8 November 2021

Enablers of an Open, Globally Connected, Secure and Trustworthy Internet

Internet Society

Table of Contents

Introduction

The Internet's potential is unlimited. As a worldwide resource, the Internet supports commerce, recreation, research, education, entertainment, and everything in between. But with different stakeholders and competing demands of the network, safeguarding the future of the Internet can seem like an impossible task.

It doesn't need to be hard. The Internet was created with a unique foundation[1] that empowers users across borders to collectively shape its evolution. Time and time again, different groups and organizations[2] worldwide with different viewpoints find common ground on a shared set of goals for the Internet. That is, a network that is open, globally connected, secure and trustworthy.

The Internet Society's mission is also based on these goals. Unfortunately, the Internet today is far from this aspirational state of being open, globally connected, secure and trustworthy. Furthermore, a variety of business developments and governmental regulatory interventions (or lack thereof) threaten to move us further away instead of closer to them. That is why protecting the Internet's evolution towards these goals is urgent and important.

These goals guide our collective journey to a better Internet. They tell us how we want the Internet to be, now, and in the future. By viewing proposed changes in policies, technologies, and applications in relation to these goals, we can better understand whether we are on track for a thriving Internet or straying from our targets.

Aspirational Goals for a Thriving Internet	
An Open Internet	The open Internet allows people and organizations to mix and match technologies without permission and with minimal barriers. Sustaining and growing an open Internet helps to spur innovation and keep it fit for future applications. An open Internet is an accessible Internet - it is easy to connect to the open Internet and use its services.

1 Internet Way of Networking: Defining the Critical Properties of the Internet https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/

2 See, for example OECD goals for Internet Policy Making (https://www.oecd.org/digital/ieconomy/oecd-goals-for-internet-policy-making.pdf), the United States Department of State statement on Internet Governance (https://2009-2017.state.gov/documents/organization/255010.pdf), the African Union (https://au.int/sites/default/files/newsevents/conceptnotes/31357-cn-background_note_on_the_au_declaration_on_ig_en_1.pdf), European Union in their Cybersecurity strategy (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN), the Council of Foreign Relations (https://cdn.cfr.org/sites/default/files/pdf/2013/06/TFR70_cyber_policy.pdf.pdf), CITEL (http://www.oas.org/CITEL/citel1/ult-ciberseguridad_i.asp), the Global Commission on Internet Governance (https://www.cigionline.org/publications/one-internet/).

A Globally Connected Internet	The globally connected Internet is inclusive. It allows networks and users to interconnect without geographical restrictions. Increasing the connectivity of the Internet makes it more valuable to every participant, as a tool for communications, learning, commerce.
A Secure Internet	A secure Internet is resistant to attacks on its infrastructure, delivering a robust service to its user community. A secure Internet does not create insecurity, such as botnets that are used in phishing scams. Improving security of the Internet increases its usefulness to all participants.
A Trustworthy Internet	A trustworthy Internet meets the expectations of its users by offering a resilient and reliable base for applications and services. Improving a trustworthy Internet makes it possible for individuals and organizations to rely on the Internet as a continuing worldwide communications resource.

Enablers of an Open, Globally Connected, Secure, and Trustworthy Internet

For each of the Internet goals, we have identified a series of supporting characteristics that advance the Internet, its infrastructure, and its use towards these universal goals. We call these supporting characteristics **"enablers"**: they advance and enable the targeted goal.

The purpose of identifying enablers is to simplify the task of analyzing the potential effects of proposed changes, and in consequence how it may affect the goals. For example, a secure Internet requires that the Internet support both data confidentiality and data integrity. Each of these is an enabler: data confidentiality supports the goal of a secure Internet, as does data integrity. If either is missing, the security of the Internet is reduced. Since the enablers, not the goals, are the tool for analysis of proposals, they are the focus of this framework.

Below, we identify enablers[3] that relate to each of the four Internet goals. To help make the meaning of each enabler and how it relates to the attainability of an Internet goal as clear as possible, we have provided examples of different policies or technologies specific to an enabler that either advance or block the goal in the area identified.

It is important to note the enablers are presented in their ideal form. By thinking of them as if they reflect a perfect state, we have a reference point that helps us determine whether a particular development moves the Internet away or towards the identified goals. The enablers can also expose some of the tensions that exist between the goals and make the potential trade-offs clearer. For example, some of the actions may have a positive effect on the security of the Internet, while making it less open at the same time.

Supporting an Open Internet

The Internet is fully open when anyone may create, use, or deploy it according to their own wishes. With a fully open Internet, anyone is is free to deploy Internet networks and build services and applications on the Internet, combine them in novel ways and deploy them without barriers, as long as this is done in interoperable ways. An open Internet is an accessible Internet – it is easy for networks to join, and for users to connect to it and use its services.

The tables below define some enablers of an open Internet. We have also provided some examples of different policies or technologies that either advance or block the goal in the area identified. Note that

3 This list of enablers is not meant to be a complete enumeration of everything that contributes to a goal. These are listed to help your analysis of changes that may affect the target positively or negatively. If you find some aspect of a change that strongly affects a target but doesn't neatly fit into the list of enablers, you may have found a new enabler – use it in your analysis and send it back to us for inclusion in the next version of this document. Some of the enablers may relate to more than one Internet goal. For example, "easy and unrestricted access" could arguably also advance the goal of globally connectivity. The framework is a simplification of this reality: since the enablers and not the goals are the primary analytical tools for the impact assessment, an enabler is attributed to one goal only to help contextualize its role.

these examples should be read as illustrations for their effect on the enabler with which they are listed. Some of our examples may have positive effects for one enabler and negative effects for others[4].

Enabler	Easy and unrestricted access
Description	It is easy to become part of the Internet, for networks and users alike. That means that for users the Internet is affordable and Internet services are accessible, and that networks can easily become part of the Internet, without unnecessary regulatory or commercial barriers for both groups.
Questions	Does the proposed change create or lower a barrier to entry, such as costs, administrative overhead, or other difficulties? Is the effect of the change to restrict who can participate, closing down the Internet? Does the proposed change create unnecessary requirements for particular skills, or raise costs?

Example 1: The Web Content Accessibility Guidelines (WCAG) is a recommendation by the World Wide Web Consortium (W3C) for making Web content more accessible, primarily for people with disabilities. For example, by recommending text alternatives for any non-text content so that it can be changed into other forms, such as speech or large print. In some jurisdictions conformity to these guidelines is required by law to safeguard the rights of people with disabilities.

This is an example of a positive effect on an open Internet for users, strengthening "Easy and unrestricted access" by facilitating the use of the Internet services by everyone.

Example 2: Spectrum licensing is a process where regulatory agencies allocate scarce finite resources—access to the radio waves—for various uses, including Internet use. Spectrum licensing policies can have a strong effect on access to the Internet in areas poorly served by fiber and copper infrastructure. For example, the US recently reallocated spectrum to support 5G services in 2020 by taking underutilized spectrum that had been originally assigned for educational television broadcasting in the 1960s.[5] Because some of the affected spectrum was already in use to extend Internet access to underserved groups, this policy change could have had a negative effect on the goal of an open Internet by removing access to spectrum that was being used for Internet access. However, the open decision-making process kept

4 For illustrations of more comprehensive assessments of impacts across multiple enablers we recommend you visit our repository of Internet Impact Briefs, available here: https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

5 https://docs.fcc.gov/public/attachments/FCC-19-62A1.pdf

intact the existing use for Internet services and opened the door for rural tribal communities to have priority access to spectrum for community networks ahead of commercial interests with deeper pockets.

This is an example of a positive effect on the goal of an open Internet for networks, strengthening "Easy and unrestricted access" through policies that favor community and non-profit Internet access.

Example 3: In some countries Internet access is only available through monopoly service providers. The effect of this is to create higher costs (through lack of competition) as well as limitations on what types of services and connection methods are available. The lack of choice among providers effectively limits overall access.

This is an example of a negative effect on the goal of an open Internet for users and networks by weakening "Easy and unrestricted access" through limitation of connectivity options and higher costs.

Enabler	**Unrestricted use and deployment of Internet technologies**
Description	The Internet's technologies and standards are available for adoption without restriction. This enabler extends to end-points: the technologies used to connect to and use the Internet do not require permission from a third party, operating system (OS) vendor, a network provider, or any other third party. The Internet's infrastructure is available as a resource to anyone who wishes to use it. Existing technologies can be mixed in and used to create new products and services that extend the Internet's capabilities.
Questions	Does the proposed change restrict how the Internet's technologies can be used or deployed? Is the effect of the change to create an unfair or discriminatory limit? Does the proposed change unreasonably limit how end users can manage and control their own devices?

Example 1: The RSA SecurID authentication system was an early multi-factor authentication system protected by patents and trade secrets. The resulting vendor lock-in and expense was good business for RSA, but also limited the ability of developers to include SecurID technology in Internet applications, depriving users of the opportunity for better security and protection against credential theft.

This is an example of a negative effect on the goal of an open Internet caused by weakening the enabler restricting the use and deployment of technologies.

Example 2: OAuth[6] is a protocol originally designed to solve the problem of sharing private user data in one application with a second application—without the user having to share their password. From this small beginning, it has grown into a very broadly used authentication and authorization solution, from Internet applications to enterprise solutions. OAuth's open, unrestricted, and collaborative nature helped it to spread across many different use cases and into many different products and applications. Having a secure, standardized, and widely accepted system for authentication and authorization reduces the barriers for further innovation and new, secure, Internet uses.

This is an example of a positive effect on the goal of an open Internet, strengthening "Unrestricted use and deployment of Internet technologies" by creating technology building blocks of an open, unrestricted, and collaborative nature.

Example 3: Google and Oracle engaged in a complicated 9-year battle[7] over the Java Application Programming Interface (API), based on Oracle's ownership of Java and Google's use of the API to make their own written-from-scratch Android operating system compatible with Java applications. Oracle claimed that the API was theirs to own and control as much as the rest of the Java source code, while Google claimed that their use of the API was not subject to Oracle's copyright under the "fair use" doctrine. In the end, the US Supreme Court[8] agreed with Google: Oracle's copyright on Java did not restrict Google's use of the API. This particular case was largely economic: had Oracle won, Google would have had a huge bill to pay based on the immense popularity of Android. But the larger issue of whether the use of the API was fair use affects future Internet innovation.

This is an example of a positive effect on the goal of an open Internet that strengthened "Unrestricted use and deployment of Internet technologies", as the US Supreme Court made it clear that some types of innovation and use cannot be restricted.

Enabler	**Collaborative development, management, and governance**
Description	The Internet's technologies and standards are developed, managed, and governed in an open and collaborative way. This open collaboration extends to the building and operation of the Internet and services built on top of the Internet. The development and maintenance process is based on transparency and consensus, and has as its goal the optimization of infrastructure and services to the benefit of the users of these technologies.

6 OAuth is developed by the IETF OAuth Working Group. More information is available at https://oauth.net/2/

7 Although far from an unbiased description of the issues, the EFF's recounting of the history of *Google v. Oracle* is available for those who would like a blow-by-blow description at https://www.eff.org/cases/oracle-v-google.

8 The Supreme Court's decision is available at https://www.supremecourt.gov/opinions/20pdf/18-956_d18f.pdf

Questions	Does the proposed change limit collaboration during development, operation, and governance? Is the goal of the proposed policy a restraint on collaboration?

Example 1: The Internet's address space is a limited resource that requires careful administration. Rather than centralize decision-making, each of the major Internet regions is responsible for governance of the address space in their region. Local address space policymaking is based on a collaborative process driven by the regional community. Policies that reach consensus are implemented by the Regional Internet Registry[9]. This creates an environment where the Internet itself can be "open" in a context that fits the region.

This is an example of a positive effect on the goal of an open Internet, strengthening "Collaborative development, management, and governance" through community-driven management of Internet resources.

Example 2: Internet Exchange Points (IXPs) offer community network operators the opportunity to connect and exchange Internet traffic[10]. By bringing together Internet stakeholders such as ISPs, municipal networks, and content delivery networks, local Internet traffic is routed more efficiently, and local users enjoy better and more resilient access to regional traffic. IXPs often include competitors working together for the benefit of themselves and of the local community. Many IXPs have unrestricted open peering policy leaving the decision of who to interconnect with to individual participants. A multilateral policy of peering with everyone is very common.

IXPs are an example of a positive effect on the goal of an open Internet, strengthening "Collaborative development, management, and governance" through facilitating open access, using non-discriminating policies and building local communities.

Supporting a Globally Connected Internet

With a truly interconnected Internet, anyone who wants to be part of the Internet can participate and exchange traffic with other participants without restrictions. A globally connected Internet is not just a technical capability, but one in which all barriers to connection are minimized and everyone who wants to use it can get a fast, reliable, and affordable connection to end-points (users, services or resources like storage, computing, sensing, and actuating) no matter where they are located.

9 More information on Regional Internet Registries is available through the Number Resource Organization at https://www.nro.net/about/rirs/

10 A longer explanation of the characteristics and benefits of IXPs is available as part of the Internet Society's "Growing the Internet" explainer series at https://www.internetsociety.org/resources/doc/2020/explainer-what-is-an-internet-exchange-point-ixp/

Enabler	Unrestricted reachability
Description	Internet users have access to all resources and technologies made available on the Internet and are able to make resources available themselves. Once a resource has been made available in some way by its owner, there is no blocking of legitimate use and access to that resource by third parties.
Questions	Does the proposed change restrict which resources a user can use and access, or restrict the resource the user may contribute to the Internet? Is the effect of the change that a third party can block access to significant parts of the resources of the Internet, or creates single points of failure?

Example 1: The Internet community worked hard to mitigate negative effects of widespread use of the Network Address Translation (NAT)[11] devices between end-user networks and the Internet, which allow for the more efficient use of limited public IPv4 address space. While NAT is harmless for most Internet users, it is extremely disruptive to some protocols, such as Voice over IP (VoIP). To work around the problems created by NAT, the Internet community has defined other protocols, including STUN[12], TURN[13], and ICE[14]. For many users, these protocols and technologies enable use of peer-to-peer type communications that would normally be blocked as a side effect of NAT.

This is an example of a positive effect on the goal of a globally connected Internet, strengthening "Unrestricted reachability" through removing barriers to end-to-end connectivity.

Example 2: In some countries, VoIP services are blocked because of government policy maintaining a state-granted monopoly on (and ability to tax) long-distance voice communications. This blockage creates economic inefficiencies, imposes higher costs, and serves to isolate users in that country from other Internet users taking advantage of VoIP technologies and services.

This is an example of a negative effect on the goal of a globally connected Internet weakening "Unrestricted reachability" by blocking services.

11 Technical readers may wish to make a distinction between various types of NAT, but for the sake of the reader we are using "NAT" to mean all types of network address and port translation technologies.

12 Session Traversal Utilities for NAT (STUN), RFC 5389 https://www.ietf.org/rfc/rfc5389.txt

13 Traversal Using Relays around NAT (TURN), RFC 8656 https://www.ietf.org/rfc/rfc8656.txt

14 Interactive Connectivity Establishment (ICE), RFC 5245 https://www.ietf.org/rfc/rfc5245.txt

Enabler	**Available capacity**
Description	The capacity of the Internet is sufficient to meet user demand. No one expects the capacity of the Internet to be infinite, but there is enough connection capacity – ports, bandwidth, services – to meet the demands of the users.
Questions	Does the proposed change act to increase the availability of Internet resources, such as bandwidth or other capacity? Is the effect of the policy to limit growth and capacity, either directly or indirectly?

Example 1: Stakeholders in the Democratic Republic of Congo have come together to set up an IXP in the primary city of Kinshasa (KINIX). After some years, the community felt the need for a second IXP in the second biggest city Lubumbashi. It was launched in 2019. Now in Q3 of 2021, the community will be launching a 3rd IXP in Goma. The establishment of these IXPs significantly reduced connectivity costs (in 2020 estimated yearly savings per network were as high as $163,000) and increased available communication capacity.

This is an example of a positive effect on the goal of a globally connected Internet by improving "Available capacity" in areas of scarcity.

Example 2: SpaceX's Starlink project aims to deliver Internet service via Low Earth Orbit satellites. While the project is in its infancy and still being beta tested, it has the possibility to deliver significant additional capacity in areas that are currently underserved. The way in which governments choose to regulate and license the Starlink product (both the space and especially the ground segments) will strongly affect whether Internet capacity in an area is increased.

If the licensing, costs, and restrictions selected by each regulatory agency covering a particular area are not onerous, Starlink will likely have a positive effect on the goal of a globally connected Internet, by increasing "Available capacity".

Example 3: Networks that choose not to deploy IPv6 but rely on Carrier Grade Network Address Translation (CGNAT)—essentially a much larger version of the NAT mentioned earlier—will reach a point where their users will starve the available resources. CGNATs necessarily restrict the number of simultaneous connections individual users can use. Without a CGNAT an individual user can use 64 thousand connections simultaneously, while in a worst-case scenario a million people behind a CGNAT

only have 16 simultaneous connections available per individual user[15]. Compare that number to the 50 simultaneous connections needed to load a typical website.

This is an example of a negative effect on the goal of a globally connected Internet. The exhaustion of IPv4, combined with the lack of IPv6 deployment, leads to starvation of resources for users, thereby weakening "Available capacity".

Supporting a Secure Internet

A secure Internet is resistant to attacks on its infrastructure, delivering a robust service to its user community. This means that its protocols and infrastructure, such as routing and DNS, should present a secure base that is resistant to both intentional attacks and accidents. In a secure Internet, data should have its confidentiality, integrity, and availability protected. Ideally, a secure Internet also does not create insecurity, such as botnets that are used in phishing scams. And the services and applications that run over the Internet itself should be secure, to the greatest extent providing defense in depth.

In this context, "secure" complements and relates to "trustworthy." When evaluating different proposed policies through the lens of the enablers both will often be taken into account.

Enabler	**Data confidentiality of information, devices, and applications**
Description	Data confidentiality, usually accomplished with tools such as encryption, allows end users to send sensitive information across the Internet so that eavesdroppers and attackers cannot see the content or know who is communicating. Allowing the transfer of sensitive information helps create a secure Internet. Data confidentiality also extends to data-at-rest in applications and on devices. (N.B., "confidentiality" also contributes to privacy, which is part of a trustworthy Internet)
Questions	Does the proposed change strengthen or weaken the ability of users to preserve the confidentiality of their information in transit or at rest? If this change is implemented, will the underlying protocols of the Internet provide stronger or weaker confidentiality?

Example 1: The Payment Card Industry (PCI) Data Security Standard (DSS) is a global standard that applies to anyone who handles payment card data. PCI DSS requires that data-in-motion must be encrypted, and

15 We assume the network operator only has a /24 of address space available, the largest block that is currently allocated by RIRs. That way a million users rely on 256 addresses times 64 thousand ports.

that data-at-rest must be protected using technologies such as encryption. By creating an 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 in an area, commercial transactions online, that have become integral to digital society.

This is an example of a positive effect on the goal of a secure Internet, by strengthening "Data confidentiality of information, devices, and applications" by requiring encryption to protect confidential and sensitive information.

Example 2: Mauritius recently proposed that all social media traffic be decrypted, inspected, and archived. The rationale was based on the relatively obscure local language and lack of physical presence of major social media organizations, leading to a poor response time to legitimate complaints from Mauritius. If it had not been dismissed, the proposed change would have impacted Internet security for people in Mauritius and their correspondents by dramatically reducing the confidentiality of information exchanged over social networks. Unfortunately, such proposals are becoming common around the world.

This is an example of a negative effect on the goal of a secure Internet by weakening "Data confidentiality of information, devices, and applications" by requesting the removal of protection of information exchanged between correspondents online.

Example 3: Most[16] websites have added encryption to provide data confidentiality for their users. This added security is based on standardized protocols (TLS/HTTPS) and frameworks to ground the encryption process securely using digital identity certificates and trusted certification authorities (CAs). Together, the certificates, CAs, and all the processes and rules that govern this ecosystem[17] are generically referred to as "the WebPKI" (for "web public key infrastructure"). While there are many legitimate criticisms of different aspects of the WebPKI, the overall result is that Internet users are able to easily and transparently use encryption to provide greater confidentiality to their Internet activities.

This is an example of a positive effect on the goal of a secure Internet, strengthening "Data confidentiality of information, devices, and applications" through a combination of industry standardization and implementation by application developers.

Enabler	**Integrity of information, applications, and services**
Description	The integrity of data sent over the Internet, and stored in applications, is not compromised. That is, information sent over the Internet shouldn't be modified in transit, unless directed by the communicating parties (e.g., a captioning bot may be useful to turn spoken words into text).

16 More than 90% of web traffic is secured by HTTPS https://transparencyreport.google.com/https/overview?hl=en

17 See, for example the CA/Browser Forum at https://cabforum.org/ and the output of the IETF working group on PKI at https://datatracker.ietf.org/wg/pkix/documents/.

	Critical underlying Internet services, such as DNS and the routing system, cannot be manipulated or compromised by malicious actors. Data stored in applications cannot be manipulated or compromised by third parties.
Questions	Does the proposed change strengthen or weaken the integrity of data, or the ability of users to verify that data are not corrupted? Does the proposed change strengthen or weaken the accuracy and integrity of Internet services, such as DNS?

Example 1: Resource Public Key Infrastructure (RPKI) is a combination of technology standards and Internet-hosted databases that help to increase the integrity of routing across the Internet. With RPKI, IP address holders can publish information about how their address blocks should be routed; at the same time, network operators such as ISPs can use the information published in the RPKI system to validate routing updates and avoid malicious behavior such as hijacking of IP address space.

This is an example of a positive effect on the goal of a secure Internet by increasing "Integrity of information, applications, and services" as far as the Internet routing system is concerned.

Example 2: In 2011, S.978, the "PROTECT IP Act" was proposed in the United States Senate. The bill contained a variety of technical requirements for Internet content filtering, including intercepting and modifying DNS queries and responses. The proposed legislation would also have been inconsistent with an important Internet security technology, DNS Security Extensions (DNSSEC), and would have resulted in a stifling of DNSSEC deployment. S.978 would have accomplished its goals, in part, by attacking the soundness and stability of DNS. (The bill never went to a vote at the Senate).

This is an example of a negative effect on the goal of a secure Internet, by weakening "Integrity of information, applications, and services" for the DNS system.

Supporting a Trustworthy Internet

Unlike security, trustworthiness depends not only on the state of the Internet, but also on the state of people and organizations that use and participate in it. The extent to which the Internet may be considered trustworthy depends upon an informed base of users who have the tools to evaluate trustworthiness, based on their current knowledge of the Internet's vulnerabilities and threats to it. [18]

18 Readers may find the terms "trusted" and "trustworthy" confusing. In our reading of the terms, the trustworthiness of the Internet can be assessed in a neutral way based on technical and policy elements that are generally objective. However, the user may not reward a trustworthy network with their confidence. An Internet that is trustworthy may still not be trusted. And an Internet that is not trustworthy may still be trusted.

The concepts of trustworthy Internet and a secure Internet are tightly intertwined: if the Internet is not secure, it cannot possibly be trustworthy. However, a completely secure Internet could still be untrustworthy if it violated user expectations or if some of its participants were not worthy of trust. Trustworthiness is not simply a matter of security.

Enabler	**Reliability, resilience, and availability**
Description	The Internet is reliable when technology and processes are in place that permit the delivery of services as promised. If, for example, an Internet service's availability is unpredictable, then users will observe this as unreliable. This can reduce trust not just in one single service, but in the Internet itself. Resilience is related to reliability: a resilient Internet maintains an acceptable level of service even in the face of errors, malicious behavior, and other challenges to its normal operations.
Questions	Does the proposed change create unpredictable variations in the Internet's reliability or in the reliability of a service or set of services? Will users be unable to know, from day to day, whether they can use the Internet and its services? Does the proposed change increase or reduce the overall level of the Internet's resilience to malfunction?

Example 1: Statuspage.io is a commercial product that focuses on showing service status – up, down, or something in between – to the service's users. By creating an entire product around delivering this information, the statuspage.io team has delivered a tool to the Internet community that fills a niche and makes it easy to transparently communicate service status. Because statuspage.io is commercial, it has also inspired both open source and commercial competitors, further making this type of transparency tool widely available to network operators and information service providers.

This is an example of a positive effect on the goal of a trustworthy Internet, by strengthening "Reliability, resilience, and availability" by increasing transparency about service performance.

Example 2: Deliberate Internet shutdowns are often used at the country level during stressful moments, such as during highly contested elections, or at times of civil unrest. Governments in Belarus, India and Venezuela have all shut down their nations' Internet in recent years[19]. The result of these shutdowns can

19 See ISOC Pulse tracker https://pulse.internetsociety.org/shutdowns for more specific examples

be unpredictable Internet reliability. The reasoning and duration of these shutdowns is rarely transparent, further reducing trust.

This is an example of a negative effect on the goal of a trustworthy Internet by weakening "Reliability, resilience, and availability" through deliberate interruption of services.

Enabler	**Accountability**
Description	Accountability on the Internet gives users the assurance that organizations and institutions they interact with are directly or indirectly acting in a transparent and fair way. In an accountable Internet, entities, services, and information can be identified and the organizations involved will be held responsible for their actions.
Questions	Does the proposed change create non-transparent authorities or hidden actors? Is the effect of the change to create unaccountable or anonymous authorities who will affect the trust users have in the Internet?

Example 1: RFC 7725[20] defines a way for a website owner to signal to users that information is not available as a consequence of a legal demand. Websites, ISPs, and search engines that are blocking access to information because of some sanction can use the mechanisms from this RFC to be very transparent: "you can't see what you are looking for because, legally, we are forbidden from showing it to you."

This is an example of a positive effect on the goal of a trustworthy Internet by strengthening "Accountability" through increased transparency.

Example 2: The Global Internet Forum to Counter Terrorism[21] (GIFCT) aims to "prevent terrorists and violent extremists from exploiting digital platforms." As part of this mission, GIFCT maintains a database of images and videos deemed "terrorist content" to be shared among its members. When a video or image that matches one in the database is detected, the database users can act on this information[22]. This database has grown to have more than 300,000 images and videos. Because the database uses one-way hashes to identify elements, the actual videos and images are not stored. This creates a lack of transparency—researchers cannot review the database; regulators cannot audit it—with significant risks

20 RFC 7725: An HTTP Status Code to Report Legal Obstacles at https://www.rfc-editor.org/rfc/rfc7725.txt

21 See https://gifct.org/ and more specifically https://vimeo.com/564638166. Founding members of GIFCT include Facebook, Microsoft, Twitter, and YouTube.

22 "It is up to each consortium member how they leverage the database, depending on, among other things, their own terms of service, how their platform operates, and how they utilize technical and human capacities." (quoted from GIFCT Transparency Report 2020 at https://gifct.org/wp-content/uploads/2020/10/GIFCT-Transparency-Report-July-2020-Final.pdf) The Transparency Report makes it clear that GIFCT is struggling to find a way to increase accountability—but has not yet achieved a good solution.

for freedom of expression, such as censorship of non-English content. The breadth of the database is hard to control too, since in some cases it is hard to determine "terrorist content" with global applicability.

This is an example of a negative effect on the goal of a trustworthy Internet, by weakening "Accountability" through designing and widely deploying opaque blocking tools with little oversight and often little recourse for the user.

Enabler	**Privacy**
Description	Privacy on the Internet is the ability of individuals and groups to be able to understand and control what information about them is being collected and how, and to control how this is used and shared. Privacy often includes aspects of anonymity, removing linkages between data, devices, and communications sessions and the identities of the people to which they pertain.
Questions	Does the proposed change improve, reduce or eliminate users' ability to understand or control how their information is collected, or to control how this information is used and shared? Is the effect to provide or eliminate the possibility for a user to act anonymously or pseudonymously?

Example 1: The British government's 2021 Online Safety Bill obliges service providers to monitor and delete "legal but harmful" content. Campaigners suggest that in practice this will oblige service providers to scan content—including private messaging. The only way to do this would be to break end-to-end encryption, meaning "private" message platforms would be subject to surveillance by non-state and state actors, even without any allegation or suspicion of crime being committed.

This is an example of a negative effect on the goal of a trustworthy Internet as it weakens "Privacy" by creating hidden actors and hidden actions based on pervasive traffic monitoring[23].

Example 2: The California Consumer Privacy Act (CCPA) gives consumers more control over the personal information that businesses collect about them. While most of the CCPA is about manually communicated policies and disclosures, the current CCPA also requires that businesses honor opt-out signals from web browsers similar to those of "Do Not Track"; this gives a simple and easily managed way

[23] RFC7258 "Pervasive Monitoring Is an Attack", https://datatracker.ietf.org/doc/rfc7258/

for the end user to signal their privacy preferences. By encouraging standardized and automated privacy controls, such as the Global Privacy Control (GPC), the CCPA helps users better manage their privacy.

This is an example of a positive effect on the goal of a trustworthy Internet, strengthening "Privacy" by providing consumers with more control over their personal information that businesses collect.

Example 3: The EU GDPR was sweeping legislation that had as one goal the creation of significant privacy enhancements for Internet users. Although implementation of the GDPR requirements in many cases resulted in sub-optimal user experience, the regulation has largely positive effects on trustworthiness by making user privacy and privacy policies are part of the business model and design of current Internet services, which has a long-term effect of increasing trust.

This is an example of a positive effect on the goal of a trustworthy Internet, as it strengthens "Privacy" by making the requirements part of the business model and design of the services.