What to Watch at WCIT

Introduction

On December 3, the world's governments will convene in Dubai for the World Conference on International Telecommunications (WCIT), a meeting organized by the International Telecommunication Union (ITU), a UN agency. At WCIT, governments will be debating changes to the International Telecommunication Regulations (ITRs). A number of the proposed revisions could expand the ITU's treaty to include aspects of internet policy. This could threaten internet openness and innovation, increase access costs, and erode human rights online. While Member States of the ITU (governments) and Sector Members (industry and others) participate, civil society and other stakeholders are largely excluded from the WCIT process.

Below is a cheat sheet of key issues to watch at WCIT, identifying concerning proposals and the positions of ITU member states (indicated as "for" or "against") as of the end of November. It is important to note that not all issues lend themselves to a for/against dichotomy and that not all submissions to the ITU cover all issues. Therefore, a country or regional group's position is only noted below if it is included in their submission to the ITU. Omissions do not imply support for or opposition to a particular issue. Articles mentioned below refer to either proposed revisions to existing articles or proposed new articles. All proposals have been made available by .nxt and can be viewed at: http://news.dot-nxt.com/itu/wcit/docs-by-meeting

General Concerns

- **Government-centric**: The International Telecommunication Union (ITU) is an intergovernmental body in which only Member States of the United Nations have a vote in decision-making. Decisions about Internet governance, by contrast, have taken place in a decentralized environment by a number of multi-stakeholder bodies comprised of civil society, governments, and the private sector. The multi-stakeholder approach to internet governance was embraced by the world's governments at the 2005 World Summit on Information Society (WSIS), which was hosted by the ITU. While there is a need to reform internet governance, particularly so that the concerns of the global south are better understood and addressed, shifting this power into the ITU, which excludes important stakeholders from key decisions, is not the answer.
- **Lack of Transparency**: The internet was developed on public lists in a transparent manner. In the lead up to WCIT, on the other hand, the public has had to rely on leaks to gain information on proposals under consideration. Only members of the ITU have access to proposals being considered at WCIT, and the ITU must get permission from governments to release this information, which they have not approved. While the Secretariat has taken steps towards greater transparency, by releasing an unattributed compilation of proposals, this falls far short of public consultation and underscores why a government-dominated body is not well-suited for internet policy-making.

Specific Proposals of Concern

1. **Definitions**- Proposed changes to definitions could change the scope of the ITRs and extend the international regulatory framework to include the internet.
   - ***Definition of Telecommunications*** *(Articles 2.1, 2.1A, 2.11, 3.1, 3A, 4.2, 4.3a)*

- A number of proposals would redefine telecommunications to include the internet services and applications that deal with user data and content. This is accomplished by adding language to the definition of telecommunication (Article 2) such as "processing," "internet traffic termination," or "telecommunication service/ICT," or by inserting a new definition of the internet itself. Other similar proposed modifications include references to "VoIP"Article 3.1, "Internet traffic and data transmission" in Article 4.2, as well as to "Internet and Internet Protocol" in Article 4.3a.These proposals would broaden the ITRs far beyond traditional telecommunications and because definitions are used throughout the treaty, *all* proposals must be viewed with an understanding that the term "telecommunications" could apply to the internet.
- For: African Telecommunications Union (ATU), Arab States, Cameroon, India, Regional Commonwealth in the Field of Communications (RCC), and Russia. Proposals from each of these countries or groups would include the internet in the definition section of the ITRs in some form, though they vary on specific language or approach. It should be noted that Russia has the strongest position in this regard, by defining "internet" and "national internet" and proposing to grant Member States equal rights to regulate it (Article 2.11).
- Against: Asia-Pacific Telecommunity (APT), Conference of European Post and Telecommunications (CEPT), Inter-American Telecommunication Commission (CITEL), Mexico, and United States.

- ***Definition of Operating Agency (****Articles 1.1, 1.5, 1.6, 1.7, 2.10A/B, 2.7, 2.8, 2.9, 2.19, 3A, 3.1, 3.2, 3.3, 3.4, 3.6, 3.7, 4.1, 4.2, 4.3, 4.4, 5.1A, 5.3A, 5.6, 5A, 6.0, 6.1, 6.2, 6.4, 6.5, 6.10 8A, 9.1)*
  - Currently, the ITRs govern "administrations," which by definition are limited to public entities ("governmental department or service" as well as "recognized private operating agencies"). However, a number of proposals would have the ITRs apply to "operating agencies" (defined as "any individual, company, corporation or governmental agency,") which can be either a private or government entity. This modification would give the ITU jurisdiction to set rules for all operating agencies, even private ones, which is a substantial increase in the scope of the jurisdiction granted by the ITRs.
  - For: Arab States, ATU, Brazil, Cameroon, CEPT (limited), India, Mexico, RCC, and Russia.
  - Against: APT, Australia, CITEL, and United States.

2. Restrictions on Content (Articles 1.0, 1.1c, 1.3, 1.8A, 2.13, 2.18, 2.24, 2.26, 3A, 3.3, 3.4A, 4.3, 5A, 5B, 6.0, 9.1)

- A number of proposed amendments to the ITRs that aim to counter cybercrime and enhance network security are overbroad and are inconsistent with established international human rights standards concerning freedom of expression. In particular, some proposals define spam (Article 2) to include information bearing "no meaningful message", and other proposals, including a new Article 5A on "Confidence and Security of Telecommunications/ICTs" mandate governments to take a range of measures to combat spam and cybercrime, without specifying what constitutes an appropriate measure

or protections for rights. Taken together, these sets of proposals would limit online content in a manner that is inconsistent with international human rights norms. Cybersecurity and countering spam are legitimate global concerns, however, freedom of expression and other human rights must be provided adequate protection.

- For: Arab States, ATU, Brazil, Cameroon, India, Indonesia, RCC, and Russia.
- Against: APT, Australia, CEPT, CITEL, Tunisia*, and United States.

*It should be noted that Tunisia proposed new language that would require governments to ensure that any restrictions placed on the exercise of freedom of expression through the means of telecommunication/ICTs be in accordance with international human rights norms.

3. **Cutting Off Access** (Articles 1.1c, 2.10B, 2.15, 2.16, 3A, 3.3, 3.4A, 5A, 5B)

- Provisions under the proposed new Article 5A would open the door to cutting off internet access in a manner inconsistent with international human rights norms. Several proposals concerning new Article 5A call for broad and vaguely defined "appropriate" measures to combat network fraud. An RCC proposal would provide justification for cutting off international telecommunication services when they are used for "interfering in the internal affairs or undermining the sovereignty, national security, territorial integrity and public safety of other States, or to divulge information of a sensitive nature."
- For: Arab States, ATU, Brazil, Cameroon, India, Indonesia, RCC, and Russia
- Against: Australia, CEPT, CITEL, Mexico, Tunisia, and United States.

4. **Privacy Concerns** (Articles 2.10C, 2.12, 2.19, 2.20, 2.21, 3.3, 3.4B, 3.5, 3.6, 4.4, 5A, 5B, 6.10)

- Proposals concerning cybersecurity also threaten privacy and anonymity online with new language on "data preservation, retention, protection", 'personal data protection' (new Article 5A of the Arab States proposal), "calling party identification", compulsory subscriber identification by operating agencies (Article 5A.9 of the RCC proposal), and allowing masked user information to be made available to authorized law enforcement agencies (Article 3.6 of the Cameroon proposal). Revisions to an article concerning international routing (Article 3.3), which would grant governments a "right to know" how traffic is routed also raises privacy concerns. These proposals are inconsistent with international norms as well as many national laws.
- For: Arab States, ATU, Brazil, Cameroon, India, Mexico, RCC, and Russia.
- Against: CITEL

5. **Increased Cost for Internet Services** (Articles 2.27, 2.29, 3.1, 3.2, 3.4, 4.3, 4.7, 6.0, 6.2, 6.5, 6.15, 6.18)

- Several countries have proposed language that would impose fees on sending networks and allow networks to make "quality of service" deals for priority delivery with certain content providers by preventing national net neutrality rules. These modifications would have the effect of requiring online content providers to pay to reach users, which would likely result in increased cost of internet access for users everywhere, limit the ability of content creators all over the world to access the global online market, and could limit the ability of users in smaller or less developed countries to access the global network.

- For: Arab States, ATU, Brazil, Cameroon, India, and RCC
- Against: APT, Australia, CEPT, CITEL, Mexico, and United States

6. **Enabling Filtering** (Articles 1.1c, 3.3)
   - Proposed changes to Article 3.3 on international traffic routing raise concerns over filtering and blocking. Modifications would grant governments a "right to know" how its traffic is routed, and in some cases a right to impose any routing regulations for purposes of security and countering fraud (Cameroon). In addition to presenting technical challenges that could require fundamental changes in the architecture of the internet, these proposals could also increase governments' ability to identify, filter, and block online communications and information, depending on how they are implemented. They also raise privacy and anonymity concerns.
   - For: Arab States, ATU, Cameroon, Mexico, and RCC
   - Against: APT, Australia, Brazil, CEPT, CITEL, and United States

7. **Violation of Net Neutrality** (Articles 1.1C, 2.27, 2.29, 3.1, 3.2, 3.4, 4.3, 4.7)
   - A number of proposals could violate network neutrality principles by adding language concerning "end-to-end quality of service." These proposals would use an international treaty to prohibit certain types of national net neutrality regulations and would likely establish a tiered internet with more expensive or reduced access to the full range of information or services online for businesses and users, particularly in developing countries.
   - For: Cameroon and India
   - Against: CITEL and United States
   - Other proposals would change language regarding quality of service from "minimum" to "satisfactory," which could also potentially violate network neutrality principles.
   - For: APT, Arab States, ATU, and CEPT

8. **Interfering with Work Done by Existing Multi-Stakeholder Bodies** (Articles 3A, 3.4A, 3.5)
   - Some proposals addressing cybersecurity as well as naming and numbering would interfere with the work done by existing multi-stakeholder bodies. For example, the Internet Corporation for Assigned Names and Numbers (ICANN) is already responsible for coordinating numbering, addressing, and naming resources. However, the ATU has proposed granting concurrent control to Member States, while the Arab States have proposed that Member States ensure that Operating Agencies in their territory apply the ITU-T Resolutions and Recommendations relating to naming, numbering, addressing and identification, both of which could lead to regulatory uncertainty and conflicting mandates. Russia's proposal would go even further, by granting all Member States "equal rights to manage the Internet."
   - For: Arab States, ATU, and Russia
   - Against**:** CITEL and United States

9. **Making ITU-T Recommendations Mandatory** (Articles 1.6, 3.1, 3.4, 3.4A, 3.4B, 3.5, 3.6, 4.2, 4.3, 5.1, 5.1A, 5.4, 6.6, 8.1, 8.2)

- A number of governments are proposing to change ITU-T Recommendations, in the form of technical standards and specifications, from voluntary to mandatory. Voluntary standards adoption is an important underpinning of the internet's innovativeness because it allows technology developers to decide how to package and build on standards. Making the ITU-T Recommendations mandatory would not only put these decisions into the hands of governments, but because many of used standards are developed outside the ITU in multi-stakeholder bodies and remain voluntary, it would skew technology development in favor of whatever is standardized at the ITU-T, regardless of the technical merit.
- For: ATU, Arab States, Brazil, Cameroon, India, Mexico, and RCC
- Against: APT, CEPT, CITEL, and United States

This is a living document and is updated as of November 28. Additions and updates are welcome and should be sent to Access Policy Analyst Deborah Brown at deborah@accessnow.org or Access Policy Fellow Matt Friedman at matt@accessnow.org.

For additional resources, please visit www.accessnow.org/policy/ITU.