Internet Society
Capítulo Brasil

CONTRIBUTION OF THE INTERNET SOCIETY BRAZIL CHAPTER TO THE POLICY DEVELOPMENT PROCESS "ENABLERS OF AN OPEN, GLOBALLY CONNECTED, SECURE AND TRUSTWORTHY INTERNET"

EXECUTIVE SUMMARY

ISOC Brazil's contribution considers the PDP documents in form, content and narrative. In each axis, advantages and shortcomings are pointed out, as formal suggestions will not solve weaknesses in content or narrative, and vice versa. And a global look at scaling up the IAT points out specific suggestions, wide-ranging improvements and general reflections.

From the six guiding questions, our view can be summarized in the following considerations:

I. Importance and challenges:
   A. The effort to design enablers is in itself commendable and valuable, but it has challenges.
   B. Lack of semantic precision in the wording of questions associated with enablers can hamper the application of the Extended Toolkit as a standard.
   C. A holistic and contextualized view in applying the Toolkit can allow communities to better understand each other's situations.

II. Problems regarding the examples:
   A. Restrictions for users to connect to the Internet must not be weighed against the barriers faced by those who operate connection or routing, transmission and switching services.
   B. Collaborative development, management and governance should consider issues of traffic exchange points.
   C. Unrestricted accessibility should adequately address censorship issues.
   D. Available capacity should consider possible negative effects of an unregulated private control.
   E. Confidentiality of information, devices and applications data should take on Brazilian issues regarding WhatsApp, as they are very common all around the world.
   F. Integrity of information, applications and services could mention most relevant and recent cases, such as Pegasus.
   G. Reliability, resilience and availability should address situations of aggression and online threats, such as political violence against women.
   H. Accountability should highlight risks to freedom of expression, as censorship of content in more languages than English, especially considering the imprecision of the concept of terrorism.
   I. Privacy should consider issues about traceability.

III. Applicability in Brazil
   A. Brazilian Draft Bill n. 2630/2020
   B. Act No. 14.172/2021
   C. Zero rating
   D. Accession to the Budapest Convention

IV. Perspectives:
   A. The addition of enablers to the aspirational goals in the framework helps in acting on the most sensitive topics to end users, such as hate speech, disinformation, and computer malware.
   B. Despite the internal consistency, the document lacks a bridge with last year's proposal, lacking a closer correlation between Critical Properties of IWN, ISOC Aspirational Goals and Enablers, thus the narrative of the IIAT should create a more solid conceptual binding for these three pieces; and
   C. Further complex case studies looking at various countries and regions should be developed within 12 months as a coordinated IIAT stress-test.

Internet Society
Capítulo Brasil

FULL REPORT

The Internet Society has been working on the "Internet Interconnectivity Mode" (IWN) project to promote and highlight a set of five critical properties of the Internet:

1. An Accessible Infrastructure with a Common Protocol;
2. Open Architecture of Interoperable and Reusable Building Blocks;
3. Decentralized Management and a Single Distributed Routing System;
4. Common Global Identifiers;
5. A Technology Neutral, General-Purpose Network.

In this effort ISOC launched the "Internet Impact Assessment Toolkit" (IIAT), as a part of the regulatory process, aimed at analyzing public policies, regulations and private practices. But the role of critical properties in promoting and protecting the IWN as a preferred model among other possible and undesirable ones does not prove sufficient to reach the Internet's maximum potential.

Thus, in expansion of the IIAT, ten "Enablers of an Open, Globally Connected, Secure and Reliable Internet" were proposed as additional evaluation aspects linked to the aspirational goals of ISOC, in a non-exhaustive list:

1. Easy and unrestricted access;
2. Unrestricted use and deployment of Internet technologies;
3. Collaborative development, management, and governance;
4. Unrestricted reachability;
5. Available capacity;
6. Data confidentiality of information, devices, and applications;
7. Integrity of information, applications, and services;
8. Reliability, resilience, and availability;
9. Accountability; and
10. Privacy.

The present Policy Development Project (PDP) thus includes a) an updated Introduction to the Toolkit and b) a "white paper" on enablers. Both proposals are subject to scrutiny by the community until September 20th.

In order to guide the contributions, the following questions were pointed as guides:

1. Do these enablers make sense?
2. Is something missing in their description, and are the examples helpful?
3. Do you have additional examples, positive or negative, that you would like to share?
4. Is it a helpful narrative for you and your community? Would they support your use of the toolkit in your local/regional context?
5. Do you have suggestions for improvements or ideas for how this toolkit can be used by the Internet Society members and allies?
6. Are you interested in producing your own analysis using this expanded version of the toolkit?

From our answers to these six guiding questions, we have structured the following six sections.

1. Enablers significance

(Do these enablers make sense?)

First, we would like to commend Internet Society on the effort of developing a framework to support local communities' assessment of political, legal and technological factors that could affect the ideal of an "open, globally connected, secure and trustworthy" Internet. The approach is very precious in its purpose of generating an adequate instrument for the production of standardized, exhaustive and complete assessments of bills, public policy proposals and private actions with a potential impact on the Internet.

It is a real challenge to objectively describe such enablers and relate them one-to-one to each ISOC aspirational goal for the Internet, given that both groups of concepts seem to be intrinsically and overall connected.

As proposed, the enablers are consistent with the idea of the framework's comprehensiveness and applicability to the diversity of local situations.

However, we consider that the guiding questions presented at the PDP deserve some enhancement. Despite the goal of explaining each enabler, the set of questions might end up leaving each concept to wide interpretations, thus giving rise to confusion and overlapping between different enablers.

For example, the question "*Does the proposed change create a barrier to entry, such as costs, administrative overhead, or other difficulties?*" may, in a certain context, apply to the *Unrestricted use and deployment of Internet technologies* enabler instead of the proposed *Easy and Unrestricted Access* one. Similarly, the question "*Is the effect of the change to restrict who can participate, closing down the Internet?*" could tie better to the *Easy and Unrestricted Access* enabler rather than to the *Unrestricted Use and Deployment of Internet Technologies* one.

Therefore, we consider the questions should be better structured, or have an additional set of explanations, in order to better guide their usage.

We also believe a holistic view on the application of the Impact Assessment Toolkit would also be very interesting. Any specific concrete case should be subjected to assessment in light of the total set of goals and enablers composing the framework, and not in regard to single enabler and goal.

The IIAT can be a great opportunity for local communities to get to know each other in depth. Ideally, each toolkit application should output a case study offered by ISOC chapters and should be accompanied by a socio-economic exposition that provides external actors with a contextualized view of the local impact assessment.

2. Definition gaps and case studies usefulness

(Is something missing in their description, and are the examples helpful?)

Easy and unrestricted access

The *easy and unrestricted access* enabler definition is centered in making Internet services more accessible and affordable for users in general, considering connection as a fundamental right. Nevertheless, the examples presented in the document are about regulatory and commercial barriers for the operators.

This approach seemingly conflates users' access rights with operators' commercial rights, to connect to the Internet and provide services.

The first example presents the Web Content Accessibility Guidelines (WCAG), aimed to promote Internet access for people with disabilities – a good example for accessibility and for facilitating Internet services for everyone. The second one discusses spectrum licensing, aimed at facilitating Internet access in areas poorly served by traditional fiber and copper infrastructure. The third example points out how, in some countries, excessive regulation can lead to the lack of service provision and generate monopolies – which might weaken Internet access due to a lack of competition and, therefore, lead to costs increase for users.

If the main goal of this enabler is to facilitate "becoming a part of the Internet", the third example doesn't seem to be a good fit. Even in economies in which competition is widespread and enforced by policy and regulations, there can be tendencies toward the development of monopolies.

Internet Society
Capítulo Brasil

Unrestricted use and deployment of Internet technologies

We understand that the *unrestricted use and deployment of Internet technologies* enabler aims to assure that the Internet's infrastructure is available as a resource to everyone "in a responsible and equitable way". The case of RSA SecurID exemplifies how patents and trade secrets can menace the development of Internet services and hinder tech improvement.

In opposition, the document presents the OAth's security protocol which enables users to share their passwords with other applications without providing private user data. This should be an example of how open sourced programs and protocols can enhance user security. Both are good examples for the enabler in question, and should be kept as is.

Collaborative development, management, and governance

The *collaborative development, management, and governance* enabler seeks to draw attention towards possible limitations or restrictions in the maintenance of an open and collaborative Internet.

Its first example discusses the Regional Internet Registries, a decentralised decision-making mechanism that allows for the accomplishment and maintenance of this goal. The second refers to the Internet Exchange Points (IXPs), which "offer community network operators the opportunity to connect and exchange Internet traffic".

This could be an efficient way to expand Internet openness, for the potential to engage more regional operators and, therefore, benefit local communities. Nevertheless, it does not consider the material possibilities and assets necessary for IXPs to be implemented, being equipment "donor fatigue" an ongoing concern, as 2016 IGF pointed out.

Unrestricted reachability

Regarding the *unrestricted reachability* enabler, the document points out that resources and technologies should be available for users, and that it should be assured that "there is no blocking of legitimate use and access to that resource by third parties".

The first example discusses the development of other Internet Protocols by the community to circumvent the limitations posed by the universal use of the IPv4 addresses, allowing a more secure and trustworthy Internet for users. Maybe this first example could be rephrased to make it clear that the focus is not the scarcity of IPv4 addresses, but the open Internet community's efforts to circumvent this limitation.

The second example discusses the prohibition of VoIP services in some countries by governments, which creates "economic inefficiencies, imposes higher costs, and serves to isolate users in that country". It seems to be more concerned with the economic issues of blocking these technologies, instead of highlighting surveillance of activists and political minorities, or censorship, which are severe issues, as pointed out by the Freedom Of The Net 2020 report on India.

Available capacity

With regards to the *available capacity* enabler, the document draws attention to the concern with measures that could decrease Internet resources availability, such as bandwidth and other capacities.

The first example, on the SpaceX' Starlink project, seems naive in terms of the economic and private interests at play. It disregards the negative effects of a private company having such an impact on Internet availability, as well as other malicious practices which may arise in the future, such as dumping. At this point, specialists are worried after Germany contracted with Google and T-Systems for citizens data storage.

Private control of such capacities should not be taken lightly, as it could lead to deep negative effects in the future, especially in the Global South – where private actors not rarely contract for unfair economic advantages within illiberal democracies and authoritarian regimes.

Data confidentiality of information, devices, and applications

Regarding the *data confidentiality of information, devices, and applications* enabler, the document calls for the maintenance of confidentiality and privacy of users' information.

The first example underlines the "industry-wide standard that requires encryption when data is sent over the Internet, PCI DSS adds to the confidentiality of data-at-rest and data-in-motion". It is a good example and should be kept as is, as well as the third example, about WebPKI.

But the second one, on Mauritius' administration attempt to decrypt users communications with the national security justification, should enumerate more situations alike, as this appears to be a very common request all around the world.

Integrity of information, applications, and services

With regards to the *integrity of information, applications, and services* enabler, the document deals with data integrity and malicious manipulation of Domain Name System and routing systems. Both given examples satisfy the understanding of the enabler. Nonetheless, the document fails to mention relevant cybersecurity threats such as NSO's Pegasus software, as detailed in section 3.

Reliability, resilience, and availability

Regarding the *reliability, resilience, and availability* enabler, the document proposes that Internet services should be predictably available for users – considering that there will always exist an acceptable level of errors and other challenges for normal operations. Its first example *statuspage.io* shows the Internet providers' service status. The second one mentions "deliberate Internet shutdowns" in some countries, especially during civil unrest times, posing a negative effect on the goal of a trustworthy Internet. Both are good examples and should be kept as is. Nevertheless, it would also be good to consider the failure of companies and the State to provide more predictability in the treatment of victims of online harms.

Accountability

Concerning the *accountability* enabler, the document lists risks of non-transparent authorities and hidden decision making procedures that could affect the trust users have in the Internet.

The example of the Global Internet Forum to Counter Terrorism especially highlights the absence of an auditable database, which operates with hashes and can lead to errors and mistakes, without possibility of external oversight. The document should point out risks for freedom of expression, like censorship of non-anglophones content. Also, the database could also produce some sort of noise, as "terrorism" is a highly contentious and hard to define category in the social sciences.

Privacy

The document points out possibilities of violations of users' right to privacy and proposes that users should be able to understand how their information is collected, stored and shared, strongly highlighting the possibility of anonymity. It mentions (1) the British government's Online Safety Bill; (2) the California Consumer Privacy Act of 2018 (CCPA); and (3) the EU GDPR.

The former is quoted as a negative example, since it allows for the break of end-to-end communication, which would be a harmful approach to dealing with online harms. In this very same direction, we suggest the document should also dive into, as another relevant case, the "traceability" debate in India and Brazil, as detailed in the next section.

3. Additional Case Studies

(Do you have additional examples, positive or negative, that you would like to share?)

The document could benefit from the inclusion of the following case studies.

First, regarding both *available capacity* and *privacy* enablers, the German government contracts with Google and T-Systems for citizens' data storage should be added as an example. As highlighted before, these sections seem to disregard the potential impact of private companies having such an influence on public data storage and Internet capacities. Malicious practices might arise, such as dumping and/or harmful contracts for citizens in illiberal democracies and authoritarian regimes.

Second, on both *data confidentiality of information, devices, and applications* and *accountability* enablers, concerns on government criteria to audit or supervise the digital platforms could be added having as examples: (1) WhatsApp legal incidents in Brazil, from judges attempting to arrest executives, prosecution threats for not decrypting user communications, despite of what *Marco Civil da Internet no Brasil* ("Brazilian Civil Rights Framework for Internet Usage") provides; (2) "traceability" provision discussed both in India and Brazil (Projeto de Lei nº 2630/2020, the "Brazilian Draft Bill for Freedom, Responsibility and Transparency on the Internet", aka. "Fake News Law"), which would make communications vulnerable to private and government surveillance, on the pretext of helding platforms accountable; (3) President Bolsonaro's recent attempt to modify *Marco Civil da Internet* with the *Medida Provisória* ("Provisional Measure") nº 1.068/2021, which would establish a rule prohibiting platforms from moderating content and profiles, with exceptions only for an inconsistent and incomplete set of "Fair Causes".

Third, with regard to the *integrity of information, applications, and services* enabler, the document could mention more recent relevant cybersecurity threats, such as the NSO's Pegasus software, a paradigmatic case study of harmful contracts between private sector and governments.

Fourth, on the *reliability, resilience, and availability* enabler, lack of trustworthiness could be illustrated in the document by describing threatening and harmful episodes of digital public sphere oppression against vulnerable social segments, with both public institutions and private platforms failing to provide safety and proper responses after attacks. This is well documented, for instance, in a report by InternetLab and Revista Azmina on online political violence against female politicians during Brazilian municipal elections in 2020. This could serve as an example of a negative effect on the goal of a trustworthy Internet as these attacks and lack of proper and equitable reactions (not only in Brazil) weakens the enabler by reducing reliability and availability.

4. Enablers usefulness for Toolkit application in the Brazilian Chapter context

(Is it a helpful narrative for you and your community? Would they support your use of the toolkit in your local/regional context?)

ISOC Brazil strongly believes that the use of the proposed enablers has the potential to contribute to the evaluation of a set of cases in Brazil. For example, regarding the aforementioned **Draft Bill 2630/2020**, (1) the *collaborative development, management, and governance* enabler contributes to assess the implications on the goal for an open Internet, as its Article 25 provides for the creation of an Council for Internet Transparency and Accountability; and (2) the *data confidentiality of information, devices, and applications* and *privacy* enablers contribute to assess the implications of traceability, object of Article 10, on the security and trustworthiness aspirational goals.

Another possible usage of the enablers regards the presidential veto to Bill No. 3477/2020, later overturned by the National Congress, which imposed its enactment. Act No. 14.172, from June 10, 2021, provided for the granting of R$ 3.5 billion in 30 days, to guarantee Internet access to students and teachers of public basic education. The President challenged the constitutionality of this law before the Federal Supreme Court (Direct Action of Unconstitutionality 6926) and issued a Provisional Measure removing the deadline for transferring the money (which is also challenged before the STF, in ADI 6971). The *easy and unrestricted access* enabler allows an objective assessment of how negatively Bolsonaro's policy option affects the openness goal.

The *unrestricted reachability* enabler helps assess the impacts to the global connection goal imposed by the "**zero rating**" mobile plans for certain online apps and services.

Also, in order to monitor and assess the paths of the country's seemingly inevitable accession to the Budapest Convention on Cybercrime in the near future, two aspirational goals could have their assessment facilitated by the enablers: for security, *data confidentiality of information, devices, and applications* together with *integrity of information, applications, and services* enablers; and for the trustworthiness, *accountability* together with *privacy*.

5. Suggestions for improvement and use of the extended toolkit

(Do you have suggestions for improvements or ideas for how this toolkit can be used by the Internet Society members and allies?)

We would like to, once again, commend ISOCs work on the "Enablers of an open, globally connected, secure and trustworthy Internet" concept, as an extension to the IIAT, which is already based on the five "Critical Properties" of the Internet Way of Networking.

The Critical Properties are very relevant for assessing policies' risk of harming Internet architecture fundamentals, for instance by imposing restrictions to the free flow or routing of packets through the many networks that build the Internet. But back when those five properties were proposed, in 2020, it was noticed by many that they were mostly restricted to the basic architecture of the Internet infrastructure.

It has been argued by some that they might not be really helpful for the community to assess the impact of technologies and policies that, in fact, affect the Internet upper layers, where end users directly interact with applications, content and services. Most current concerns of end users, and also of legislators and regulators – such as content moderation fighting hate speech and fake news, and end-user security regarding malware of various types – are not directly related to those five critical properties of the IWN, and could not be assessed solely under them.

For most end users and legislators, the Internet is not its infrastructure – of which most of them are not even aware: it is the applications, services and content it offers to society. The IWN definition seemed to trap the Internet Society mission into the lower layers of the Internet (apparently as a consequence of its "technical" history and background) and, therefore, far from many nowadays relevant concerns.

The strategic definition of the "Enablers" moves the Internet Society to amplify the IIAT to address those concerns, thus becoming relevant for a much larger range of stakeholders and creating a new, extended conceptual background for its advocacy efforts.

Nonetheless, the overall resulting framework seems fragmented. Now it lacks dialogue among the three conceptual pieces: the five Critical Properties of the IWN, the four Aspirational Goals (open, globally connected, secure and trustworthy Internet), and the (as of now) ten Enablers of those goals.

The proposal provides "*examples of different policies or technologies specific to an Enabler that either advance or block the Goal in the area identified*". But the document does not seem to make an effort to use those same examples to assess the impact of these technologies or policies on the five Critical Properties of the IWN. Enablers and Goals, from one side, and Critical Properties, from another side, seem two worlds apart, at least from reading the document.

Some of the Enablers may be easily related both to the Aspirational Goals and to the Critical Properties. For example, the goal of an "open Internet" – the document states that "*an open Internet is an accessible Internet – it is easy to connect to the open Internet and use its services*". This statement may be interpreted as referring, for instance, both to the connection of new networks (which directly maps to the Critical Properties) and to the services and applications at the upper layer of the Internet.

One of the Enablers of this aspiration goal is *easy and unrestricted access*. But none of the three examples illustrate how this Enabler might be impacted by technologies and policies related to the Internet infrastructure and, thus, to the five Critical Properties. Similar considerations can be made with regard to the other Aspirational Goals and examples.

Therefore, it seems desirable for the Internet Society to make an additional effort of crafting a more consistent and less fragmented framework, particularly bridging closely the five Critical Properties, from one side, and the Aspirational Goals and Enablers, from another.

It seems that, actually, a lot of aspects and resources can be recognized as an Enabler. Creating a rather limited list, with specific titles and expressions open to interpretation, could backfire to generate confusion instead of clarifying the role of each Enabler. Despite making clear that there can be additional Enablers and the list will be updated, it would be better simply to have a working definition of what does ease the Aspirational Goals, and what does run in the other direction, creating obstacles and doing harm to those Goals, or just "disable". The Internet is too complex to limit Enablers as well as disablers of openness, security, trustworthiness and connectivity to a closed and confined list of expressions. It should be up to the stakeholders and the community to articulate all the things that do enable or not, based on a solid concept for both categories, provided by ISOC.

Maybe, as a first and practical step in that direction, examples should be sought that illustrate how technologies and policies impact not only the enablers, but also and mainly the five Critical Properties of the Internet Way of Networking. On a longer perspective, the whole narrative of the IIAT should be then adapted, creating a more solid conceptual binding for these three pieces: Critical Properties, Aspirational Goals and Enablers.

6. Expanded toolkit usage of Brazil interest

(Você teria interesse em produzir sua própria análise usando esta versão expandida do kit de ferramentas?)

ISOC Brazil proposes to develop, in the coming months, more complex case studies regarding the use of the IIAT, which shall simultaneously cover several Enablers, point out positive and negative impacts on different Aspirational Goals, and allow the evaluation of their effects on the critical properties of the IWN. Examples like this could help build a solid bridge between Critical Properties and Enablers, a link that seems to be missing in the current proposal for the expanded description of the IIAT.

The intention is to conduct a stress test of the IIAT by means of such case studies: more robust, developed over a longer period of time, and targeting a large country in the Global South, with a complex and peculiar reality for the development and use of the Internet. For consistency, ISOC Brazil strongly suggests that further, equally complex case studies with other countries and regions be developed as part of a coordinated IIAT stress-testing effort, to take place within 12 months. Then, in light of the lessons learned from such studies, ISOC would be in a better position to prepare a complete review of the IIAT, in a new collaborative process with its community.

CREDITS

This contribution was collectively drafted by members of the Internet Society Brazil Chapter's Working Group on Intermediary Liability (GTRI-ISOC Brasil), who volunteered to be part of a Task Force dedicated to the Policy Development Process on "Enablers of an Open, Globally Connected, Secure and Trustworthy Internet".

Internet Society
Capítulo Brasil

Members of the PDP Enablers Task Force

Alexandre Arns	Flávio Rech Wagner	Rodrigo Duarte
Bruna Martins dos Santos	Paulo Rená da Silva Santarém	Thais Aguiar
Camila Akemi	Raquel Gatto	Yasmin Curzi
Giovanna Michelato	Roberta Battisti	

The **GTRI-ISOC Brasil**, led by Bruna Martins dos Santos and Paulo Rená da Silva Santarém, as Senior Public Policy Consultants at ISOC Brazil, continues the work of the Chapter on the subject of intermediaries liability. Its purpose is to develop and implement strategies for the preservation of the legal regime designed in Marco Civil da Internet (*Civil Rights Framework for Internet*) and for the dissemination of the ISOC Brazil's Decalogue of Recommendations on the Brazilian Model of Liability for Intermediaries.

The **Internet Society Brazil Chapter** is a non-profit organization of Brazilian civil society, with an autonomous structure, whose objective is to locally foster and promote the mission and principles of ISOC.