Freedom of expression and Internet

Executive summary

This report, by the Office of the Special Rapporteur for Freedom of Expression for the Organisation of American States, examines the impact of the internet on freedom of expression in the context of the Inter-American system for the protection of human rights. It sets out the case for standards to protect freedom of expression and thought online, reviewing the challenges posed by a fast changing technical environment.

The report begins by assessing how the internet has had a transformative impact upon people's ability to communicate instantaneously and at low cost and that states should seek to preserve its open, distributed and inter connected nature. It also examines instances where countries in the region have begun to adapt their domestic legislation to international human rights principles that extend to the right to freedom of expression on the Internet.

In order to preserve the benefits of the internet to freedom of expression, the report holds that states need to develop guiding principles that can shape the development of law and policy in the following areas:

1. Access – to ensure universal and affordable access to the internet;
2. Pluralism – to promote plurality and diversity in public debate;
3. Non-discrimination – to take affirmative action to ensure equality;
4. Net neutrality – to ensure no discrimination or interference in internet traffic.

The report considers some issues in specific detail.

Net Neutrality

States should provide adequate legislation to protect the neutrality of networks, by which is meant there should be no_discrimination, blocking, filtering or interference with internet traffic based on factors other than the engineering of the network. Network neutrality should also apply to ways of accessing the Internet, without restrictions on compatible devices. States should ensure the application of rules should be independent, transparent and respectful of due process.

Access to the internet

Access to the internet requires three actions from states: A positive obligation to close the digital divide (including the gender divide); the obligation to ensure that infrastructure and services promote universal access, including for linguistic and cultural minorities; and the obligation to refrain from blocking or limiting access to the internet and that people are not shut off for exercising their rights.

Restricting freedom of speech – general considerations

Freedom of expression, including online, is not an unlimited right and can be subject to certain narrowly defined restrictions. The unique nature of the internet means that proposals to restrict freedom of speech online must be examined carefully. The report reviews the criteria for applying legitimate restrictions to speech – that it should be defined by law, be necessary, proportionate and appropriate to fulfill an urgent objective, and be subject to review by the courts (together known as the three part test).

As the internet is a global medium it requires – in order to avoid conflicting state jurisdictions imposing a chilling effect – an approach by states consistent with international standards. Proposals to restrict speech brought under legitimate grounds should be careful to confine themselves to the state jurisdiction where the content originates, with an emphasis placed upon correcting erroneous information rather than any attempt to apply legal restrictions. Throughout, the report argues that careful consideration should be given to the open and dispersed nature of the internet in applying restrictions so as not to limit the benefits that it brings.

Given the ease of accessing digitalized content, copyright has emerged as a distinctive issue. The report argues that while there is a public interest in asserting copyright, this needs to be balanced against the rights to culture, education and information and protection of copyright should be exercised proportionately.

Filtering and blocking

The blocking and filtering of content is only permissible in cases where the content violates human rights norms and after scrutiny by an impartial court. Such decisions should be transparently and only as a last resort.

The role of intermediaries

The functioning of the internet depends upon intermediaries of various kinds and these are vulnerable to both state and private actors seeking to exercise control over the internet. Intermediaries should not be held liable for the content they carry unless specifically receive a court order to that effect. Nor should they be required to supervise content that passes through their services (anymore than telephone companies are held liable for the traffic they carry). This position is supported by a range of expert opinion and legal judgments.

So-called “safe harbor” provisions allow intermediaries to avoid liability if they agree to take down content when requested by states. But placing such a responsibility in the hands of private actors threatens free expression protections as such actors are not equipped to weigh all the relevant considerations and this should only be exercised with the authority of a court (a system in operation in Chile and proposed by the Marco Civil in Brazil).

Given the importance of private actors as intermediaries they must establish clear and transparent service conditions that respect users' rights to freedom of expression and privacy. They should also be allowed to disclose requests from government agencies for access to their data and challenge those requests if they violate human rights principles.

Cybersecurity, privacy and freedom of expression

Cybersecurity

Cybersecurity should be understood as embracing both the security of critical infrastructure and the security of individual users but not used to create new categories of computer crimes (for example defamation and fraud which are defined offline), which could criminalize use of the internet. States should bear in mind the open and dispersed character of the internet in formulating cyber security policy and the need to protect human rights and bear in mind the provisions of the three part test set out above.

While states may develop security standards for public entities they should not seek to impose these on private actors as they can inhibit innovation and restrict the openness of platforms. States should also report on measures they are imposing on grounds of cybersecurity and such measure should be subject to the courts.

Privacy

Online freedom of expression requires respect for peoples' privacy. Privacy includes both the right to a private life and to the confidentiality of data about a person (the rights to data protection), though rights to privacy should be exercised proportionately so as not to restrict rights to freedom of expression. People should be able to express themselves without being forced to identify themselves unless they are engaged in acts that violate the rights of others. Online identification and authentication requirements should therefore be applied narrowly to high-risk transactions and interactions.

Modern use of the internet generates an enormous amount of personal information and states should establish systems to protect people's data and the way it is collected, managed and used to ensure compliance with human rights norms. States should provide rights of access to data held about them and provide that such data is only collected for lawful purposes.

Surveillance

Legally established programs of surveillance may be legitimate for purposes such as the prevention of crime or national security. Given the nature of the internet and its technical possibilities however, such programs can be invasive and damaging to privacy and free expression rights. Legal frameworks have not kept pace with technology increasing the risk of human rights violations as surveillance can now be conducted on an unprecedented scale. States should set

limits on the monitoring of online communication in accordance with established norms providing for the surveillance to be conducted in accordance with laws that establish clearly and precisely the grounds for surveillance.

Great care should be taken with concepts such as national security, which have been used to restrict the rights of human rights defenders, journalists and others. This means any such laws should only apply in exceptional circumstances and not be exercised with prejudice or discrimination. There should be appropriate procedural protections. Finally any surveillance programs should be authorized by a court competent to make such rulings and should only be secret under the strictest circumstances which are themselves established by law. In general states should publish general information on the numbers of requests for communication interception and surveillance that have been made. No one should be sanctioned for publishing information about such programs in the public interest.

Requirements by states to host data locally, could however restrict freedom of expression by reducing the availability of services, increasing the barriers for entry to new providers, reduce the open global nature of the internet and force people to hold their data in less secure legal environments.

Multi stakeholder participation.

Governance of the internet is an important aspect of its ability to promote freedom of expression. It is important that all relevant points of view are taken into account in formulating internet policy. A good example of this is the Internet Management Committee (CGI) in Brazil, comprising members of the government, business and civil society. It co-ordinates the country's internet services transparently and openly.

This would require states to adhere to Principle 20 of the Declaration of Principles of the World Summit on the Information Society which states: "*Governments, as well as private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centered Information Society is a joint effort which requires cooperation and partnership among all stakeholders*."