Human rights and building confidence and security in the use of ICTs
Grace Githaiga, KENYA ICT Action Network (KICTANet)
October 19, 2015

The topic of Human rights is one that is close to our hearts as civil society. In this regard, different civil society organizations met here in New York a few days before today's consultations and looked at the zero draft. In terms of human rights, we had various concerns which I will now present on behalf of the civil society represented in our meeting.

We propose that in order to achieve the WSIS vision of a people-centered, inclusive, and development-oriented information society, the WSIS framework must be underpinned by human rights. And any restrictions on human rights should be in accordance with international human rights law.

This means that any restrictions on Human rights should be prescribed by law, and must be necessary and proportionate in consideration of a legitimate aim and in line with international human rights law.

Human rights are an essential foundation of the Information Society, and the General Assembly resolution 68/167 recognizes, that the rights that people have offline must also be protected online. For us, these rights include economic, social, cultural, civil and political as captured in international human rights instruments.

We reaffirm the need for respect and protection of personal data and information. In light of this, we propose that the General Assembly resolution 69/166 (The right to privacy in the digital age) be implemented in its entirety, setting up domestic and international mechanisms to allow individuals to fully enjoy and exercise their fundamental rights to privacy. We are opposed to arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data. These we find as highly intrusive acts, which violate the rights to privacy and freedom of expression and go against the principles of a democratic society. We would propose that States review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, with a view to upholding the right to privacy and ensuring the full and effective implementation of all their obligations under international human rights law.

Article 29 of the UDHR reminds us that the individual has not only rights but also duties (Paragraph 1), and that limitations on rights (Paragraph 2) must (Paragraph 3) be drawn.
We emphasize that states have the obligation to protect human rights. This entails protection against human rights violations by non-state actors and requires public actors to take appropriate steps to prevent, investigate, punish and redress violations through effective legislation and remedies. We reaffirm, in accordance with the UN Guiding Principles on Business and Human Rights that private actors should avoid causing or contributing to adverse impacts on human rights and should cooperate in the provision of effective remedies to such impacts including through appropriate judicial or non-judicial mechanisms. Private remedies should not seek to substitute or replace existing public remedies, but should complement them.

We recognize that anonymity and encryption have roles such as privacy protection and freedom of expression, and therefore facilitate dialogue human rights issues.

We note that decisions related to the technical dimension of the information society and to the development of the use of the internet and ICTs might have implications for human rights. However, emphasis should be paid in particular on the need to promote human rights considerations in the development of Internet standards and protocols. In addition, the alignment of Internet and ICT-related laws and policies should be in line with International Human Rights Law.

We acknowledge the work that governments, the private sector, civil society, technical community, academia, and international organizations are undertaking, through a wide variety of initiatives, to strengthen confidence, trust and security in the use of ICTs, including in the field of cybersecurity and cybercrime. We therefore encourage efforts to improve collaboration and transparency, bearing in mind protection of the right to privacy.