A policy framework for an open and trusted Internet

An approach for reinforcing trust in an open environment*

Beta version - This paper is intended to be used as input for the 2016 OECD Ministerial Meeting on the Digital Economy: Innovation, Growth and Social Prosperity and other fora where issues of Internet trust are being considered. It may be updated as a result of various dialogues.

Executive Summary

- Diminishing trust is a challenge for the Internet. To protect the opportunities of the Internet, we have to counter diminishing trust.
- Large scale data breaches, uncertainties about how our data is being used, cybercrime, surveillance and other online threats are impacting Internet users' trust, how they use the Internet, and hindering Internet adoption.
- Policymakers are facing an important challenge today: How to fully embrace the digital revolution while, at the same time, ensuring the safety and security of their citizens.
- The Internet Society believes the Internet needs a solid foundation in trust to achieve its full potential. Trust is a cornerstone for all successful connectivity strategies, in developing and developed countries alike. This can only be achieved through collective responsibility and collaboration.
- An 'open and trusted Internet' is a globally interoperable Internet that cultivates innovation and creates opportunities for all. Its foundation lies in user trust, technologies for trust, trusted networks and trustworthy ecosystem.
- This policy framework outlines an approach for addressing the complexities of building trust in an open environment such as the Internet. It describes **four interrelated dimensions of trust to be considered when developing policies for the Internet, and provides principles to help build a trusted Internet.**

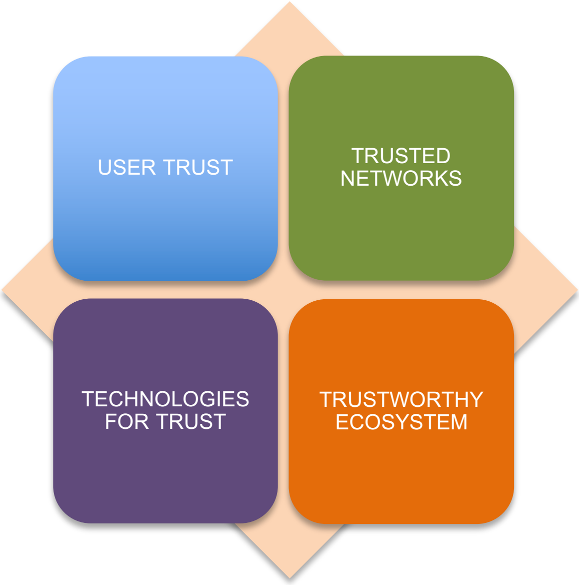

Fig. 1 The four dimensions for an open and trusted Internet

* *This framework is not intended to address issues of cyber warfare.*

Introduction

The open Internet offers economic and social opportunity for all. However, the Internet's full potential will only be realized if it has a solid foundation in trust. A recent survey in the US found that 45% of users had changed their online behavior because of their fears. Articles from around the world voice similar concerns. Internet users are anxious about how their data is being used by governments and business. They feel a lack of control, and worry about profiling and discrimination. They also fear that they will become victims of data breaches, identity theft, and other forms cybercrime. For some, this scenario has already become a reality. Internet users are also very troubled about the impact pervasive surveillance has on their privacy and other rights.

Many governments are now assessing the effects of the Internet on society. Some are concerned that the Internet is enabling and amplifying threats from criminals, other states, and even their own citizens. They are responding with stronger government controls, such as restricting access to content and impeding the use of social media channels. Some have imposed data localization measures to keep Internet traffic within their own borders. Others have considered banning key trust technologies (e.g. encryption) or forcing technology providers to create weaknesses in their products because they believe those technologies hamper law enforcement's ability to combat crime. Yet, without encryption and other trust technologies, there would be no secure banking or communications confidentiality for *any* Internet users. These policies result in the opposite of what is actually needed: they further damage user trust, remove opportunities and stifle innovation.

> *The Internet needs a solid foundation in trust for its full potential to be realized.*

Today, policymakers have a choice to make about which path to take in developing Internet policies. One path leads to an open and trusted Internet with all the social and economic benefits it brings. The other path leads to an untrusted and increasingly closed off network that fails to drive growth. One path leads to opportunity, the other to stagnation. The key is trust, and how to sustain the Internet as a fundamentally vibrant and trusted space.

The Internet: trust in an open environment

An 'open and trusted Internet' is a globally, distributed, interoperable network of networks that cultivates innovation and creates opportunities for all. Its foundation lies in user trust, technologies for trust, trusted networks and a trustworthy ecosystem. It offers inclusive governance, is built on sound policy principles and strives to put the interests of Internet users at the heart of decisions.

A 'trusted Internet' is not an island utopia, shut off from the threats of the world. There will always be risks and downsides to an open network system. Malicious actors will find ways to exploit vulnerabilities. Technologies and capabilities we develop to improve one part of life may negatively impact another. But, threats can be mitigated, risks distributed, weaknesses shared and repaired. The Internet's openness is also the means to protect it.

All stakeholders have a positive role to play in nurturing a trusted and open Internet. We need to work to secure core aspects of Internet infrastructure, to protect the confidentiality and integrity of the data that flows over it, and to ensure the right policies are in place to support the technologies, networks and actors that make the Internet work. We do this through collective responsibility and collaboration.

A useful foundation can be found in the principles of Collaborative Security: fostering confidence and protecting opportunities; collective responsibility; fundamental properties and values; evolution and consensus; think globally, act locally.

The Internet Society's policy framework for an open and trusted Internet outlines an approach for addressing the complexities of building trust in an open environment such as the Internet. It is described through four interrelated dimensions of trust that need to be considered when developing policies for the Internet, and provides principles to build a trusted Internet.

This framework for a trusted Internet embraces the important and valuable differences that give our world its rich diversity. There is no 'one size fits all' solution to decision-making about the Internet. Pro-Internet policies can take many different shapes, matching each country's unique needs. But one thing unites them all; their starting point is '*how do we build trust in an open environment such as the Internet?*'

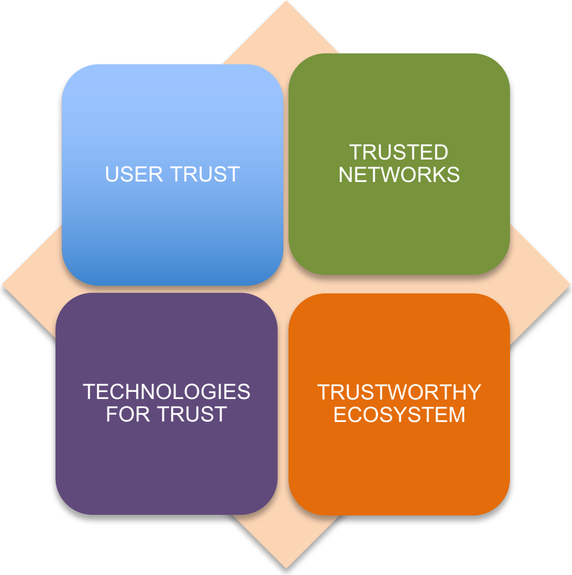

Fig. 1 The four dimensions for an open and trusted Internet

User trust: *How and why Internet users – including government, private sector and citizens - trust the Internet, and how to build that trust.*

Technologies for trust: *The technical building blocks for establishing and maintaining trusted networks, applications and services.*

Trusted networks: *The Internet's strength is that it is an ever-evolving collection of interconnected networks with distributed ownership and control. Trust is the glue that keeps networks connected and exchanging data.*

Trustworthy ecosystem: *How the Internet is governed and how it deals with Internet issues.*

This division finds its origin in the layered and modular nature of the Internet. A network of trusted networks provide global reach, while a set of technologies for trust allow applications that use the Internet to provide confidentiality, integrity and the ability to authenticate. With those technical legs in place, a trustworthy ecosystem allows for systemic trust, while user trust is the engine for all the creativity and innovation that we see on the Internet.

Trust is not just a nice idea. It is a set of choices, tools and capabilities already hard-wired into the open Internet.

Policy principles to support user trust

Human Rights: Human rights considerations should be integrated in Internet policies as they are developed, not added as an after thought. Individuals' rights must be protected on the Internet.

Communications confidentiality: Internet policies should support the principle that Internet users should have the ability to communicate confidentially online. They should also encourage innovation and the use of tools to facilitate confidential communications (e.g. encryption).

Privacy: Individuals' privacy rights and expectations should be protected on the Internet, irrespective of nationality or residence. There should be no pervasive surveillance of Internet communications. Individuals should have the ability to communicate anonymously or pseudonymously.

Consumer Protection: Consumers rights should be respected across the Internet. Governments should support consumer trust by enacting and enforcing consumer protection laws for business conducted in their territory or under their control. They should also engage in international cooperation across borders to ensure consumers' rights are protected no matter where they reside.

Control over data: Internet users should be empowered to exercise control over their data. They should have the ability to take their data from one service to another.

Transparency in policymaking: Governments should be open and transparent about their decisions, policies, laws and practices. They should actively involve stakeholders in Internet policy development.

Legal certainty: Governments should ensure that laws are clear, easy to understand and accessible to all. They should refrain from exercising lawmaking and enforcement powers capriciously or arbitrarily.

Enforcement and remedies: Governments should ensure regulatory authorities have the necessary resources and independence to provide effective law enforcement and remedies for Internet users who have suffered loss, damage or other forms of harm.

Non discrimination: Governments should ensure their laws and policies prevent the use of the Internet as a means to discriminate against an individual, based on the group, class or category to which that person or thing is perceived to belong to; or based on data profiling.

Watchdogs and Whistle-blowers: All stakeholders should recognize and support the value that watchdog organizations and individuals provide to society.

User trust

Everyone who uses the Internet is an 'Internet user', whether they are a government official, an advertiser, a school teacher, a travel agent, a student, an artist. Everyday we decide how much we trust (or distrust) the Internet for our social, professional, financial and other interactions.

User trust is important to the future success of the Internet because if users do not trust the Internet, they will restrict their use, and may even cease using it for certain activities. This could have a serious impact on the evolution of the Internet, its use and growth.

As far back as 1996, the Internet Architecture Board, the organization overseeing development of the Internet's technical protocols, recognized that the growth of the Internet depended on users having confidence that the network would protect their information and communications (RFC 1984).

However, building user trust does not mean simply reassuring people and hoping for a positive outcome. Building user trust means putting in place the right infrastructure (trusted networks), empowering users to protect their activities (**technologies for trust**), setting the right **policies**, and providing a responsive environment that properly addresses users' well-founded concerns (**trustworthy ecosystem**).

The policy principles for enhancing user trust enable individuals and organizations to make informed and rational decisions about how they use the Internet.

> *All of us - government, private sector, civil society and citizens - are Internet users. If we start by asking 'what can we do to make the Internet better for us as users?' we will already be half way to building a trusted Internet.*

Technologies for trust

Technologies for trust are the technical building blocks for establishing and maintaining trusted networks, applications and services. They are the technical foundation for a trusted Internet.

One commonly used trust technology is Transport Layer Security (TLS), a cryptographic protocol used to provide communications confidentiality and integrity, e.g. between a user's device and a website server. TLS was developed through an open process in the Internet Engineering Task Force (IETF). Today, virtually all banks and government online services use TLS.

Trust technologies are important for reinforcing trust on the Internet because they are the technical tools that enable Internet users to communicate privately (confidentiality), know who they are communicating with (authentication), know that the information they are sending or receiving has not been altered in transit (integrity), to restrict access to their data or communications (authorization), and know whether their device or technology has been tampered with (tamper-detection and resistance).

Technologies for trust are used to secure the networks, applications and services that we use everyday. Without trust technologies such as TLS and its predecessors, we would never have seen the explosion of online commerce that drives GDP growth and spreads opportunities globally. Without communications encryption, governments, companies and individuals would not be able to keep their communications confidential and their information secure.

Technologies for trust evolved thanks to a key characteristic of the open Internet – innovation that does not require prior permission or special approval from an authority. Permission-less innovation built the Internet and is essential for the future health of the Internet and the economies that depend on it.

As threats continue to emerge and grow, we must ensure we all have the necessary tools for privacy, security, and, ultimately, economic and social opportunities.

We need policies that support rather than hinder the development, availability and use of trust technologies.

Policy principles to support the use of trust technologies

Governments should:

- empower users to adopt their own technical measures of protection for their Internet communications and data;
- encourage the open development and open access to "easy-to-use" tools that enable users to communicate confidentially;
- encourage online service providers to offer their customers end-to-end encryption solutions.

Regarding encryption:

(These recommendations summarize the principles of the www.securetheinternet.org initiative, endorsed by many companies, individuals and organizations, including the Internet Society.)

Internet users should have the option to use, and companies should have the freedom to provide, the strongest encryption available, including end-to-end encryption, without fear that governments will compel access to the content, metadata, or encryption keys without due process and respect for human rights.

Governments should not ban or otherwise limit user access to encryption in any form, or otherwise prohibit the implementation or use of encryption by grade or type.

Governments should not mandate the design or implementation of "backdoors" or vulnerabilities into tools, technologies, or services.

Governments should not require that tools, technologies, or services are designed or developed to allow for third-party access to unencrypted data or encryption keys.

Governments should not seek to weaken or undermine encryption standards or intentionally influence the establishment of encryption standards except to promote a higher level of information security. No government should mandate insecure encryption algorithms, standards, tools, or technologies.

Governments should not, either by private or public agreement, compel or pressure an entity to engage in activity that is inconsistent with these tenets.

We depend on technologies for trust every day, to secure our networks, our transactions, even our lives. They need to be as strong and as ubiquitous as we can make them.

Trusted networks

The Internet is an ever-evolving collection of interconnected networks with no common ownership or centralized control. Trust is the glue that keeps networks connected and exchanging data.

> *Building and sustaining a trusted Internet means different players – with different roles and responsibilities – need to take action, closest to where the issues are occurring.*

There is no such thing as one single, global network – the Internet is a 'network of networks'. The communications path is not decided in advance, and it does not follow national borders. Internet users do not decide how their communications are routed: they simply "trust" that network operators will deliver the data where it needs to go. It is a transport strategy that may seem chaotic, but it provides resilience and speed on a scale that humanity has never achieved before.

Trust in this context is not a hope or a feeling; it is a practical and reciprocal way of 'doing business'. Network operators trust that their peers will carry out the operations needed to provide end-to-end communication. If an operator fails to live up to this trust, its peers will find other ways to route their traffic and simply cease to deal with it. This approach is important because it provides workable options and it does not allow the system to break down.

The keystone of trusted networks is **collective responsibility and collaboration**. This is the notion that all stakeholders must collaborate and share the responsibility for addressing Internet issues.

The core elements for trusted Internet networks are the Internet Society's Internet invariants and the Collaborative Security principles.

Adopting these core elements as the foundation for decision-making creates an environment in which trusted networks will continue to evolve and thrive.

Policy principles to support trusted networks

Security:

National cybersecurity strategies and policies should advance economic and social prosperity: they should not hinder growth, innovation or development.

In developing cybersecurity strategies and policies, governments should embrace the expertise of *all stakeholders* and work with them to collaboratively develop solutions.

Cybersecurity policies should integrate human rights: they should strive to provide safety and security, while maintaining individuals' rights.

Governments should lead by example, but also recognise that some stakeholders may be the leaders in their field. Sometimes the best solutions are those that emerge organically without any government direction. Solutions should be defined and implemented where they can have the most impact.

Cross-border collaboration will be essential for maintaining the security and resilience of the Internet.

Connecting networks and sending traffic:

Governments should not mandate data localization or prescribe Internet traffic routes.

Governments should encourage regional and international companies to participate in the local interconnection and peering environment (e.g. by reducing barriers and/or providing economic incentives).

Governments should foster investment in additional Internet infrastructure (e.g. submarine cables, IXPs and national infrastructure) for greater resiliency for the benefit of the whole Internet ecosystem.

Governments should provide a legal environment that supports competitive markets in online services.

Open technical standards:

Policies should support an Internet built on open technical standards. Stakeholders can show their support by endorsing and promoting the OpenStand principles.

Trustworthy Ecosystem: Attributes of successful Multi-stakeholder Governance

Inclusiveness and transparency: Inclusiveness is the basis of legitimacy in collaborative decision-making. Those significantly affected by a decision should have the chance to be involved in making it. Inclusiveness is not just an admirable goal, but an essential part of an effective process. The less inclusive a process is, the less likely it is to engender the trust and support of those outside of the process. Transparency is an essential condition for inclusiveness, as it brings expert and affected groups into the process. Transparency of inputs, process and decision-making is fundamental to the Internet.

Shared responsibility: All stakeholders share collective responsibility for the continued vitality of the Internet and the benefits it brings our societies and the global economy. In the technical community, we share a sense of *collective stewardship* of the Internet and the open standards its technologies are based on.

Effective decision-making and implementation: The most effective decisions are those based on an open and deliberative process that considers a broad range of information sources and perspectives. This holds for both the quality and implementation of the decision.

As the Internet is operated by a variety of public and private sector and civil society stakeholders, successful implementation of decisions needs imaginative and collaborative solutions. It is not as straightforward as passing a national law. Stakeholders who have been part of the process work harder to make its implementation a success.

Collaboration, distributed and interoperable governance: To effectively harness the efforts of many actors, the technical community has evolved autonomous governance systems based on collaboration and mutual respect. The many organisations involved in Internet governance have complementary roles to play. We need to recognise this autonomy and keep dialogue and mutual participation in areas of overlap between organisations.

This is a summary of the characteristics of successful Internet governance approaches in the Internet Society's '**Internet Governance: Why the Multi-stakeholder Approach Works'**.

Trustworthy ecosystem

When governments make policies for the Internet, they think about more than just 'do we trust the Internet for our own use?'. They also think about the impact the Internet may have on their citizens' safety and well-being, their economy, their sovereignty, as well as 'who has control'. Balancing all these interests, is a much more complex trust equation than user trust. But, it is critical to address because this is why governments focus so intently on the trustworthiness of the Internet ecosystem and its governance.

The trustworthiness of the Internet ecosystem stems from how it was developed and its multi-stakeholder governance processes, where those affected by decisions have the opportunity to be part of them.

The Internet became a global platform for innovation and economic growth through participatory bottom-up processes, prioritising the stability and integrity of systems, and maintaining the open nature of the underlying technologies. These principles are part of the Internet's 'DNA'.

At its core, multi-stakeholder governance embodies transparency, inclusiveness, shared responsibility, embraces accountability, and is effective at solving common Internet issues.

Additionally, in the technical community, we share a sense of collective stewardship towards the public core of the Internet and the open standards on which its technologies and networks are based.

These characteristics fortify stakeholder trust in the way that the Internet ecosystem is operated and governed.

> *The Internet does not present a 'command and control' problem; it is a coordination challenge. How can we work effectively with those responsible for all its different parts, many of whom are beyond our borders?*

Conclusion

To ensure the benefits of the digital economy reach everyone around the world, and that innovation thrives, we need to build an open and trusted Internet together. We believe this policy framework provides an approach for addressing the complexities of building trust in an open environment such as the Internet.

We ask you to think about these different trust dimensions, and how they are all inter-related, as you consider policies related to the Internet. We also encourage any feedback you may have about this policy framework for an open and trusted Internet. Please send your comments to trust@isoc.org

An open and trusted Internet is vital to the success of the digital economy. We need to work collaboratively to make this a reality.

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva
Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave.
Suite 201
Reston, VA 20190
USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881
Email: info@isoc.org