



FIGHTING PIRACY WITHOUT BREAKING THE INTERNET

To combat online piracy, such as illegal football streams, governments and rightholders increasingly rely on blocking measures based on Internet Protocol (IP) addresses and the Domain Name System (DNS).

Yet these tools are blunt, they cannot reliably distinguish illegal from lawful content. IP address blocking inevitably results in the disruption of legitimate services delivered via content delivery networks (CDNs) or shared web hosting, for example. Ultimately this impacts many services and users who have nothing to do with piracy, including those using virtual private networks (VPNs).

Moreover, blocking fails to remove illegal content from the internet. It merely hides one route to it, instead of addressing the problem at the source. Pirates also adapt quickly, shifting to new IP addresses or domains.

WHY BLOCKING DOESN'T WORK

Process



Outcomes

Blocking may interrupt traffic to an illegal stream briefly, but it also disrupts legitimate services, burdens neutral intermediaries, and does not tackle piracy in the long term.



1. PIRATES EVADE INSTANTLY, SUPPLY IS UNAFFECTED

Illegal streams reappear under new domain names or IP addresses that constantly rotate, leaving the overall scale of piracy unchanged.



2. USERS LOSE ACCESS TO LAWFUL SERVICES

Because blocking targets shared infrastructure, hundreds of unrelated websites and services are disrupted at the same time.



3. NEUTRAL INTERMEDIARIES IN IMPOSSIBLE POSITION

CDN, DNS, and VPN providers face liability, for both failing to block quickly and for overblocking lawful content. Moreover, obliging VPNs to enforce copyright undermines the privacy-by-design and cybersecurity of the VPN ecosystem.

HOW IP & DNS BLOCKING MISS THE REAL PROBLEM



IP BLOCKING INCORRECTLY ASSUMES ONE IP ADDRESS EQUALS ONE WEBSITE

In reality, modern web hosting providers, or CDN services, place thousands of unrelated websites and services behind the same IP address or load balancer. Blocking one address cuts access to all.



DNS BLOCKING CANNOT DISTINGUISH BETWEEN DOMAINS & SUBDOMAINS

Many legitimate services assign subdomains to individual users (such as user321.example.net). DNS blocking affects all associated subdomains and services – including lawful services that have no connection to piracy.

3 NEXT STEPS TO FIX EU PIRACY ENFORCEMENT



1. TARGET PIRACY NETWORKS AND STRENGTHEN ENFORCEMENT

- ▶ **Focus enforcement** on 'Piracy-as-a-Service' providers, payment gateways that knowingly process illegal IPTV fees, and advertisers.
- ▶ **Equip law-enforcement, courts, and regulators** with the resources, training and expertise to disrupt piracy networks.
- ▶ **Ensure fast redress and clear liability protections** to address accidental overblocking and to maintain accountability across the enforcement chain.



2. ENFORCE THE DIGITAL SERVICES ACT (DSA) PROPERLY

- ▶ **Boost cross-border cooperation** and respect DSA procedures, avoiding unilateral action against services established in other Member States.
- ▶ **Ensure enforcement orders issued by national authorities** strictly adhere to the conditions set out in DSA Articles 8 and 9 on illegal content.
- ▶ **Uphold the 'country-of-origin' principle** to prevent extraterritorial overreach and maintain legal certainty.



3. SUPPORT MARKETS AND COOPERATION

- ▶ **Improve access to affordable legal content** for consumers, and increase transparency, through industry dialogue.
- ▶ **Launch European Commission-led cooperation** among sports organisers, broadcasters, and intermediaries to effectively curb online piracy.
- ▶ **Establish a dedicated Member State network**, building on the EUIPO Observatory, to share best practices and minimise overblocking.

About CCIA Europe

The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and internet industry firms.

As an advocate for a thriving European digital economy, **CCIA Europe has been actively contributing to EU policy making since 2009.**

CCIA's Brussels-based team seeks to **improve understanding of our industry and share the tech sector's collective expertise**, with a view to fostering balanced and well-informed policy making in Europe.



Visit us at



ccianet.eu



x.com/CCIAEurope



linkedin.com/showcase/cciaeurope

CCIA Europe
Rue de la Loi 227, first floor
1040 Brussels • Belgium