

26 September 2025

The Director-General,
Department of Communications and Digital Technologies (DCDT)
iParoli Office Park
1166 Park Street
Hatfield
Pretoria
0001

Per Email: fwpsa2025@dcdt.gov.za

RE: Anti-Piracy Coalition (APC) submission on The Draft White Paper on Audio and Audiovisual Media Services and Online Safety.

Introduction

The Anti-Piracy Coalition (APC) is comprised of members of the industry that aim to:

- Establish a legal and operational framework to block pirate websites and protect intellectual property.
- Forge a mutual understanding with policymakers to prevent the abuse of South Africa's ICT networks.
- Ensure cooperation among industry players to facilitate a mutual operating environment to ensure adherence to copyright laws and IP rights ownership.

APC is supported by a strong network of industry leaders. Its founding members are the Department of Communications and Digital Technologies (DCDT) and the Companies and Intellectual Property Commission (CIPC), supported by the Music Publishers Association of South Africa (MPASA), the Publishers Association of South Africa (PASA), the Recording Industry of South Africa (RISA), Publishing SA, Sheer Music Publishing, Animation SA, and the Independent Producers Organisation (IPO).

Their collective involvement adds weight, insight, and industry alignment to APC's mission.

The APC recently convened a workshop on Digital Safety to gather the opinions and views of industry on the Draft White Paper on Audio and Audiovisual Media Services and Online Safety which took place on 23 September 2025 to enhance collaboration and forging ways to work together with role players to highlight the need for regulatory reform to tackle issues that relate to digital safety and digital safety awareness.

Submission

The Anti-Piracy Coalition (APC) thanks the Department of Communications and Digital Technologies (DCDT) for the opportunity to provide comments on the Draft White Paper on Audio and Audiovisual Media Services and Online Safety as published on 10 July 2025. APC is supported by a strong network of industry leaders, including the Music Publishers Association of South Africa (MPASA), the Publishers Association of South Africa (PASA), the Recording Industry of South Africa (RISA), Publishing SA, Sheer Music Publishing, Animation SA, Darlo Media Group, and the Independent Producers Organisation (IPO). Their collective involvement adds weight, insight, and industry alignment to APC's mission.

APC is a staunch advocate for the imperative integration of robust protocols within the legal framework governing electronic communications. Specifically, the APC champions the embedding of mandatory site-blocking mechanisms directly into the amendments of the Electronic Communications and Transactions Act 25 of 2002 (ECTA). This proposed amendment is seen as a crucial step towards creating a more secure and regulated online environment, particularly in combating the proliferation of illegal and harmful online content.

The rationale behind this advocacy stems from a comprehensive understanding of the challenges posed by illicit online activities, including but not limited to intellectual property infringement, cybercrime, and the dissemination of objectionable material. By entrenching mandatory site blocking within ECTA, the APC believes that South Africa can establish a clearer and more enforceable legal basis for internet service providers (ISPs) to restrict access to websites identified as engaging in or hosting illegal content. This would empower authorities with a more effective tool to combat online wrongdoing, moving beyond reactive measures to a more proactive and preventative approach.

Furthermore, the APC emphasises that any such implementation must be accompanied by stringent safeguards and clear definitions to prevent abuse and ensure that fundamental rights, such as freedom of expression and access to information, are not unduly compromised. This would necessitate a transparent and accountable process for identifying and blocking sites, likely involving judicial oversight or an independent regulatory body. The APC's position is therefore not merely about censorship, but about establishing a balanced and effective legal framework that protects users and rights holders while upholding democratic principles in the digital sphere.

The proposed amendments to ECTA, therefore, represent a significant opportunity to modernise South Africa's digital governance in response to the evolving landscape of online threats and opportunities.

By allowing the industry to take the lead, APC believes a more responsive, adaptable, and relevant regulatory environment can be fostered, one that truly understands the intricacies and evolving nature of digital piracy and distribution. This industry-led model would also promote innovation by avoiding overly rigid or prescriptive interventions that currently exist.

A recent proposal advocating for the establishment of an ombudsman has been put forward, with the primary objective of bridging the existing legislative void. This gap, it is argued, has emerged due to the rapid, exponential growth in digital platforms and services that are currently not adequately addressed by prevailing legislation. However, this perspective, while well-intentioned, presents significant practical challenges, particularly in the context of fostering a truly self-regulating environment.

The creation of such an ombudsman could inadvertently hinder the agility and adaptability required to effectively manage cutting-edge technology and to implement timely measures addressing the burgeoning concerns of digital safety and security. A self-regulating framework, by contrast, would empower the industry to rapidly develop and deploy solutions tailored to the evolving digital landscape, rather than being constrained by the slower, more rigid processes often associated with legislative oversight.

Furthermore, the practical implementation of an ombudsman mechanism presents considerable hurdles, primarily due to the substantial financial responsibility involved in its initiation and ongoing operation. Establishing a new regulatory body, complete with the necessary infrastructure, staffing, and operational mandates, would entail significant public or private investment.

This financial burden could prove to be a significant impediment, making it difficult to get such a mechanism off the ground and sustain its operations effectively. The inherent complexities and costs associated with establishing and maintaining such a body underscore the need for a more pragmatic and industry-led approach to address the dynamic challenges of digital governance.

The Broadcasting Complaints Commission of South Africa (BCCSA), operating as a statutory body under the auspices of the National Association of Broadcasters (NAB), serves as a compelling example of an effective industry-led self-regulatory framework. Its mandate extends to the comprehensive regulation of broadcast content, the diligent handling of violations, and the paramount assurance of audience safety and well-being.

The success of the BCCSA model, characterised by its efficiency and responsiveness, strongly suggests that a similar industry-driven approach would be highly advantageous for the regulation of content within the broader audio and audiovisual media services (AAVMS) realm. This expanded scope would encompass a diverse array of platforms and delivery mechanisms, including but not limited to traditional broadcasting, streaming services, on-demand content, and various digital media platforms in line with the evolving digital landscape in South Africa.

Implementing a comparable framework for AAVMS would offer several key benefits. This would, firstly, cultivate increased industry ownership and accountability, motivating content creators and distributors to adhere to stringent ethical standards and best practices, as well

as ensuring compliance with the classification codes set by the Film and Publications Board (FPB). Secondly, such a model could be more agile and adaptable to the rapid technological advancements and evolving consumption patterns within the AAVMS landscape, as compared to solely government-led regulatory bodies, which often struggle to keep pace. Thirdly, it could provide a more efficient and cost-effective mechanism for addressing complaints and resolving disputes, thereby reducing the burden on state resources. Finally, by involving industry stakeholders directly, it can promote a sense of shared responsibility for maintaining content quality, protecting vulnerable audiences, and ensuring a diverse and vibrant media ecosystem.

While entities like the Independent Communications Authority of South Africa (ICASA)'s Complaints & Compliance Committee (CCC) and the Information Communication Technologies and Media Regulators Forum (ICTMF) play crucial roles in regulating illicit online content, their current mechanisms may not fully address the complexities of the digital landscape. A more robust and formalised approach is needed to strike an effective balance between industry self-regulation and strict regulatory compliance.

One such potential solution lies in the implementation of "No-fault Site Blocking." This approach could offer a streamlined and efficient method for addressing the proliferation of harmful or illegal content online. Unlike traditional methods that often involve lengthy investigations and fault-finding, no-fault site blocking would focus on the immediate removal of access to content proven to be illicit, regardless of the intent or culpability of the content host. This mechanism could significantly reduce the time it takes to mitigate the spread of such material, thereby protecting users from its detrimental effects.

The benefits of no-fault site blocking extend beyond mere expediency. It could foster a more proactive environment for online safety, encouraging platforms and service providers to implement more stringent content moderation policies. Furthermore, by clearly defining the criteria for what constitutes "illicit content" and establishing a transparent process for site blocking, this approach could provide much-needed clarity for both content creators and consumers.

However, the implementation of no-fault site blocking also necessitates careful consideration of potential challenges. Safeguards must be put in place to prevent overreach and ensure that legitimate content is not inadvertently blocked. This includes establishing independent oversight bodies, providing clear avenues for appeal, and regularly reviewing the effectiveness and fairness of the blocking mechanisms. A nuanced approach that prioritises human rights, freedom of expression, and due process will be essential for the successful and ethical deployment of such a system. Ultimately, no-fault site blocking represents a promising avenue for strengthening online governance and creating a safer digital environment for all South Africans, complementing existing regulatory frameworks and adapting to the evolving nature of online threats.

No-Fault Site Blocking

Site blocking is a mechanism that is utilised to restrict access to copyright-infringing material, protect minors from adult content and also protect national security through the establishment of protocols that are essential to balance the freedom to access information and also the ability to curb piracy facilitated by carrier networks, internet service providers (ISPs) and other intermediaries.

No-fault site blocking is a measure which APC strongly advocates for in that service providers are not held legally at fault for the blocking of access to websites that house pirated content and copyright-infringing materials, and is solely dependent on the voluntary participation of ISPs, right holders and other stakeholders.

No-fault site blocking is premised on a successful track record in the 60+ countries in which it is in place as it has been proven to decrease the number of users that access pirate host websites thereby stopping large-scale online infringements and also enables rightsholders to seek remedy for infringements without assigning “blame or fault” from intermediaries that are best positioned to enable for the halting of such activities.

No-Fault site blocking can take two forms: Dynamic Site Blocking and Domain Name System (DNS) Filtering, which will be explained more extensively below.

Dynamic Site Blocking

Dynamic site blocking represents the most advanced and preferred method for combating online content infringement. This adaptive approach is particularly effective in addressing the rapid dissemination of pirated content, especially for live broadcasts such as sporting events or newly released audiovisual material. Its key advantage lies in its ability to update and modify blocking measures without the need for fresh judicial or administrative proceedings for each new instance of infringement. This agility is crucial in an environment where pirate sites frequently change their hosting or domain names to evade detection.

The application of dynamic site blocking has seen significant expansion, now extending to Content Delivery Networks (CDNs) and Domain Name System (DNS) resolvers. This broader scope allows for more comprehensive and effective disruption of illicit content distribution channels. CDNs, which are networks of servers that deliver content to users based on their geographical location, are often exploited by pirates to ensure high-quality streaming. By targeting CDNs, enforcement agencies can cut off the supply of pirated content at a critical point in its delivery chain. Similarly, blocking at the DNS resolver level prevents users from even being able to resolve the domain names of infringing websites, effectively making them inaccessible.

The European Union (EU) Commission has been a strong proponent of dynamic site blocking, recognising its potential to significantly enhance copyright enforcement across member states. This commitment is evidenced by the release of two key recommendations that underscore the urgent need for EU member states to adopt these sophisticated tools. These recommendations serve as a clear directive, encouraging national governments to integrate dynamic site blocking mechanisms into their legal and technological frameworks.

Among the EU member states, Greece and Spain have emerged as frontrunners in the adoption and implementation of effective dynamic site blocking mechanisms. Their proactive approach in developing and deploying these tools provides valuable case studies and demonstrates the tangible benefits of such systems. These countries have successfully navigated the legal and technical challenges associated with dynamic blocking, setting a precedent for other nations to follow. Their experiences highlight the importance of legislative support, collaboration between rights holders and internet service providers, and continuous technological innovation to ensure the ongoing effectiveness of these anti-piracy measures.

DNS Filtering

This process leverages a Domain Name System (DNS) to proactively safeguard users from malicious online threats and filter out harmful or inappropriate content. At its core, a DNS resolver acts as an intelligent filter, meticulously delisting flagged websites that have been added to a comprehensive blocklist. This blocklisting extends to web properties, identifying and restricting access by both domain name and IP address.

This method is considered highly effective because it prevents the DNS resolver from successfully resolving queries for flagged content. In essence, the resolver simply does not look up or provide the necessary information to access these blacklisted domains. As long as these domains remain on the blocklist, access to them is disallowed, creating a robust and preventative barrier against undesirable or dangerous online content. This approach not only blocks access but also significantly reduces the risk of accidental exposure to malware, phishing attempts, or other cyber threats, thereby enhancing overall online security for users.

Recommendation

Site blocking represents a critical objective in the ongoing effort to establish a more secure and responsible digital environment. Its implementation is essential for fostering the widespread adoption of policies that are not only universally accepted but also demonstrably enforceable. This is particularly crucial in areas where a uniform consensus has emerged regarding the necessary measures to ensure digital safety and awareness for all users.

The urgency for effective site blocking mechanisms is underscored by the current legislative landscape. Existing laws, largely conceived in an earlier digital era, frequently lag behind the

rapid advancements and evolving complexities of the modern digital economy. This disconnect creates significant vulnerabilities and makes it challenging to adequately protect individuals and organisations from various online harms. Therefore, it is imperative to amend and update current legislation to align it with the realities of the contemporary digital world. This modernisation should specifically address the need for robust site blocking capabilities, ensuring that legal frameworks are sufficiently agile to respond to emerging threats and technological shifts. By doing so, we can create a more resilient and protective digital space that promotes innovation while safeguarding users.

The Anti-Piracy Coalition (APC) firmly believes that no-fault site blocking represents the most effective form of creating a digitally safe environment on the internet. This pioneering approach will protect our sovereign ICT infrastructure and safeguard investments into the creative economy.

Furthermore, the APC contends that the establishment of an ombudsman is not necessary. The rationale behind this stance is the strong and sufficient support already present within the industry for self-regulation. This internal commitment ensures not only compliance with all statutory requirements but also goes above and beyond their existing licensing obligations. This approach fosters a proactive and responsible industry environment, where members are empowered to uphold high standards of conduct and accountability without the need for external oversight.