DC Core Internet Values discussion paper 2017

Focus on Freedom from Harm

Introduction

The Internet connects a world of multiple languages, connects people dispersed across cultures, places knowledge dispersed (or concealed) across cultures accessible to every culture. The Internet is more than an invention. It is a precious gift to humanity as an opportunity to connect globally and evolve. The Internet connects people and their devices. The Internet is beyond what was foreseen at the time of the invention of its protocols. Its values were not intentionally built in, but contained within and become manifest and understood along its path of evolution.

The Internet has become increasingly a support for all kinds of human activity, constructive, destructive and ambivalent as this may be. The Internet has been used to foster never-imagined levels of communication, access to information and creativity, and given rise to businesses and social transformation that reach both those connected and many who are not. Accompanying these generally positive trends, cybercrime, verbal and non-verbal abuse, and interference with human rights have also appeared on the Internet. Some forms of abuse and some attempts to correct or modulate conduct on the Internet may impinge on the way the Internet operates, as may be the case with ways to block content from reaching certain destinations or to restrict the technological features that enable businesses and social transformation.

The Dynamic Coalition on Core Internet Values, which began its work as the Workshop on Fundamentals: Core Internet Values during IGF 2009 at Sharm El Sheikh, chaired by then Internet Society President Lynn St. Amour, progressed as a Dynamic Coalition and has deliberated since 2009 on fundamental questions such as “What is the Internet? What makes the Internet what it is?” to define the Core Values that characterize the Internet.

The Dynamic Coalition in its recent deliberations during and between the Internet Governance Forums discussed the recent socio-political developments and the specific threats to the way the Internet evolves and functions. Some of Internet’s technical principles seemed to be challenges to adhere to, in their intended form. For instance, the relevance of the end-to-end architecture became questionable in the face of real world threats of the recent past. Such challenges gave rise to the question whether the values are unalterable at all.

The Internet is global, open, end-to-end, shared and distributed without central points of control.

“Value” and “values” are not to be used loosely. Values are what are profound, values are beyond evaluation and debate, values are as understood. Known and respected and beyond notions of utility, relevance or evaluation by any other yardstick.

The Dynamic Coalition will seek in its 2017 session to better delimit its scope. Experience from the last few years shows that as one moves from the better-defined technical principles like Interoperability to the broader-sense wordings like “Free” the ability to even discuss them is lost in a muddle of culturally-tinted points of view, and overlaps more than necessary with the subject matter of other Dynamic Coalitions.

Whilst Core Values are imprescriptible, challenges emerge and vary from time to time.

One striking feature of the Internet is its ability to evolve with little or no change in its fundamental design principles and the order in which they are prioritized. Further, it has a mechanism, mainly in the IETF, to make the adaptations that become necessary. Further layers like that coordinated within the ICANN ambit, are modelled on the same open processes and have successfully preserved interoperability, openness, etc. and propagated them to the layers above and below the internetworking layer.

Core Internet Values

- Global – The Internet is a global medium open to all, regardless of geography or nationality.
- Interoperable – Interoperability is the ability of a computer system to run application programs from different vendors, and to interact with other computers across local or wide-area networks regardless of their physical architecture and operating systems. Interoperability is feasible through hardware and software components that conform to open standards such as those used for internet.
- Open – As a network of networks, any standards-compliant device, network, service, application, or type of data (video, audio, text, etc.) is allowed on the Internet, and the Internet’s core architecture is based on open standards.
- Decentralized – The Internet is free of any centralized control.
- End-to-end – Application-specific features reside in the communicating end nodes of the network rather than in intermediary nodes, such as gateways, that exist to establish the network.
- User-centric – End users maintain full control over the type of information, application, and service they want to share and access.
- Robust and reliable – While respecting best-effort scenarios for traffic management, the interconnected nature of the Internet and its dense mesh of networks peering with each other have made it robust and reliable.

To evolve or not to evolve

The Internet evolves around the principles that remain at its core. When there is a new development, for instance, “wireless modems” “smartphones” or “micro-devices” the Internet evolves along its path of evolution, without the compulsions to “remove” any of its values, or

without the need to “add” a new value around which the evolution would progress. What is “new” is in the realm of evolution, not in the core of values.

One could say outright that Core Internet Values are unalterable and that the list of values themselves cannot be amended nor expanded. However, this question has been discussed in past years and when “Freedom from Harm” was introduced, it appeared to be accepted as an additional Core Value. In fact, debate during last year’s session went further, taking evolution for granted, but attempting to define whether there should be enforcement of this value in particular.

A starting point was that “There should be no overarching system and industry self-certification might be a solution moving forward”. That could be true for all Core Values.

In the history of the last four decades, Internet design principles have mapped well to some social values which are widespread but not universally accepted, nor free from interpretation. Societies that are against openness have difficulties with the Internet. Companies that act against interoperability cause problems to the Internet. Regulations that make end-to-end difficult make the Internet's life harder (witness Network Neutrality.)

So any serious modification and some possible additions to this short, compact, proven list may make the Internet be less of what it is and can be. The proposal is therefore that the DC-CIV work within a framework that assumes immutability over decades.

As one of the panellists on the Coalition’s session at IGF 2016 mentioned: consider “Freedom from Harm” in the context of the general principle “do no harm”. Then this overarching principle is applicable to all Core Internet Values. By extension, Freedom From Harm does not contradict any Current Core Internet Values.

Freedom from Harm

What is freedom from harm?

The Internet needs to become a much safer place and the people that designed it did not foresee misuse of devices.
Malware is a technical challenge and there is difficulty in applying software updates across the network, especially for the Internet of Things (“IoT”).
Proposal for a new Core Value for the Internet: Freedom from Harm (“FFH”), which should drive the technical community’s work in the coming years.

Why is this needed?

In its core design principles, security was not ignored. The team of people that designed the Internet were using the maximum security available at the time, working with extremely sensitive assets. The security was on the systems, it was evolving fast, and it made little or no sense to implant security into the network itself as it would not scale and would not adapt to innovations

without needing to tear down and replace the whole network for each new advance, say, in cryptography. However, today the threats are different, more sophisticated and the range of devices that these threats can affect are more diverse than when the Internet was first invented.

How could it be implemented?

Without altering Core Values.

Transparency

One way to face these risks, and adding to the principle proposed, is to introduce/increase transparency and accountability for all responsible players, such as device manufacturers, regulators in charge of approving the sale of devices, software developers, etc.

Standards Development

Implementation issues could be mandatory for all Standards development. Would the IETF add a section on FFH considerations to RFCs? How would other standards-development organizations (SDOs) treat the principle?

1. Technical means to inhibit harm
2. Detect harm and act against its source, e.g. legal means, prosecution.
3. Moral persuasion: put pressure on programmers and others responsible for products which can be harmful

Overall, the accountability of technical standards-makers must be clearer.

A Multi-Stakeholder way

Is there an “Internet way” to approach this problem? A multistakeholder, Internet-proper mechanism such as the IETF or ICANN in their respective fields?

Coordination

Work already being done against attacks (prevention, mitigation, isolation, response, etc.) should be considered. Coordination of such work in an open manner could bring synergies together for a safer Internet whilst avoiding the risk of creating “walled gardens”.

Certification / Good Practice

This is found to be a challenge in a network of networks that spans the whole globe.

On the one hand, one could foresee solutions in from other fields: for example, the certification of electrical devices in the US through Underwriters Laboratories (UL) thus a “cyber-UL” could be developed to certify the safety of Internet devices and systems and could operate with partial automation, based on voluntary submissions. On the other hand, safety standards are mostly predicated within a context of national laws. A principle like “thou shall not develop bad code” isn’t working well. Bad systems are being used because they are novel, useful and exciting, with pressure on time-to-market causing some to cut edges. Thus, on a borderless Internet, no safety standards can be enforced.

This brings us to the potential for a set of Good Practice Standards which are voluntarily adhered to. These should not be the remit of a single overarching authority. They should be collaborative in scope, open, and should be promoted by all stakeholders, including Government, the Private Sector and Civil Society.

Steps forward

Focus the DC on CIV to concentrate more on the technical design principle than on the higher layer rights and values, which are much less well-defined, and universally variable.

Work with other stakeholders to build a set of Good Practice Standards that will enhance “freedom from harm” in a technical perspective.

It is expected that this work should include collaboration with the Dynamic Coalition on Internet of Things (DC-IOT) in particular. Collaboration with other Dynamic Coalitions is being considered too.