ISPA Position Paper on Internet Blocking

(Version 1.1, 2026-04-10)

1. Introduction

Internet service providers (ISPs) play a critical role in making information available to the public. All South Africans connect to the internet via an ISP, whether that be a commercial ISP, a mobile network, an academic network, or a community network. This places ISPs in a unique position when it comes to *preventing* members of the public from accessing specific content. In short, it is possible (with limitations) for ISPs to block users of their network from accessing some of the content available on the internet.

Globally, ISPs face pressure to block content from many sides. Commercial enterprises want ISPs to block sites that infringe their intellectual property rights. Gambling regulators want ISPs to block sites that do not hold licences to operate in their jurisdiction. Law enforcement authorities want ISPs to block sites that host illegal content, such as child sexual abuse material or terrorist and violent extremist content. In some countries, governments force ISPs to block dissenting political views.

There are a number of different technical ways to implement blocking, varying from domain name blocking and Internet Protocol (IP) address blocking to deep-packet inspection. All blocking, by definition, has an impact on the users of a network, disrupting their normal service. Many types of blocking can be circumvented by end-users using Virtual Private Network (VPN) technologies or similar. Some types of blocking may have unintended consequences, preventing access to content other than the intended target of the block. All blocking has cost implications for ISPs, either an administrative cost, and/or a cost to procure, install and operate equipment required to do the blocking. Blocking may also have a negative impact on network performance.

2. Goal of this document

ISPA is a representative body representing more than two hundred ISPs. While there are currently no requirements in South Africa for ISPs to block content, more than fifty countries now have legislation providing for some form of internet content blocking. Given this, it would be naïve for ISPA to assume that there will never be such obligations put in place in South Africa. It would also be imprudent for ISPA to take a position that ISPs should *never* block content, since there are some forms of content, such as child sexual abuse material, for which there is near unanimous societal support for blocking. Therefore, the goal of this document is to set out a reasonable position on internet blocking for ISPs to take — one that balances the need to block some content against the impact on internet users and ISPs and which takes cognisance of the rights enshrined in the South African Constitution.

3. Current South African legal framework

There are currently no general obligations in South African law for ISPs to block content. Absent a court order, an ISP does not have to accede to any request to block internet content. Notwithstanding this lack of general blocking obligations, some legislation is pertinent.

3.1. The Constitution

South African Constitution is one of the world's most progressive and the Bill of Rights contains several pertinent sections:

- The right to **privacy** includes the right not to have the privacy of communications infringed.
- The right to **freedom of expression** includes the freedom of the press and other media, and the freedom to receive or impart information or ideas. This right is expressly constrained, but those constraints are limited to:
    - propaganda for war,
    - incitement of imminent violence, and
    - advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm.
- The right of **access to information**, specifically any information held by the state and any information that is held by another person and that is required for the exercise or protection of any rights.
- A **limitation of rights** is permitted only to the extent that the limitation is reasonable and justifiable in an open and democratic society, taking into account factors which include whether there are less restrictive means to achieve the purpose.

3.2. The Electronic Communications and Transactions Act (No. 25 of 2002) ("**ECTA**")

The ECTA contains several provisions that are of direct relevance to ISPs, as providers of information systems:

- The **mere conduit** provisions in section 73 makes it clear that a service provider is not liable for providing access to third party information systems, but provides for a competent court to order a service provider to prevent unlawful activity in terms of any other law.
- The **take-down notification** process in section 77 (read with section 75) sets out a framework for a service provider to remove or disable access to unlawful content hosted on its network. This process targets content on the network of the service provider, whereas blocking targets content on third-party networks, not under the control of an ISP. The existing take-down notification process is effective; through its members, ISPA removes hundreds of reportedly unlawful websites from the South African internet each year.
- Section 78 states that a service provider has **no general obligation to monitor** the data which it transmits or stores, or to actively seek evidence of an unlawful activity.

It is worth noting that in 2023, the South African Bookmakers' Association (SABA) approached ISPA with a legal opinion that section 11 of the National Gambling Act (No.

7 of 2004) — which states that: "a person must not engage in or make available an interactive game except as authorised in terms of this Act or any other national law" — placed an obligation on ISPs to block unlicensed gambling sites and that the failure to do so was an offence (as set out in section 82(1) of the National Gambling Act).

ISPA subsequently obtained its own legal opinion which comprehensively refuted this argument and noted that failing to voluntarily block a website is not the same as "making available" an interactive game. An interpretation of the National Gambling Act read with the ECTA that best conforms with the Constitution is one in which ISPs retain their status as mere conduit providers, subject only to ECTA s73(3) and s79(c) which provides for a court to order a service provider to prevent unlawful activity in terms of any other law.

3.3. The Regulation of Interception of Communications and Provision of Communication-Related Information Act (No. 70 of 2002) ("**RICA**")

The RICA goes one step further than ECTA in that it expressly prohibits the monitoring of communications:

- Section 2 contains a general **prohibition of interception of communication**, which states that no person may intentionally intercept or attempt to intercept any communication in the course of its occurrence or transmission, except as provided for in RICA.
- Importantly, the definition of intercept in RICA includes the monitoring of any communication. RICA thus limits the ability of an ISP to interfere with its customers' communications with a website or other internet content.

3.4. The Cybercrimes Act (No. 19 of 2020)

The Cybercrimes Act adopts and confirms the ECTA approach. Reporting obligations imposed by section 54 of that Act must not — subject to any other law or obligation — be interpreted to impose obligations on ISPs to:

- Monitor the data which it transmits or stores, or
- Actively seek facts or circumstances indicating any unlawful activity.

4. Technical approaches to blocking

This document does not attempt to provide an exhaustive analysis of the many different ways that internet blocking can be technically implemented. However, a high-level view of the main approaches is useful to provide context to any discussion of content blocking.

4.1. Domain name blocking

Websites and other internet content is often accessed via the domain name system (DNS). This is essentially a directory mapping a domain name ("www.ispa.org.za" for example), to a particular content server on the internet. When an end-user types a domain name in a web browser, their device typically queries their ISP's domain name resolver to locate that website.

The simplest form of content blocking is to interfere with domain name requests for sites that are to be blocked. The domain name requests simply fail with no explanation.

Some implementations of domain name blocking attempt to send the user to an alternative site, to provide an explanation for the blocking of the original site. This is only feasible for insecure (http://) sites, and cannot be done for secure (https://) sites without forcing the user to ignore warnings of invalid certificates. It must therefore be assumed that any domain name blocking will not provide clear feedback to the user that the site is being blocked.

Domain blocking is relatively easy for ISPs to implement and has minimal cost implications. However, end-users are not required to use the domain name resolvers of their ISPs and can easily configure their devices to use an alternative open resolver that does not have the block in place. The fact that a blocked domain will appear to be a technical problem with the domain could even incentivise technically proficient users to move to alternative domain name resolvers to access the blocked site.

Blocking a single domain blocks users from accessing the content at that particular domain, so the risk of unintentionally blocking other content is low. However, blocking a domain blocks *all* of the content at that particular domain. Thus, blocking "docs.google.com" will prevent an end-user from accessing *all* documents hosted by Google, and cannot block only a single problematic document.

Pros	Cons
• Easy and low-cost for ISPs to implement • Unlikely to accidentally block unrelated sites	• Extremely easy for end-users to circumvent

4.2. IP address blocking

Hidden behind the domain name system are Internet Protocol (IP) addresses. These are numbers that look like this: 196.10.55.0 (IPv4) or 2001:43f8:1f5:: (IPv6). When an end-user's device queries a domain name resolver, the resolver responds with the IP address identifying the server hosting the content in question.

In a similar way that an ISP can block a domain name query for a particular domain, it is possible to block a user on the ISP's network from exchanging traffic with a particular IP address. Exactly how this is done depends on the architecture of the operator's network, which means both the cost and the complexity of implementing IP address blocking varies considerably. Most ISPs will be able to redirect a request to a blocked IP address to an alternative site (to notify the user that that site is blocked), but in some cases doing so would involve significant more effort than having the connection silently fail.

As with domain name blocking, IP address blocking is relatively easy for end-users to circumvent by installing a Virtual Private Network (VPN). The target website can also change its IP address (without having to change the domain name), to avoid IP address blocks.

The most significant concern with IP address blocking is the unintended blocking of other websites. Particularly for cloud hosting situations, but even for simpler web server configurations, one IP address can be used for multiple, unrelated web sites. Since blocking that IP address blocks a user from accessing that particular server

entirely, this form of blocking frequently has the unintended consequences of blocking innocent websites.

Pros	Cons
● Low to medium cost for ISPs to implement ● Low to medium complexity for ISPs to implement.	● Extremely easy for end-users to circumvent ● Significant risk of accidental overblocking ● Blocked sites can change their IP addresses to avoid blocks

4.3. Packet inspection

A third, far more invasive mechanism for blocking requires that ISPs inspect each packet of data generated by an end-user. The data packet is examined for a particular Uniform Resource Locator (URL) and if this matches a blocked site, the packet is not routed.

Packet inspection requires specialised, costly equipment and because every packet of data on the network must be inspected, it also has a negative impact on network performance. This impact increases with the number of sites that must be blocked. Shallow packet inspection examines only the portion of the data packet which typically contains the address of the content server, while deep packet inspection examines the entire contents of the data packet.

Some forms of packet inspection can be bypassed by websites that use end-to-end encryption (https://) since only part of the URL (the domain name) or the Server Name Indication (SNI) is visible during the initial Transport Layer Security (TLS) negotiation. While blocking this initial negotiation can result in a successful content block, there are more secure technologies such as Encrypted SNI being rolled out which prevent most forms of packet inspection from successfully blocking content.

Shallow packet inspection can be bypassed by an end-user using a VPN. Deep packet inspection can prevent the use of VPNs as a bypass mechanism, but in order to do so, the system must essentially entirely block the use of particular VPNs, thus preventing end-users from using those VPNs entirely (even for completely legitimate purposes). End-users can still bypass even deep packet inspection by making use of alternative VPNs (ones that aren't blocked) or configure blocked VPNs to use different ports that are not blocked.

Pros	Cons
● Harder for end-users to bypass than domain or IP address blocking.	● High cost and complexity for ISPs to implement. ● Requires examination of the contents of end-user communications. ● Can still be bypassed by determined end-users.

5. Approaches in other jurisdictions

In jurisdictions which have legal frameworks in place for internet blocking, the majority require the party seeking to have content blocked to approach a court to obtain the blocking order. A smaller number have a framework in which a regulatory or administrative body (not a court) issues a blocking order. A few countries have a voluntary blocking approach, where ISPs voluntarily block sites, typically those identified by rights-holder organisations.

Most countries with blocking legislation implement static blocks, with the site to be blocked identified in the original blocking order. If the site moves to a different domain then the requesting party must seek a fresh blocking order with the new details. A smaller number of jurisdictions provide for a dynamic blocking order, which permits the requesting party to amend the block if the content provider moves the content to a different location without approaching the court (or regulator) anew.

6. A proposed approach for South Africa

ISPA supports the following approach for internet blocking in South Africa:

6.1. Judicial legal framework

ISPs should not engage in any blocking voluntarily. All blocking obligations should be clearly set out in an appropriate legislative framework, and be subject to appropriate oversight and judicial review.

Since internet censorship by its nature involves interfering with fundamental constitutional rights, blocking requests should be judicial in nature, rather than administrative. Any request to block internet content should be directed by an applicant to either a court or a designated judge (in a similar manner to that established in RICA) rather than issued by an administrative body.

The principle of less restrictive means of achieving the purpose, as enshrined in the Bill of Rights, must apply to any blocking obligations. A request to block content should only be granted if there is no less restrictive means of preventing access to that content.

There must be a clear, expeditious and impartial appeal process available to both internet users and the content providers who believe that a blocking request has been granted in error.

Any variation of a blocking order should be subject to judicial oversight.

ISPA notes that several jurisdictions have developed expedited and flexible processes for courts to issue blocking orders:

Australia	Under section 115A of the Copyright Act 1968 the rights-holder applies to the Federal Court of Australia for an injunction requiring carriage service providers to take reasonable steps to disable access to an online location outside Australia whose primary purpose or primary effect is to infringe or facilitate infringement of copyright. These orders typically take a few weeks to a few months to obtain.
India	The Indian High Court has developed a procedure under the Copyright Act 1957 under which rights-holders apply to the High Court for injunctions against rogue websites. The procedure includes a dynamic injunction mechanism: the initial order identifies specific URLs/domains, and the court permits the applicant to return on a simplified basis to extend the order to mirror sites and alphanumeric variants without a full fresh hearing.
United Kingdom	Under section 97A of the Copyright, Designs and Patents Act 1988 the rights-holder applies to the High Court for an injunction requiring ISPs to block access to specified websites. The process has become operationally streamlined — applications are typically made on notice to the ISPs (who generally do not oppose if the legal threshold is met), with supporting technical evidence. Orders can be obtained within weeks.

6.2. Mandatory public disclosure

Any blocking obligations on ISPs should be transparent, and subject to public scrutiny. Citizens whose access to information and freedom of expression rights may be infringed by mandated blocking of content by ISPs should know the extent to which those rights are being limited.

Where technically feasible, ISPs required to block access to content should redirect end-users to information setting out the legal basis for the block.

6.3. Time-limited measures

All blocking measures should be temporary and subject to periodic review to ensure that they remain relevant, necessary and proportionate.

6.4. Blocking should not require network modification

Content blocking orders should not dictate the method used by an ISP to block that content, and should not require an ISP to install additional equipment on their network to be able to implement a block. An ISP should be required to implement a block to the best of its ability within the technical constraints of its network.

The technical method of blocking must also be consistent with a less restrictive means approach. ISPs should never be required to block additional, unrelated sites in order to execute a blocking order.

6.5. Fair allocation of costs

The costs of any blocking obligations should be fairly allocated. ISPs must not be left out-of-pocket as a result of implementing mandatory blocking of content. Equally, ISPs must not profit by charging fees for blocking requests that are higher than the cost of executing such requests. ISPs should be entitled to levy an administrative fee to implement a block, but this should be limited to the cost to the ISP for putting the block in place.

There is some international precedent on blocking costs. In Cartier International AG and other v British Telecommunications Plc and another, the UK Supreme Court confirmed that courts have jurisdiction to order ISPs to block websites infringing trade marks (not only copyright), but held that rights-holders generally bear the implementation costs.

7. Version notes

Version 1.1	2026-04-10	Added examples of expedited court processes in other jurisdictions. Added UK precedent on responsibilities for the costs of blocking. Clarified that redirecting to alternative sites when blocking domains is not possible for secure sites. Added more detail on the limitations of packet inspection for secure sites.
Version 1.0	2026-02-13	Initial release.