

and Democrat blogs and analyzes the links between them to know how is the opinion produced on the Internet. Evidence says that 91% of the links originating from either the conservative or liberal communities stay within that community.

In fact, people who use Internet to make their opinion have a much larger probability to not be exposed to the opposition party's arguments. This divide can be extremely harmful for democracy, as people are not getting all the necessary information to make their electoral decision.

I am not saying that Internet has brought this problem, as we have always tended to move in a certain sphere -and buying certain newspapers, and watching certain TV channels- according to our

opinions. However, on newspapers and TV, we are more able to be confronted to other topics and realities. Behind its curtain of plurality, Internet -or our use of it- could just be accentuating the intellectual segregation. The dream of a public sphere on the web where public opinion could be created by the confrontation of different arguments can thus be fading away in our faces.

As Internet is gaining importance in our daily lives, could we possibly go towards a model where people will be half-informed, even if theoretically they could get access to an inexhaustible source of information?

Emmanuel Neisa is interning at Digital Empowerment Foundation on issues related with ICT's for development.

should be read through these issues. As a user, one is of course concerned that one is not defrauded on the internet - whether through credit card fraud, identity theft etc. The increase in opportunity for such cyber crimes to be perpetrated makes people wary about transacting over the internet - whether that are online banking or purchasing goods and services. And I want to be confident that the companies I transact with on the internet can keep my data secure, and secondly will not share it or have it accessed and used without the proper authority (mine and/or theirs). The growth of the internet into more places and internet users mean the opportunity/ threat of becoming a victim of a cyber crime also increases proportionately.

A number of legal instruments have been drawn up to promote confidence in internet security and curb online criminality. The key issues here concern with these is whether and the extent to which they infringe - in their conception and practical implementation - on human rights, particularly the right to privacy, the right to freedom of expression, and access to information. The proliferation of these national laws and global conventions has developed legal means for states to effectively snoop on their citizens. In the post-9/11 period, it has been easier for states to put pressure on - in some violate - citizens rights, citing the "terrorist threat."

The main policy is how to balance the tensions between cyber security on the one

**The growth of the internet into more places and internet users mean the opportunity / threat of becoming a victim of a cyber crime also increases proportionately.**

hand, and privacy and openness on the other. Currently the dynamic is skewed towards increasing cyber security measures at the expense of human rights, with measures in place to collect unprecedented amounts of information about private citizens - with the ability to track physical movement, how the internet is used, consumer and life-style choices etc - without enough assurances that this information will not be abused by the very people who collect it (with state sanction). Another measure exercised by states - and also within other organisational structures - is the capacity to block content which it finds "threatens state security". One of the dangers of this measure is that the goal post of what is "dangerous" will shift to also include what is deemed "offensive" so that the morality of an elite group - with the power to make such decisions - is imposed on an entire population. State decisions to cut access to particular kinds of information more often than not infringes on the freedom of expression of large tracts of its citizenry.

Natasha Primo is with APC. She can be contacted at [natasha@apc.org](mailto:natasha@apc.org)

## Internet Governance: Challenges in relation to cyber crime and laws

NATASHA PRIMO

**M**y concern is mainly with advocacy on openness and maximising access to information and knowledge for (human) development and social jus-

tice. So my entry into discussions on cyber crime and cyber laws is filtered through an openness lens. My other main concern is data privacy. My interest in cyber-security