Just Net Coalition statement to the BRICS Summit in Fortaleza, Brazil

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

BRICS must 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 in the unipolar world since the 1990's, resulted in mass surveillance, violation of people's rights, and an enormous concentration of economic power in the hands of a few US-based global corporations. This model excludes major sections of the global population from full participation in, and the benefits of, digitally enhanced development. The current governance structures have failed to respond to deep violations of human rights, and overall in ensuring economic equity and social justice.

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 ensures equity and social justice for all citizens of the world. The BRICS, as a group of countries representing about 40 % of the world's population and almost 30% of the world's GDP in Purchasing Power Parity (PPP) terms, are uniquely placed to formulate an alternate model of Internet governance as well as to lead in the development of new Internet platforms and digital tools. Such developments can 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 the BRICS countries meeting in Fortaleza, Brazil, to provide leadership to the world towards a reform of the US dominated Internet governance structures. We further call on the BRICS countries to take a leadership position in recognising 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. 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 digital, 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, as achieved in Brazil through the Marco Civil legislation. The BRICS should call for a Framework Convention on the Internet and take up leadership in developing global Internet-related policies.

3. We welcome the initiative in the UNHRC to develop a treaty for reining in human rights abuse by Trans-National Corporations. The BRICS leadership must strongly support all such initiatives. They must also promote policies that ensure that the Internet is a platform for global sharing of knowledge, and resist the Intellectual Property Rights (IPR) intensive Internet fovernance regimes that are creating huge monopolies and extracting unreasonable and inefficient global economic rents.

4. BRICS countries should lead the development of new open Internet platforms and tools including in the areas like search, operating systems, data storage and cloud services given that they have the necessary skills, large internal markets and political motivation to break with the current mass surveillance and rent-seeking based business models. These should be made available to all as public utilities and in the languages of all peoples. As an Annex to this statement, we provide detailed recommendations to the BRIC countries for taking some concrete steps in this direction.

Appendix: Concrete steps towards trustworthy ICT

This paper argues that BRICS 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 US products and services that currently dominate the space.

BRICS countries are uniquely placed to lead the development of new Internet platforms and tools given they have the necessary skill sets, large internal markets and political motivation to break the mass surveillance business model.

Snowden's revelations have demonstrated the need for secure email, calendaring, messaging, search, file sharing and storage and video systems, which would protect BRICS 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 BRICS Science and Technology and IT Ministers establishing the strategic framework for cooperation on science and technology and IT include an explicit commitment to collaborate on open source secure software and communications hardware.

2. BRICS 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, ease of use of tools for securely encrypted communication must be improved.

3. BRICS commission a feasibility study on options for collaboration or commissioning a suite of secure software and communications hardware.

4. BRICS 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.

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

Vulnerability to mass surveillance is due to 96% of those with Internet access using tools and platforms developed by US companies such as Google, Facebook, PayPal, Amazon, Twitter, Yahoo, and Microsoft that are subject to US law. While the US citizens may have some protection under the 4th Amendment, non-US citizens have none under existing the 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.

Companies such as Google, Facebook and Yahoo have created monopolies that must be broken with such 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 has about 55% of the world's content. Therefore, preserving local languages, literature and culture also demands that the monopoly of the US companies be reduced.

The popularity of these platforms comes from their ease of use, ability to use multiple tools using a common user interface and platform and quality of their products for free (the true cost is 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 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 or being located in the national jurisdiction of the US, subject to laws that make it incumbent to permit mass 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 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 space, it is necessary to focus on how they can they provide alternate tools that will provide the same degree of user comfort with similar level services. As long as there are no comparable products, it is difficult to stop people from using these platforms. It means building the equivalent of Gmail, Facebook, Twitter, YouTube, and search engines that can provide the same services to users that Google provides. These must also 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. Therefore, the need for a Free and Open Source Software (FOSS) approach to develop 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 is already available in the BRICS countries

There are three important reasons for a FOSS approach and not a proprietary approach. The first is that as the code is public, it makes it very difficult to embed backdoors in such software. This would also make such platforms more easily acceptable worldwide; it would not be seen to be a 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. A BRICS support for FOSS through such

projects would also help in promoting open systems – both hardware and software – and 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.

The BRICS/IBSA countries are uniquely placed to lead such an effort. They have the necessary skill-set and a large internal market. Brazil, South Africa and India have a public policy of supporting FOSS. They also have the need for non-English material for their citizens. Even South Africa and India, where English is widely used, need other languages to protect peoples' culture and allowing a greater penetration of Internet services. As e-governance becomes important, providing government services to the people will need a much greater localization that global Internet companies may not provide.

It *is* possible to create a free and open source software solutions for email, instant message, video conferencing and file sharing and storage.

It is possible today – if we can treat it as a critical task – to create such platforms. The cost of such an effort, if we use a free and open source approach and are backed by BRICS countries would not be very large.

Investing in the human capital required to create these solutions would accelerate capacity development and nurture south-to-south networks that would likely bear fruit well beyond the initial efforts.

We urge the BRICS countries to seize the post-Snowden moment to collectively benefit from the tools being developed by the free and open source community and enhance the human and economic resources of the BRICS towards creating a comprehensive suite of secure software.

Just Net Coalition (Coalition for a Just and Equitable Internet)

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 .