July 2026

ISOC Brasil Contribution to the Internet Society Community Consultation on VPN Restrictions Policy Brief

Internet Society
Capítulo Brasil

Prepared by

Thobias Prado Moura

João Moreno Rodrigues Falcão

José Arthur Alves

Pedro Amaral

Bruno Marcolini

Luiza Dutra

Gustavo de Oliveira Ferreira

Executive Board

Table of Contents

1. Introduction

The Internet Society Brazil Chapter (ISOC Brasil) welcomes the opportunity to comment on the draft "VPN Restrictions" Policy Brief. The draft addresses a subject that has moved, over the past two years, from the margins of technical policy to the centre of legislative and judicial debate in several jurisdictions, including Brazil. Its central proposition, that virtual private networks are general-purpose security technologies and that restricting them weakens user protection without addressing the underlying harms, is sound and well supported.

The comments below are organised around the four blocks of the consultation questionnaire. Sections 3 to 5 respond to the questions on clarity, terminology, balance and the quality of the principles and recommendations. Section 6 gathers further observations on points where the Chapter believes the draft could be strengthened beyond what the questionnaire expressly asks. Sections 7 and 8 respond to the regional/local and additional-insights blocks, respectively, using Brazilian material not as a request for localisation but as evidence of a pattern likely to recur elsewhere. Section 9 consolidates the proposed amendments in tabular form, and section 10 concludes.

For the record, the Chapter's answers to the scaled questions of the questionnaire are as follows. On whether the brief is clear and informative overall, the Chapter selects "Clear and informative". On how relevant and useful the brief is for policy discussions in the region, the Chapter selects "Relevant". The reasons for not selecting the highest option in either case are set out in the sections that follow, and each of them is addressed by a specific proposal for amendment.

2. About ISOC Brasil

ISOC Brasil is the Brazilian chapter of the Internet Society, with more than 1,200 members throughout the country. Its membership is plural and multistakeholder, bringing together the technical community

involved in the development and operation of the Internet, businesses involved in Internet infrastructure and digital services, academic communities across different fields, and civil society organisations concerned with the Internet's social and economic impacts.

The Chapter maintains standing working groups on encryption, intermediary liability, meaningful connectivity and digital sovereignty. These comments were prepared within that institutional structure and draw on the Chapter's participation in the Brazilian legislative and regulatory processes described in section 7.

3. Clarity and terminology

The Internet Society Brazil Chapter considers that the draft already uses technically accurate language to explain how virtual private networks work and why they matter for security, privacy and trust online. Even so, a small number of terms could be adjusted so that the brief speaks more directly to current regulatory debates, particularly now that these tools are discussed not only as technical artefacts but also in debates over platform regulation, age assurance, online safety enforcement and the circumvention of platform blocks and other access restrictions.

3.1 Connecting technical properties to protected legal interests

Expressions such as encrypted tunnel, confidentiality, integrity and authentication are accurate and helpful, since they situate virtual private networks within the security architecture of the Internet rather than treating them as inherently suspicious. The draft would gain from linking these technical terms more explicitly to the legal interests they protect. Where it refers to confidentiality, integrity or privacy, it could note that these properties also enable the exercise of rights such as data protection, freedom of expression, access to information and the physical safety of users at risk.

This addition would strengthen its global usefulness, making clear that restrictions on these tools affect both network security and the broader conditions under which people communicate, seek information and protect themselves online. It would also give legislators a vocabulary in which to express the constitutional dimension of measures that are frequently drafted as though they concerned nothing more than a technical detail of enforcement.

3.2 Terms to add or clarify

The draft would benefit from a small number of terms now recurring in legislative and judicial debate, which would help policymakers recognise the categories of measures under discussion across jurisdictions:

- penalty enhancements for the use of anonymisation tools, under which virtual private networks, proxies or address-masking techniques are treated as aggravating factors in criminal or regulatory schemes;
- third-party punishment, under which sanctions fall on users, intermediaries or providers of security tools rather than on the underlying unlawful conduct;
- age assurance based on sensitive data, under which age verification or estimation relies on official documents, biometric data or behavioural analysis, creating new privacy and security risks.

Incorporating these terms would let the draft engage directly with live policy proposals while preserving its broader analytical structure. They are descriptive and name the mechanism at issue rather than the political intention behind it, which makes them usable by policymakers who do not share the Chapter's conclusions.

3.3 A more precise taxonomy of restrictive measures

The draft would also gain from more precise language describing the restrictions at issue. The three current categories are useful, but they group together measures that differ substantially in their technical

implementation and in the legal questions they raise. The brief could distinguish, for instance, between network-level blocking of virtual private network traffic; app-store removal, licensing or registration schemes imposed on providers; mandatory logging, data-retention or interception obligations imposed on providers; and sanctions imposed on end users for the use of these tools in particular contexts.

The distinction matters because each measure raises different questions of feasibility, proportionality, collateral effects and human rights impact. Network-level blocking is indiscriminate and technically fragile; licensing schemes operate as barriers to entry and tend to consolidate the market around providers willing to accept surveillance obligations; retention mandates transform a privacy tool into a repository of exactly the data it was designed not to keep; and sanctions on users shift the burden of enforcement onto the population the policy claims to protect.

4. Balance of the diagnosis

The Chapter considers that the draft offers a largely balanced treatment of the issue. It recognises that policymakers face legitimate concerns, including the protection of children online, the enforcement of platform rules, the investigation of crime and the response to harmful content and abuse, while distinguishing those underlying problems from the general-purpose security tools that are sometimes targeted instead of the harmful conduct itself. That balance could be reinforced in two respects.

The first is a more explicit recognition of the goals and constraints under which policymakers operate. The draft already notes that governments face complex challenges around online safety, child protection and digital regulation. It could go further by acknowledging that some of these frameworks respond to international obligations and to sustained social pressure to act on serious harms. Making this explicit shows that the document understands the political and institutional context surrounding restrictions, even while arguing that such restrictions are frequently misguided and ineffective.

The second is a clearer articulation of the risk of misdirected measures. The draft rightly emphasises that banning, limiting or surveilling virtual private networks does not address the root causes of online harms and weakens security, privacy and trust in the process. The argument would be stronger if it clarified that the problem is not that policymakers are acting, but that some proposals act upon the wrong object. Treating security and anonymisation tools as an aggravating factor in criminal law, or sanctioning individuals for circumventing platform blocks, shifts attention away from harmful conduct and onto neutral tools on which most users rely for protection.

In this sense, the draft's diagnosis is balanced. The objectives of policymakers are legitimate, but restrictions on virtual private networks are frequently misaligned with those objectives. The Brazilian episodes described in section 7 show how quickly a safety tool can be recast as suspicious, and a small number of concrete examples along these lines, without singling out any one country, would make that balance more evident. The brief is not opposed to tackling harms; it is concerned that measures should target those harms directly rather than undermine essential security and privacy infrastructure.

5. Principles and recommendations

The Chapter considers that the policy principles and recommendations are clear and concise, and that they convey the core message effectively. Virtual private networks are essential security and privacy tools; bans, mandatory surveillance and blocking obligations are harmful and often ineffective; and policy responses should address unlawful content and conduct at the source rather than the tools people rely on to protect themselves. They would become easier to implement with slightly more detail in the following respects.

5.1 Sanctions attached to the mere use of security tools

The principles could state more clearly that legal and regulatory frameworks should not attach penalties, or enhanced penalties, to the use of virtual private networks and other anonymisation tools as such.

Where proposals treat techniques to conceal address information as a generic aggravating factor, more precise guidance would help policymakers distinguish between targeting harmful behaviour and stigmatising tools on which most users rely for legitimate protection. This is not a hypothetical concern, as section 7.2 illustrates through a bill approved by Congress and awaiting presidential sanction.

5.2 Naming the categories of disproportionate measures

The recommendations could describe, in broad terms, which categories of measures are likely to be disproportionate or misaligned with the objectives stated for them, for example:

- blanket network-level blocking of virtual private network traffic;
- app-store removal or licensing schemes that effectively exclude reputable providers from a market;
- extensive periods of logging and data-retention mandates applicable to all users of a service;
- sanctions imposed on individuals for using these tools to access services subject to blocking orders.

Naming these categories provides policymakers with concrete reference points against which to assess draft laws and regulatory action, while giving civil society a shared vocabulary for responding to them.

5.3 Anchoring the alternatives in existing policy instruments

The draft recommends addressing unlawful content at its source and using less intrusive measures, including clear legal standards, user-controlled filtering and cooperation across jurisdictions. These suggestions would become more operational if briefly connected to instruments that are already in place in many jurisdictions globally, such as due process mechanisms, notice-and-action and takedown procedures with judicial oversight, data protection rules on minimisation and necessity, and multistakeholder cooperation in law enforcement and child protection. That link would help legislators see how to apply the recommendations within frameworks they already use, rather than treating them as external to existing regulatory practice.

The draft could also distinguish restrictions on access from measures aimed at provider trustworthiness. Concerns about unreliable or exploitative providers can be addressed through independent audits, transparency reporting and verifiable data-minimisation practices, rather than through bans or blanket licensing requirements.

5.4 A multi-scalar governance logic

The recommendations would gain conceptual clarity if organised around a multi-scalar governance logic, under which different regulatory problems belong to different institutional layers and call for different responses. Questions of unlawful content and of the accountability of specific actors are, first and foremost, matters of law enforcement and transnational cooperation. Questions of blocking, routing and network integrity are infrastructure matters. Obligations concerning identification, retention and monitoring of users belong to the domain of data protection, privacy and information security. This distinction finds support in the digital governance literature, which treats control, coordination, incentives and trust as related but analytically distinct governance mechanisms, each requiring its own design logic rather than a single undifferentiated instrument.[1]

A similar diagnosis appears in the platform governance debate, where controversies over whether certain actors should be treated as neutral intermediaries, content hosts or media companies turn on distinguishing the technical function performed from the harmful conduct that may run through it.[2] The governance of virtual private networks faces the same categorisation problem: treating an infrastructure-layer tool as though it were, by itself, the source of a content-layer or conduct-layer harm.

This logic also clarifies why many governments turn to restrictions in the first place. The reason is often not that a ban is the most precise or effective response, but that governments face limited digital

[1]HANISCH, Marvin; GOLDSBY, Curtis M.; FABIAN, Nicolai E.; OEHMICHEN, Jana. Digital governance: a conceptual framework and research agenda. Journal of Business Research, v. 162, 2023.

[2]FLEW, Terry; MARTIN, Fiona; SUZOR, Nicolas. Internet regulation as media policy: rethinking the question of digital communication platform governance. International Journal of Digital Television, v. 10, n. 1, p. 33-50, 2019.

investigative capacity, weak channels for international cooperation, or underdeveloped notice-and-takedown mechanisms. In these settings, restricting the tool functions as an institutional substitute for capacities that the state has not yet developed to address unlawful content, services or conduct at the source. Comparative research on regulatory maturity in digital governance supports the proposition that the mere existence of a law does not guarantee compliance or transformation unless it is matched by enforcement mechanisms, institutional capacity and technical infrastructure.[3] Countries at an early stage of regulatory maturity display precisely this pattern of institutional fragmentation and overlapping mandates, which prevents legislative ambition from translating into operational outcomes.

A recent study of cybercrime enforcement involving virtual private networks in Indonesia illustrates the same dynamic concretely, pointing to the absence of specific regulation, limited technical and forensic capacity, and weak coordination among the national police, the cybersecurity agency and the telecommunications ministry.[4] The study concludes that the real bottleneck lies in institutional capacity and inter-agency cooperation rather than in the absence of a specific prohibition, which reinforces the point that restricting the tool tends to be a weak substitute for investing in investigative capacity. Presenting this argument explicitly would allow the brief to answer, rather than merely reject, the question that policymakers are actually asking.

Overall, the principles sit at an appropriate level of generality, but a modest amount of additional detail, particularly on what should and should not be done in law and regulation, would make them easier to apply in practice, including in jurisdictions where virtual private networks are expressly named in bills and court decisions.

[3]JORDANOSKI, Zoran. The role of regulatory frameworks in shaping e-governance: insights from selected case studies. In: DG.O 2025 - 26th Annual International Conference on Digital Government Research, Porto Alegre, 2025.

[4]NUGROHO, Teguh; SOESATYO, Bambang. Problems of cyber law enforcement against cyber crimes using virtual private network technology in Indonesia. Jurnal Greenation Sosial dan Politik, v. 3, n. 4, p. 713-721, 2025.

6. Further observations on the draft

The following observations go beyond the questions expressly posed in the consultation. They are offered because the Chapter considers that the draft is well positioned to become a reference document for legislators and regulators, and that a limited number of additions would substantially strengthen its authority.

6.1 Anchoring in the international human rights framework

The draft argues from technical and consequential premises but does not invoke the international human rights standards that already address the question. The report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on encryption and anonymity states that encryption and anonymity enable the exercise of the rights to privacy and to freedom of expression and deserve strong protection, and that restrictions must satisfy the tests of legality, necessity and proportionality.[5] A short paragraph situating the argument within that framework would give legislators an external standard against which to measure draft laws, and would connect the brief to the extensive body of work on encryption, within which the governance of virtual private networks is a specific application.

6.2 Due process, transparency and effective remedy

The draft cites decisions of French and Spanish courts ordering providers to block lists of domains, and the Italian automated blocking system, but it treats them exclusively as illustrations of over-blocking. There is a second and equally important critique to be made. Depending on their procedural design, such orders may be issued in proceedings to which the affected providers, the operators of lawfully blocked services and the users are not parties; may be dynamic, in the sense that the list of targets can be

[5]UNITED NATIONS. Human Rights Council. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye. A/HRC/29/32, 22 May 2015.

expanded administratively after the decision; and may provide no accessible remedy to those whose lawful services are caught by the measure. A principle on due process, transparency and effective remedy would cover situations in which the substantive objective is legitimate but the procedure is not, and it would apply even in jurisdictions that reject the rest of the argument.

6.3 Prior assessment of impacts on the Internet

The Internet Society already maintains an analytical framework for assessing whether a given measure may affect the critical properties of the Internet and the enablers of trust, and it has applied that framework to comparable proposals.[6] The draft would gain from an express recommendation that measures capable of restricting virtual private networks be preceded by such an assessment, whether conducted by the proposing authority or by third parties. This converts a general appeal to proportionality into an identifiable procedural step, and it links the brief to an instrument that regulators can actually use.

6.4 Enterprise and consumer services and the limits of network-level blocking

The draft notes in a footnote that restrictions frequently exempt businesses and governments. That observation deserves to be developed in the body of the text, because such exemptions can be difficult or impossible to implement reliably at the network layer. Corporate remote access, consumer subscription services and the tunnelling used by banking, telemedicine and industrial control applications rely on the same protocols and, in many cases, on the same infrastructure. Measures that block traffic by protocol fingerprinting or deep packet inspection may be unable to distinguish reliably between the categories that the law purports to separate, meaning that an exemption drafted in legal terms may not survive technical implementation. This is one of the strongest arguments available to the brief, and it is currently only implicit.

[6]INTERNET SOCIETY. Internet Impact Assessment Toolkit. Available at: https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

6.5 The circumvention surface beyond virtual private networks

Where the draft addresses age assurance, it could observe that virtual private networks represent only one part of a broader circumvention surface. Shared or borrowed credentials and device sharing can bypass account-based age-assurance systems, while proxy services, encrypted name resolution and anonymity networks can circumvent certain network- or location-based restrictions. The empirical evidence on which methods predominate remains limited. A measure that addresses one vector while leaving the others untouched imposes its full cost on compliant users while achieving a marginal reduction in circumvention. Stated in those terms, the effectiveness argument does not depend on any contested premise about the value of privacy.

6.6 Distributional effects and the market for free services

The draft observes that restrictions drive users towards less reputable providers. The distributional dimension of that observation could be made explicit. Where reputable subscription services are removed from application stores or priced out of a market, the substitution is not neutral across income levels. Users who cannot access or afford reputable paid services may migrate to services that rely on monetising the very data the tool was meant to protect. This risk is greater in jurisdictions with weak data-protection enforcement. Restrictions can therefore redistribute security risk towards those least able to absorb it, which is a proposition that policymakers concerned with the protection of vulnerable users should find difficult to dismiss.

6.7 Evidence base and geographic balance

The examples in the draft are drawn almost entirely from Europe, North America and Asia. The absence of Latin American and African material weakens the claim that the phenomenon is global and reduces the usefulness of the document in those regions. The Chapter offers the Brazilian material in section 7 for that purpose and would be glad to assist in identifying comparable cases elsewhere in the region.

Two points of sourcing also deserve attention. Where the draft supports a central claim about the technical limits of VPN protection, it relies on a commercial technology publication, making the claim easier to challenge than if it were supported by independent research. Where it addresses trust in the Internet, it relies on survey data from 2019, which is now sufficiently dated that a reader may discount the conclusion. The Chapter also suggests moderating the assertion that concerns about circumvention by minors may be unfounded. The survey cited supports a narrower proposition: the available evidence does not establish that the increase in use is attributable to minors. This formulation avoids overstating what the data show and places the evidentiary burden on proponents of restriction.

6.8 Internal and editorial consistency

Four minor points of consistency may be noted. The principles in the executive summary are addressed to policymakers, while the identical principles in the body are addressed to governments; a single formulation would be preferable, and policymakers is the broader term given that several of the measures discussed originate in courts rather than legislatures. The executive summary presents three principles and two recommendations, while the analysis in the body supports the additional principles proposed in sections 5 and 6 above. The date formats in the notes alternate between two conventions, and one bibliographic reference gives a publication date that does not correspond to the source path cited. The conclusion, finally, is noticeably shorter than the argument it closes and could usefully restate the taxonomy of measures and the alternative pathway.

7. Regional relevance: the Brazilian context

From the perspective of the Chapter, the Brazilian regulatory landscape makes the brief particularly applicable, and it also shows where its guidance is most needed. Legal and political pressure can shift the framing of virtual private networks from a security tool to a suspicious circumvention mechanism in a

very short span of time, and Brazil has produced, within two years, examples of several forms of restriction discussed in the draft.

7.1 The 2024 platform blocking and the fine imposed on users

The most visible episode is the suspension of a major social media platform in 2024. The decision that ordered the suspension also imposed a daily fine of fifty thousand reais on natural and legal persons who resorted to technological subterfuges, expressly including virtual private networks, in order to access the platform.[7] The Brazilian Bar Association petitioned for reconsideration, arguing that a generic and indeterminate prohibition imposed without adversarial process violated the principles of legality and due process.[8] The episode fuelled lasting public confusion as to whether the use of these tools is itself unlawful, when in fact it remains lawful in Brazil and is widely used for remote work, journalism, secure communications and the protection of users at risk. It also illustrates the point made in section 6.2, since the sanction was addressed to an indeterminate class of persons who had no opportunity to be heard.

7.2 Bill 3066/2025 and the proposed article 226-A

The second development is legislative. Bill 3066/2025, which establishes measures to combat and prosecute sexual violence against children and adolescents, including in digital environments and with the use of artificial intelligence, contains a provision increasing the penalty by one third to two thirds where an offence is committed using what the bill calls a “proxy modulator” or techniques for masking, concealing, falsifying, altering or anonymising an IP address or another digital identifier, with the aim of preventing or hindering identification.[9] The final text also provides that the aggravating factor does not

[7]Decision of Justice Alexandre de Moraes, Federal Supreme Court, 30 August 2024. The decision initially extended to the blocking of the applications themselves; that part was subsequently reconsidered, while the fine on users was maintained.

[8]Petition of the Ordem dos Advogados do Brasil to the Federal Supreme Court, 31 August 2024, endorsed by thirty-two lawyers, requesting reconsideration or clarification of the passage of the decision imposing fines on users.

[9]Bill 3066/2025, proposed article 226-A of the Child and Adolescent Statute (Law 8.069/1990). The original text included a proposed article 241-G criminalising the provision of such tools. That formulation was removed during the legislative process. The final text of article 226-A, approved by the Senate on 7 July 2026 and sent for presidential sanction on 17 July 2026, retains

apply to the legitimate use of privacy and digital-security technologies for lawful purposes, including the protection of personal or commercial data, privacy and cybersecurity. The trajectory of the provision is instructive. Concern that earlier drafts could reach developers and providers of legitimate technologies led to the removal of the criminalising formulation, while the final text contains an express legitimate-use safeguard. These changes show that technical advocacy influenced the legislative process; the aggravating factor nonetheless survived, leaving residual questions about the breadth of the technical categories and the practical distinction between legitimate protection and conduct intended to frustrate identification.

Civil society organisations, including this Chapter, objected to earlier versions on the ground that the provision treated technically distinct tools as legally equivalent and risked allowing the use of a neutral security technology to contribute to a harsher penalty.[10] The legitimate-use safeguard in the final text addresses part of that concern, but application of the provision will still depend on broad technical categories and on a case-by-case distinction between legitimate protection and use intended to impede identification. The signatories supported the central objectives of the bill and confined their objection to article 226-A, which is the posture the Chapter would recommend to organisations facing comparable proposals elsewhere. The episode is instructive not because it is uniquely Brazilian, but because it shows both how technical advocacy can improve legislation and how residual ambiguity can persist once the core aggravating-factor logic remains.

7.3 A converging regulatory agenda

Brazil is entering a phase of convergence across several digital regulatory fronts. In 2025, the Federal Supreme Court partially invalidated article 19 of the Marco Civil da Internet; in June 2026, it finalised the

---

the aggravating factor but includes an exception for the legitimate use of privacy and digital-security technologies for lawful purposes.

[10]Open letter addressed to the Federal Senate requesting the deletion of article 226-A from Bill 3066/2025, signed by Brazilian and international digital rights organisations and by individual experts, July 2026. Available at: https://www.isoc.org.br/uploads/download/260

governing thesis on platform liability. The Digital Statute for Children and Adolescents entered into force on 17 March 2026, with the data protection agency designated as the supervisory body and age-assurance obligations among its provisions.[11] Enforcement of the general data protection law has intensified, and cybersecurity requirements have expanded. Virtual private networks sit at the intersection of these agendas, which raises the likelihood that they will be addressed in fragmented and occasionally conflicting ways by authorities whose mandates were not designed to overlap.

These dynamics do not require the brief to become specific to Brazil, but they do show why its core principles are highly relevant. Avoiding punishment for the mere use of security tools, focusing on harmful conduct and content, and preserving access to privacy-enhancing technologies are precisely the propositions at stake in each of the episodes described above.

8. Additional insights

The Chapter would like to highlight two further developments that reinforce the relevance of the brief. The first concerns the institutional side of blocking. Public discussion in Brazil has raised concerns about the emergence of increasingly automated blocking infrastructure and about whether the telecommunications regulator may be assigned responsibilities beyond its statutory mandate. This connects directly to the analysis of collateral damage in the draft and to the risk of building permanent institutional structures around blocking rather than around rights-respecting governance. The Chapter considers that, once such infrastructure exists, the marginal cost of its use falls and the range of purposes for which it is invoked tends to expand, a dynamic the brief could name explicitly.

[11] Law 15.211/2025, in force since 17 March 2026 and regulated by Decree 12.880/2026; Law 15.352/2026 fixed the entry-into-force date and transformed the National Data Protection Authority into the National Data Protection Agency, a special autonomous agency.

The second is the open letter described in section 7.2, whose arguments on technology neutrality, the distinction between tools and conduct, and the long-term risks of establishing such precedents align closely with the core message of the brief and suggest that similar tensions may arise in other jurisdictions. These are not hypothetical scenarios but regulatory trajectories already under way. The brief can serve as a reference point for lawmakers and regulators facing proposals that expressly mention virtual private networks, helping them pursue legitimate aims, including the protection of children, without undermining the security, privacy and rights of users who rely on these tools for lawful, everyday purposes.

9. Summary of proposed amendments

The table below consolidates the proposals set out above. The order follows the structure of the draft rather than the order of the sections of this contribution.

Section of the draft	Proposed amendment	Purpose
A Brief Overview of VPNs	Add one or two sentences linking confidentiality, integrity and authentication to the legal interests they enable, namely data protection, freedom of expression, access to information and the safety of at-risk users.	Prevents the technical description from being read in isolation from the rights it supports.
VPN Restrictions (introduction to the three categories)	Refine the taxonomy by distinguishing network-level blocking, service-level and app-store restrictions, obligations imposed on providers, and sanctions imposed on end users.	Each measure raises distinct questions of feasibility, proportionality and collateral effects.
VPN Restrictions (categories 1 to 3)	Introduce the terms “penalty enhancements for the use of anonymisation tools”, “third-party punishment” and “age assurance based on sensitive data”.	Allows policymakers to recognise the categories of measures currently under discussion in legislatures and courts.

Section of the draft	Proposed amendment	Purpose
VPN content blocking	Develop the procedural dimension of the private enforcement injunctions already cited, including dynamic orders, absence of adversarial participation by affected third parties and lack of remedies for over-blocking.	Adds a due-process argument that does not depend on the merits of the underlying claim.
Guiding Principles	Add a principle stating that legal frameworks should not attach penalties, or enhanced penalties, to the mere use of virtual private networks and other anonymisation tools.	Responds to bills and decisions that treat the tool, rather than the conduct, as the object of sanction.
Guiding Principles	Add a principle on due process, transparency and effective remedy for measures that restrict or block virtual private networks.	Ensures that even legitimate measures are subject to procedural safeguards.
Guiding Principles	Anchor the principles in the international human rights framework on encryption and anonymity, in particular the tests of legality, necessity and proportionality.	Provides an external standard against which draft laws can be assessed.
Recommendations	Recommend that measures affecting virtual private networks be preceded by an assessment of their effects on the critical properties of the Internet and on the enablers of trust.	Connects the brief to the Internet Society's own analytical framework.
Recommendations	Organize the alternatives around a multi-scalar governance logic that assigns unlawful content, network integrity and identification duties to distinct institutional layers.	Clarifies why restricting the tool functions as a substitute for investigative capacity that has not been built.
Recommendations	Address the incentives for trustworthy provision, including independent audits, transparency reporting and verifiable data-minimization practices.	Answers the concern about untrustworthy providers without resorting to restriction.

Section of the draft	Proposed amendment	Purpose
Evidence base	Broaden the geographic range of the examples beyond Europe, North America and Asia, and replace commercial sources with independent research where the claim is load-bearing.	Increases the authority of the document and its usefulness outside the jurisdictions cited.

10. Conclusion

The Internet Society's draft states the essential proposition clearly, namely that virtual private networks are part of the technical infrastructure that keeps users safe and that restricting them does not address the harms invoked to justify the restriction. The Chapter endorses that proposition without reservation.

The suggestions offered here have a single purpose, which is to increase the operational usefulness of the brief in jurisdictions where such measures are being debated, drafted or implemented. Greater precision in the taxonomy of measures, an explicit anchoring in the international human rights framework, a principle on due process and effective remedy, and a broader evidentiary base would allow the document to function not only as a statement of position but as a working instrument for legislators and regulators. ISOC Brasil remains available to assist in the drafting of any of the passages proposed above and to provide additional documentation on the Brazilian cases described in section 7.