Commission published a recommendation on combating online piracy of 'sports and other live events'.[7] Consumers can buy these illegal subscriptions online also from sellers that are located outside of the EU.

[5] https://www.aapa.eu/illicit-iptv-in-europe-an-aapa-economic-report

[6] https://www.euipo.europa.eu/nl/publications/online-copyright-infringement-in-eu-2023

[7] Commission Recommendation (EU) 2023/1018 of 4 May 2023 on combating online piracy of sports and other live events, OJEU 2023, L 136/83.

Circumvention of technical protection measures

Services aimed at the circumvention of technical protection measures, parasitizing the methods of exploitation available to the rights holders, remain a significant issue. Such services provide the ability to access legal distribution channels such as streaming platforms or online newspapers, in a manner normally limited to paying subscribers, circumventing the paywall as well as any other technical protection measures applied by the distributor to prevent illegal access or (re)use of the works they intend to make available to their customers.

Amongst such circumvention services, so called 'stream ripping services', as were also included in the 2022 watchlist continue to be a key threat in particular to stakeholders in the music industry.[8] Stream ripping services provide the ability to create a permanent offline video or audio file containing a copy of any work available on a video streaming platform, a service normally only available to paying subscribers and subject to technical restrictions that prevent the further distribution of the offline copy.

Another significant threat are the so-called 'paywall bypassing services', which although absent from the 2022 report, are no less undermining of the earning capacity of in particular stakeholders in the area of publishing especially publishers of newspaper and other periodicals. Paywall bypassing services enable users to access online articles without having to pay a subscription. Typically this is done either by 'live' bypassing of the technical protection measures that prevent (further) access to the non-paying consumer or by making available a copy of the protected work that the 'bypassing service' permanently stores for ready access.

Vinyl

Vinyl continues making a comeback. A report[9] of The Recording Industry Association of America (RIAA) shows that revenues from Vinyl records in the US grew 10% to 1.4 billion dollars - the seventeenth consecutive year of growth. In the US vinyl now accounts for 71% of physical format revenues. The Global Music Report 2024[10] of The International Federation of the Phonographic Industry (IFPI) concludes that for a third consecutive year, global physical revenues rose with an upswing of 13,4% in 2023, with vinyl experiencing a faster growth rate than subscription streaming. Driven by gains in CD revenue and the continued expansion of interest of vinyl, physical formats were worth 5.1 billion dollars in 2023 and accounted for 17,8% of the global market.

The revival of vinyl simultaneously causes a rise in the manufacturing and selling of unauthorised vinyl in the form of counterfeit and bootleg albums originating within and outside of the EU. There is also an increasing amount of ‘grey’ bootlegs (albums consisting of unauthorised pressings of live radio or tv broadcasts) entering the market, where actors take advantage of the ambiguity

[8] European Commission, Commission staff working document. Counterfeit and Piracy Watch List, 1 december 2022, SWD(2022) 399 final p. 19 -20

[9] https://www.riaa.com/wp-content/uploads/2024/03/2023-Year-End-Revenue-Statistics.pdf

[10] https://globalmusicreport.ifpi.org/

surrounding the legal status of live recordings. These grey bootlegs are oftentimes being sold through legitimate (online) retail shops.

Artificial intelligence

Artificial intelligence (AI) is developing at lightning speed. For rights holders, AI offers opportunities but also threats. There are great advantages to be gained from AI. For example, it enables more efficient work. It can also help in the creative process. Unfortunately, in practice there also appears to be large-scale illegal and infringing use of AI.

So far, for example, BREIN ran into gigantic illegally compiled datasets for training generative AI large language models (LLMs) that copied content from obviously illegal sources and from sources that explicitly made a copyright reservation. Copying from illegal sources, and thus data mining for the purpose of AI, is never allowed[11]. Illegal sources include, for example, the obviously illegal websites that are also blocked in the Netherlands (see above). BREIN has taken offline a database intended to train an LLM containing more than 70,000 Dutch-language ebooks from illegal sources. BREIN also sees datasets for training AI models based on massive scraping of legal sources. This too is not allowed if a copyright reservation is made in accordance with article 15o Dutch Copyright Act (DCA). This concerns the article (together with article 15n DCA) that implements the so-called text and data mining exception of articles 3 and 4 of the DSM Directive[12]. BREIN also acted against infringements in the form of AI-generated summaries of ebooks and a chatbot aimed at making unauthorized VOD content available. Also BREIN has come across illegal deepfake videos and voice clones.

BREIN applauds the arrival of the European AI[13] Act which will hopefully create a level playing field for all AI applications (to be) offered on the European market. BREIN also urges rightsholders - if they have not already done so - to make use of the copyright reservation if they do not want their creations to be used for (training of) AI. BREIN is not against AI but it is against the infringing and unlawful use of AI. BREIN fights for the right of rights holders to determine for themselves what happens to their creations.

[11] See: CJEU Case C-435/12 https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140058en.pdf

[12] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (DSM Directive): https://eur-lex.europa.eu/eli/dir/2019/790/oj

[13] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act): https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202401689&qid=1723479753614

Web 3 / IPFS

Web3 is the next generation of the internet that aims to decentralize the web using blockchain technology, giving users greater control over their data and digital identities. It relies on a network of nodes instead of central servers, incorporating cryptocurrencies for secure transactions and smart contracts for automated agreements. These technologies also introduce specific risks and challenges related to piracy, for example:

- Immutable storage - Content stored on blockchain-based systems is immutable and cannot be altered or deleted. Once pirated content is added to the blockchain, it remains there permanently, posing a significant challenge for copyright enforcement.
- Cryptocurrency transactions - Development of anonymous cryptocurrency services like Monero complicates enforcement measures as users cannot be pinpointed directly.
- Lack of central authority - Decentralized systems lack a central authority that can be approached to take down infringing content.
- Smart Contracts for automated piracy - Smart contracts can automate the distribution of pirated content without human intervention. This complicates enforcement efforts.

One of the Web3 applications is IPFS (InterPlanetary File System), a decentralized, peer-to-peer network similar to BitTorrent. Users of IPFS (acting as nodes) all hold a portion of the overall data making it difficult to track and remove pirated content. Some of the known examples of pirate platforms utilizing IPFS are Library Genesis and Anna's Archive. By using IPFS they can make sure content remains accessible despite takedown efforts.

Some of the mitigation strategies for dealing with these new piracy threats could be the development of legal and regulatory frameworks, as proposed by the European Commision[14], to address the challenges posed by decentralized networks. Another method could be the development of content recognition technologies to detect pirated material. Also the blocking of illegal websites offering (hyperlinks links to) copyright protected content using IPFS is a method to reduce damages. This is what BREIN has done with Library Genesis and Anna's Archive.

* * *

[14] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-blockchain