

Just Net Coalition statement on Internet governance

([Just Net Coalition](#) is a global coalition of civil society actors working on Internet governance issues)

All states should work together to provide a new global Internet Governance model that ensures human rights, as well as equity and social justice for all people of the world

The US led model of Internet governance that developed alongside the rise of the Internet has failed to respond to deep violations of human rights, and overall in ensuring economic equity and social justice. In particular, it has given rise to mass surveillance, abusive use of personal data and their use as a means of social and political control; the monopolization, commodification and monetisation of information and knowledge; inequitable flows of finances between poor and rich countries; and erosion of cultural diversity. Many technical, and thus purportedly 'neutral', decisions have in reality led to social injustice as technology architectures, often developed to promote vested interests, increasingly determine social, economic, cultural and political relationships and processes.

In view of the Internet becoming a major driver of change in society today, there is a need for a new model of shaping and governing the Internet, as a global commons, that embeds and promotes human rights, and endeavours to ensure equity and social justice for all citizens of the world. All countries should work together for formulation of alternate models of Internet governance, which would include new Internet platforms and digital tools. Such new models should not only ensure a more people-centric Internet, but also break the monopoly of a few global corporations who with their national government partners are both commercialising public and commons data and contributing to the building of an integrated global surveillance state.

The Just Net Coalition, a global civil society coalition, calls on all countries to work together towards a reform of the current US dominated Internet governance structures. We further call on all countries to recognise that freedom of expression and the right to privacy are fundamental on the Internet as elsewhere, and that there is an urgent need to ensure a just and effective distribution globally of the rewards and benefits of the digital economy. These elements are tightly linked: there can be no true freedom of expression without privacy, and freedom of expression is instrumental in achieving economic and social equity. In particular, we recommend the following:

1. Internet related standards and critical resources (including names and numbers) should be developed in a manner that ensures an open and consistent Internet architecture, in conformance with the global public interest, upholding people's civil, political, economic, social and cultural rights, as well as the right to development.
2. It must be ensured that the online, like the offline realm, is subject to legitimate political authority and jurisdictions and not to private law and policing as is increasingly the norm. Such a regime should be rights-based and democratic. We invite all countries to call for a Framework Convention on the Internet and to take up leadership in developing global Internet-related policies.

3. We welcome the initiative in the UN Human Rights Commission to develop a treaty for putting measures in place to prevent human rights abuse by Transnational Corporations. We invite all countries to support all such initiatives. We also invite all countries to promote policies that ensure that the Internet is a platform for global sharing of knowledge, and resist the Intellectual Property Rights (IPR) intensive Internet governance regimes that are creating monopolies and extracting unreasonable and inefficient global economic rents.
 4. All countries should participate in the development of new open Internet platforms and tools including in the areas of search, operating systems, data storage and cloud services in order to break with the current mass surveillance and rent-seeking based business models. These functionalities should be made available to all as public utilities and in the languages of all peoples. As an Appendix to this statement, we provide detailed recommendations for taking some concrete steps in this direction.
-

Appendix **Concrete steps towards trustworthy Information and Communication Technologies (ICTs)**

This paper argues that countries should collectively invest in the development of a suite of open source software to enable secure communication over the Internet, providing viable alternatives to the monopoly and rent-seeking products and services that currently dominate the space.

While some larger and IT-wise more active countries are well placed to lead the development of new Internet platforms and tools given that they have the necessary skill sets, large internal markets and political motivation to break the mass surveillance business model, other countries can join this effort, and contribute to and benefit from it.

Snowden's revelations have demonstrated the need for secure email, calendaring, messaging, search, file sharing and storage and video systems, which would protect all countries' economic and cultural spaces, as well as leaders and citizens from Five Eyes spying.

Recommended options

1. A MOU to be agreed and signed among participating countries establishing a strategic framework for cooperation on science and technology and IT and including an explicit commitment to collaborate on secure open source software and communications hardware.
2. Participating countries establish a fund to support development of a secure decentralized communications stack of open source software solutions for email, instant messaging, video conferencing, and file sharing and storage designed to run on today's Internet. In particular, tools for securely encrypted communication must be improved and made easier for widespread use by less experienced users.
3. Participating countries commission a feasibility study on options for

collaboration towards commissioning a suite of secure software and communications hardware.

4. Participating countries commission on-going research into new standards, protocols and technology that could form the basis of a next-generation Internet. With appropriate changes it will in particular be possible to significantly improve the security of “who communicates with whom” metadata.

5. Participating countries engage with civil society and local industry regarding this initiative and encourage their voluntary participation.

Why the Development of Alternate On-line Platforms and Tools Using FOSS is needed

Vulnerability to mass surveillance results from the use of insufficiently secure services, many of which maintain centralized databases. Indeed, the vast majority those with Internet access use tools and platforms such as Google, Facebook, PayPal, Amazon, Twitter, Yahoo, and Microsoft. Since those companies are headquartered in the US, they are subject to US law. While US citizens may have some protection under the 4th Amendment, non-US citizens have none under existing US laws. Data held in the US cloud, or in any server of a US company located anywhere, is subject to US law. This makes the passage of laws to mandate local data storage less effective than establishing alternative platforms.

Dominant positions such as those of Google, Facebook and Yahoo can and must be broken with the design of appropriate alternatives. Google, Facebook and Yahoo control more than 40% of the global digital advertising revenue of \$117.6 billion (2013), with Google alone raking in \$38.6 billion. Fifty per cent of Google's revenue comes from its dominance in the search engine market, where it holds nearly a 70% share of the market, with Baidu coming in as a distant second. US policies in Internet governance are tailored to protect the monopoly of these companies. As these companies grow, so does the ability of the US to expand its surveillance overreach.

The dominance of US Internet companies has also resulted in English becoming the most commonly used language on the Internet; with only about 12.5% English speakers, English is the language of about 55% of the world's Internet content. Preserving local languages, literature and culture also requires that the current monopoly position of the dominant Internet companies be reduced.

The popularity of these platforms comes from their ease of use, ability to use multiple tools across a common user interface and platform, and the quality of their “free” products (the true payment being in the loss of control over one's private data). In economic terms, it is the economies of scale and network effects that have resulted in more and more people joining these on-line platforms.

The Post-Snowden Imperative

The Snowden revelations have made clear that cloud services and social media have been deeply compromised by the NSA and other intelligence agencies. It is not just private data that has national security implications but also data that pertains to international negotiations and economic issues. The global Internet

giants have been either willing parties in US spying or, being located in the national jurisdiction of the US, are required by law to permit mass (and targeted) surveillance. Additionally, as more data is centralized in the databases of a small number of US companies, mass surveillance becomes ever easier. For example, as we have seen with the US Foreign Intelligence Surveillance Act (FISA) order on Verizon, one order may involve the collection of millions of users' data.

If countries want to protect their citizens, and also their economic and cultural integrity, it is necessary to focus on how they can they make available alternate tools that will provide a similar degree of user comfort with a similar quality level of services. As long as there are no comparable products, it is difficult for people to stop using these platforms. This means building alternative equivalents to Gmail, Facebook, Twitter, YouTube, and search engines that can provide the same services to users that Google and the others provide. These also must not be based on proprietary platforms as closed platforms cannot be examined by independent experts to ensure they do not have backdoors that allow surveillance. There is thus a need for a Free and Open Source Software (FOSS) approach to the development of such platforms.

Why should we use a FOSS based approach to develop such platforms?

The advantage today in attempting to create an alternate set of tools or platforms is that, already, FOSS communities have created:

- Operating systems such as GNU/Linux that are relatively much more secure and already popular
- A large set of tools that are available to create packages/suites/platforms
- A large support base for FOSS already available in key countries such as BRICS (Brazil, Russia, India, China, and South Africa)

There are three important reasons for a FOSS approach and not a proprietary approach. The first is that, as the code is public, it is very difficult to embed backdoors into such software. This would also make such platforms more easily acceptable worldwide; it would not be seen to be a potential but competing surveillance platform to the existing US one. The second is that there is a global FOSS community that has already developed or is developing tools that can be easily embedded into such platforms. The third is simply the cost issue - with the level of free software tools available and collaboration with groups working elsewhere on such packages, the costs of creating such platforms would be relatively much less than attempting a proprietary approach.

Already, countries such as Brazil and India have committed themselves to open standards and use of FOSS in government activities, wherever feasible. Support by major economic blocs like the BRICS and European Unions (EU) for FOSS through such projects would also help in promoting open systems - both hardware and software - and in this way could reduce the monopoly of the US based software and hardware companies.

Without governmental support, it is difficult, perhaps impossible to combat the dominance of global Internet monopolies.

<http://JustNetCoalition.org>, info@JustNetCoalition.org

The Just Net Coalition (JNC) is a global network of civil society actors committed to an open, free, just and equitable Internet. Founded in February 2014, the coalition engages on topics of the Internet and its governance, with the goal to promote democracy, human rights and social justice. Our founding principles and objectives are contained in the Delhi Declaration: <http://justnetcoalition.org/delhi-declaration> .