Towards Reform of Global Internet Technical Framework

- Area: COMBINED INTERNET GOVERNANCE PRINCIPLES AND ROADMAP
- Entitled by: Rishab Bailey
- Region: India and Brasil
- Organization: The Society for Knowledge Commons
- Sector: Civil Society
- Keywords: encryption, decentralisation, open source, social platforms

Abstract

In addition to mass surveillance, principles and governance structures are required to address the monopolization and commodification of information and knowledge; abusive use of personal data - in particular its unchecked monetization, the erosion of cultural diversity, the concentration of power in the hands of one state and technical decisions that lead to social injustice. While policy and legal frameworks are required to ensure a reformed and internationalized Internet, many of the solutions for the future of Internet governance are technical, and without a technical grounding many of the policy and legal frameworks might be meaningless.

Document

Knowledge Commons appreciates the opportunity to present a submission on the technical architecture that will be required for a more democratic Internet to the Global Multi-stakeholder Meeting on the Future of Internet Governance. While policy and legal frameworks are the principle focus of the NetMundial meeting, many of the solutions for the future of Internet governance are technical, and without a technical grounding many of the policy and legal frameworks might be meaningless.

As an organization that includes technology specialists, we offer the following observations and recommendations on the understanding that good engineering and technical solutions will require political and social support.

The technological architecture that worked when the Internet was born and grew in its infancy is in many ways outdated. The impetus for the NetMundial arose because trust and confidence in the Internet was fundamentally undermined by mass surveillance and economic espionage, both possible because of the Internet's technical architecture.

Leaving current practices, protocols and infrastructure unchanged poses risks to the privacy of citizens, the capacity of governments to engage with one another in trust, and the ability of the financial system to function. Therefore there is a need to alter the technical architecture of the Internet.

1. The future growth of the Internet needs to emphasize decentralized architecture and more evenly distributed infrastructure

Decentralization and distribution of network architecture is needed to improve the storage and privacy of data.

The Internet's infrastructure of copper, fiber optic cable and satellite communications is global and often described as a decentralized network of networks. However, the bulk of global voice and Internet traffic passes through the territory or company servers of one country and is subject to its laws.

This centralization of ownership and control of physical cables, routers, servers and data is at the core of the problem's made clear by the revelations of Edward Snowden; if all the data is going through a single location it is vulnerable to the back doors in software and hardware utilized by agencies of that country. Scholars have described this as 'governance by architecture' or 'governance by design'.

The global north currently owns the cloud and most of the fiber optic cable. Countries in the global south should be encouraged to aggressively lay their own cables and generate domestic cloud capacities, to protect privacy and encourage local innovation and competition via architecture.

The question of being connected is urgent for 5 billion people currently not enjoying access to the Internet. However, connecting them with the most polluted tools, storing data and applications in locations unknown and routing data through jurisdictions that do not guarantee their rights will simply magnify the privacy and security problems currently experienced by the 2 billion people online.

Naming systems are essential for the Internet to work, but the current naming system is hierarchical and gives control to entities in control of this hierarchy. Control over the naming system has led some parties to illegally take over domain names without due process.

2. Free and Open Source Software and Hardware without backdoors

When we do not know what our machines are doing and what is on our motherboards, we cannot have communication and services that uphold our universal human rights to privacy, freedom of expression and association. To ensure that, software and hardware should be fully auditable and interoperable. Only Free and Open Software and Hardware implementing Open Standards can give us the chance to stop the backdoors, allowing complete auditability and interoperability.

An open and decentralized Internet requires strict enforcement of open and public standards, which allow fully interoperable implementation by anyone in any type of software and hardware. The trend towards privatization of digital standards must be stemmed and measures must be introduced to ensure that standards are publicly owned, freely accessible and implementable.

The applications and protocols necessary for a connected life must be free and open source. These include operating systems, mobile phones basebands, distributed data storage, email clients, instant messaging and video/voice communication. User friendly and affordable technical solutions need to be made available to individuals and governments. A strong responsibility lies with technologists and their industries to provide more user friendly, easy to run solutions and options for secure communications.

The long-term solutions, particularly hardware production, requires enormous human and economic resources, but every citizen will benefit from free software and open hardware that is verifiably safe and based on architectures that does not give power to a central or single entity.

3. Private social platforms put users at risk, and compromise local interests

Commercial social media platforms displaced the open distributed systems that made up the original applications used on the Internet, rather than platforms based on open protocols like email, Usenet, IRC etc. People communicate on sites like Facebook and Twitter and rather than hosting media on their own web servers, with domains under their control, they use sites like YouTube and SoundCloud. The commercial nature of these companies means that collecting data on their users is required for them to make profits.

These are global north based companies with a market position that allows them to dominate global markets, thereby squeezing out local alternatives and collecting massive amounts of data on citizens of other countries without regulatory oversight.

Public funding was necessary to build out key infrastructure like the telephone system and the railways, and public funds continue to support local culture in many countries by way of supporting public broadcasting on TV and radio, and provides funding for local film and arts. In order for a free Internet to be developed for the best interests of local citizens and local business, public funds will need to support development of tools that will give users alternatives to the social media monopolies. These applications and tools must be open and distributed on nature, and designed to protect the users privacy.

4. Strong encryption must be mandatory in all core protocols

There are a large number of core protocols that currently have strong cryptography added as an afterthought, if at all, and frequently have optional insecure fallback modes, which can be in various cases coerced by an attacker. Many protocols containing sensitive information are communicated in the clear, and many protocols requiring validation of authenticity are sent without any such authentication, making fake identity attacks trivial.

To guarantee that citizens have their privacy protected, all cryptographic libraries used in the core protocols should be open and frequently verified, so that their implementations will be safe for global usage.

5. There is a difference between what is technically possible and what is legal or acceptable – new agreements will require trust and technical verification

This difference is recognized in International Humanitarian Law – the laws of war – where indiscriminate weapons and torture are outlawed. New treaty agreements – or additional protocols to existing treaties – are needed to apply similar limits to online activities, to elaborate rights and prohibit certain acts.

Existing treaties, human rights and trade instruments oblige governments to secure data, protect citizen's human rights to privacy and freedom of expression, and to not spy on each other's citizens. These treaties all recognize that there are legitimate surveillance activities and actors, and provide a license for them to act with proper oversight and warrants based on reasonable suspicion of wrong-doing. However, we now know that governments and corporations are bypassing oversight and abusing the capacity to surveil their own citizens – and those of foreign countries – just because they technically can.

The technology can be configured differently.

Technical experts will be needed to ensure that any new principles agreed upon by governments actually prohibit and police indiscriminate data collection, backdoors into software or hardware, the hacking of submarine cables, the sabotage of networks etc. And new standard operating procedures with regular reporting on arrangements between governments and corporations that protect private data will need to be implemented.