APC-LA RUE FRAMEWORK FOR ASSESSING FREEDOM OF EXPRESSION AND RELATED RIGHTS ON THE INTERNET

APC developed the APC-La Rue Framework based on the work of and recommendations by former UN Special Rapporteur on Freedom of Expression Frank La Rue[1] and on the UN Human Rights Committee's General Comment 34[2] on Article 19 of the International Covenant on Civil and Political Rights. The framework consists of a checklist of indicators that are intended to provide guidance in monitoring and reporting on internet-related human rights violations, specifically those related to freedom of expression. Further work is needed, and is underway, to develop more comprehensive guidance for reporting on a wider range of internet-related human rights including women's rights, sexual rights and economic, social and cultural rights, as steps towards turning the framework into a monitoring tool for human rights online.

1. General protection of freedom of expression

- National constitution or laws protect internet-based freedom of expression.
- State participates in multistakeholder initiatives to protect human rights online.

2. Restrictions on online content

2.1 Arbitrary blocking or filtering

- There are no generic bans on content.
- Sites are not prohibited solely because of political or government criticism.
- State blocks or filters websites based on lawful criteria.
- State provides lists of blocked and filtered websites.
- Blocked or filtered websites have explanation on why they are blocked or filtered.
- Content blocking occurs only when ordered by competent judicial authority or independent body.
- Where blocked or filtered content is child pornography, blocking or filtering online content is connected with offline national law enforcement strategies focused on those responsible for production and distribution of content.

2.2 Criminalising legitimate expression

- Defamation is not a criminal offence.
- Journalists and bloggers are protected against abuse or intimidation.

1. Available here: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf
2. Available here: www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

CONNECT YOUR RIGHTS! INTERNET RIGHTS ARE HUMAN RIGHTS

- Journalists and bloggers are not regularly prosecuted, jailed or fined for libel.
- Journalists, bloggers and internet users do not engage in self-censorship.
- National security or counter-terrorism laws restrict expression only where:
  (a) the expression is intended to incite imminent violence;
  (b) it is likely to incite such violence; and
  (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

2.3 Imposition of internet intermediary liability

- State does not delegate censorship to private entities.
- Internet intermediaries are not liable for refusing to take action that infringes on human rights.
- State requests to internet intermediaries to prevent access to content, or to disclose private information, are:
  (a) strictly limited to purposes such as the administration of criminal justice; and
  (b) by order of a court or independent body.
- There are effective remedies for individuals affected by private corporations' actions, including the possibility of appeal through the procedures provided by the intermediary and competent judicial authority.
- State discloses details of content removal requests and accessibility of websites.

2.4 Disconnecting users from the internet

- Internet access is maintained at all times, including during political unrest.
- Disconnecting users is not used as a penalty, including under intellectual property law.

2.5 Cyber attacks

- State does not carry out cyber attacks.
- State takes appropriate and effective measures to investigate actions by third parties, holds responsible persons to account, and adopts measures to prevent recurrence.

2.6 Protection of the right to privacy and data protection

- There are adequate data and privacy protection laws and these apply to the internet.
- The right to anonymity is protected.
- State does not regularly track the online activities of human rights defenders, activists, and opposition members.
- Encryption technologies are legally permitted.
- State does not adopt real name registration policies.
- Limitations on privacy rights are exceptional (such as for administration of justice or crime prevention) and there are safeguards to prevent abuse.

3. Access

- State has a national plan of action for internet access.
- State fosters independence of new media.
- Concrete and effective policy is developed with public and private sector to make the internet available, accessible and affordable to all.
- Development programmes and assistance policies facilitate universal internet access.
- State supports production of local multicultural and multilingual content.
- State supports initiatives for meaningful access by marginalised groups.
- Digital literacy programmes exist, and are easily accessible, including primary school education and training to use the internet safely and securely.