Champions of Internet freedom ignore online ethics at their own peril

MAREIKE LE PELLEY
January 2013

- Advocates of Internet freedom need to develop more responses to cybercrime and online ethics to make sure that real concerns are not exploited by repressive governments to impose Internet controls and other measures, which violate the rights to freedom of expression and freedom of information.

- An improved multi-stakeholder system of Internet governance, increased transnational cooperation and increased investment in Internet safety technology is needed to combat rising levels of cybercrime.

- Principles of self-regulation can and should be increasingly extended to online media and online communication to fight ethical lapses in Internet content. While the nature of the Internet can compound some of the ethical problems encountered it simultaneously displays features which can help to make self-regulation work.

- The promotion of information and media literacy will make Internet users more responsible and critical in their approach to online contents and will enable the individual to detect and react to bias, falsities, incitement and hate speech. Increased debate and diversity of opinions can be effective tools against ethical and even criminal abuses of online and mobile communication.

- Internet and mobile communication play an important and increasing role in the social, economic and democratic development of countries. Government controls and censorship are likely to hamper the realization of this development potential.

Rapid developments in information and communication technologies and their impact on politics and society have stayed popular media topics for many a year now; though the hypes have changed over time. While the Arab spring of 2011 triggered an avalanche of articles about the role of social media in the political upheavals in particular, and about how social media will change the nature of political discourse in general, the headlines of 2012 dealt with the backlash by governments and increasing tendencies by states to control and censor cyberspace and spy on their citizens.

While most Sub-Saharan African countries so far do not systematically restrain Internet freedom, Ethiopia is a notable exception, where government has blocked websites and access to the Tor network, which allows Internet users to browse anonymously and access blocked websites, manipulated online discussions, arrested individuals because of their online activities, and might be seeking to install an online surveillance system.[1] In other countries, such as Zimbabwe and Rwanda but also in Uganda, government has on and off attempted to block social media, censored websites or gone after individual bloggers. Furthermore, the introduction of an E-Bill in Malawi and attempts to deregister an online news site in Zambia, both in October 2012, have caused some concern among freedom of expression and Internet freedom activists.

Internet governance, too, was a topic at the World Conference on International Telecommunications (WCIT) which was convened by the International Telecommunications Union (ITU) and took place from 3-14 December 2012. The WCIT sought a review of the International Telecommunications Regulations (ITRs) of 1988 but failed to reach consensus on the new version when almost 40 per cent of the treaty parties present at the conference refused to sign the Final Acts.[2] The most contentious Articles 5A and 5B of the revised ITRs contain cyber security and spam references, which may not only be used by governments to censor the Internet but also imply that the new treaty covers the Internet. Furthermore, the (non-binding) Internet Resolution, which is part of the Final Acts, confirms not only the role of nation states in Internet governance but also gives the ITU, and therefore a UN body whose members are nation states, an explicit role in Internet governance.[3]

The implications of the WCIT failure for Internet governance are not yet altogether clear. While some see it as a victory of the old, multi-stakeholder model, others see legal ambiguity as the 88 countries that signed the Final Acts may decide to implement the new provisions unilaterally. In the meantime, many civil society organisations and initiatives continue lobbying to prevent the fragmentation of the Internet, i.e. the creation and control of »national Internets« by nation states, and to ensure that the Internet remains (or becomes once more) free. Their cause has been strengthened by a report of the UN Special Rapporteur on the right to freedom of expression and a subsequent resolution of the Human Rights Council, which both confirmed that the right to freedom of expression extends to the online world and that Internet freedom has to be respected by countries everywhere.[4]

No Internet governance is the best governance?

While discussions on Internet governance have been going on, much less attention has been paid to ethically problematic online contents. This type of contents may and does feed into the arguments made by repressive governments to curb freedom of expression on the Internet. The perceived dangers of complete Internet freedom alone should force advocates of total laissez-faire to consider responses to counter real and feigned concerns by autocratic regimes. To preserve Internet freedom, its champions have to propose solutions for real ethical problems, while at the same time debunking the hypocrisy of repressive regimes and their methods.

There are at least two types of problematic online contents. One involves criminal activities ranging from violations of privacy and personality rights to child pornography, human trafficking, drugs and other organised

1. http://en.rsf.org/ethiopia-government-steps-up-control-of-07-06-2012,42735.html (accessed 31st December 2012), Kelly, Sanja et al. (eds.) (2012): Freedom of the Net 2012. Freedom House.

2. http://www.itu.int/osg/wcit-12/highlights/signatories.htm (accessed 28th December 2012)

3. ITU (2012): Final Acts. World Conference on International Communications, http://www.itu.int/en/wcit-12/Pages/itrs.aspx (accessed 31st December 2012)

4. Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/17/27 to the 17th session of the Human Rights Council in May 2011 and the resolution of the Human Rights Council, A/HRC/20/L.13 at its 20th session in June 2012.

crime. While these criminal Internet activities have received some media attention, other ethical issues have been little dealt with by defenders of Internet freedom. These ethical online concerns range from publishing factual falsities and spreading gossip and rumours to blackmail, harassment and intimidation, from defamatory and inflammatory remarks to hate speech and incitement to violence or even genocide.[5]

All of these ethical and many criminal breaches were not invented along with the Internet or with mobile phones; many have existed as long as people have been able to communicate.[6] Many, if not all, are dealt with in the codes of conduct of media houses or media councils and in national criminal laws. However, the Internet and mobile communication make tackling them more difficult due to the very nature of cyberspace:

- National criminal and civil laws are much less effective because of the cross-border/global nature of the Internet.
- Content via the Internet spreads faster and to more people than via traditional media platforms, telephones or word of mouth.
- Electronic content stays around for longer than spoken or written words or one-off broadcasts.
- Perpetrators can remain anonymous more easily on mobile and online platforms.
- And some argue that because of the (perceived) anonymity of the Internet, people are less restrained by social mechanisms and more likely to behave unethically.

Government controls and censorship are not an option

While some – mostly democratic – governments respond to illegal online activity by requesting relevant platforms such as *Facebook* or *YouTube* to take down illegal contents[7] others argue for more and broader government controls and censorship. There are at least two problems with this latter approach:

First and foremost, Internet censorship violates the right to freedom of information and the right to freedom of expression, whose protection online just as much as offline was confirmed by the 2011 report of the UN Special Rapporteur and by the 2012 resolution of the Human Rights Council. Government filters and blockages are generally broad, thus laying huge traps purportedly to catch criminals, or just to censor behaviour considered unethical, thereby (at the same time) blocking large amounts of material, which is not violating any ethical standards or laws, and often cutting off regime critical sites. These measures violate the principle of proportionality, and are not legitimate restrictions to this crucial and fundamental human right.

Furthermore, the increasing attempts by governments to acquire personal data by using surveillance technologies and requesting online platforms to release such data threaten or actually violate privacy rights and the right to informational self-determination. In addition, violating the right to privacy further infringes on the right to freedom of expression since the former is often essential for the exercise of the latter.

Secondly, government controls or government instated regimes to deal with cybercrime and censorship technologies to get rid of unwanted online content do not only open the doors to violations of human rights, they may also not be effective. Cybercriminals adapt quickly, and governmental structures cannot provide the necessary speed and flexibility to respond to cybercrimes effectively. The necessary technological responses and solutions, too, are better developed with the involvement of many stakeholders.

Furthermore, blocking and filtering technologies to censor unwanted content are only effective to some degree as they trigger the development of online tools that circumvent blocking programmes and government surveillance, thus initiating a continuous cat and mouse game, which requires ever increasing funding. Even though

5. Some of these are criminal offenses in some countries.

6. There are, of course, criminal activities that are Internet-specific. These include attacks against computer data and systems, hacking into online financial services, the deployment of viruses, Botnets, and various email scams such as phishing. Crimes old and new exploit the speed, convenience and anonymity of Internet and mobile communication. See also http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (accessed 31st December 2012). This paper focuses on online and mobile content rather than processes.

7. See http://www.google.com/transparencyreport/removals/government/ (accessed 31st December 2012).

governments can probably outspend software developers of circumvention software, the fact remains that effectiveness is limited and the large amounts of financial resources spent on staying ahead of the game could quite possibly be better spent on other things.[8]

Instead of heavy handed state censorship and government controls, several soft approaches may prove to be effective without violating human rights. In some of these approaches, a government's involvement is important, e.g. in promoting media literacy, in others, governments could and should be involved as one of several stakeholders or could play a supporting role.

Cybercrime: Decentralised multi-stakeholder Internet governance

Taking the complexity of the Internet and the speed of technological development into account, the current transparent, decentralised, multi-stakeholder system of Internet governance seems to provide the best basis to deal with the threats of cybercrime. It offers the ability to respond rapidly to changing threats by developing effective solutions with the participation of many stakeholders, including ICT companies Internet engineers, law enforcement agencies, government departments, human rights advocates, user groups and other civil society organisations.[9] Several such initiatives have already been successfully tested or are currently being established.[10] These approaches make use of existing national and international laws and the combined expertise of a variety of stakeholders. It requires education and awareness of all stakeholders, including users, transnational co-operation among all stakeholders, including governments, and a continued and increasing commitment to invest in the development of Internet security technology, which helps to fight cybercrime, protects the individual and is not used to violate freedom of expression. Cybersecurity should hence be based on cross-border co-operation between the public and private domain. This approach needs to be improved on but should not be replaced by government controls of the Internet because of the serious freedom of expression issues at stake.

Codes of ethics for convergence and online media

Regulating the online presence of conventional media houses, be they print or broadcast, is relatively straightforward as individual media houses would just extend their respective code of ethics to their online platforms. Similarly, the (self-) regulatory body of a country would expand its mandate and the application of its code of ethics to online platforms of conventional media and to pure online media. This is already happening. Just like any other journalist, online journalists would be obliged to apply professional ethical standards relating to accuracy, fairness, multi-sourcing and the verification of sources, privacy provisions, separation of fact and opinion etc. They would also have to apply these principles to user-generated contents (UGC) before using UGC for their contributions. To cater for the immediate and interactive nature of online user comments, professional codes could be expanded to advise journalists how to deal with these or how to organise and react to them in a moderated forum.

Nevertheless, media houses increasingly face the situation where employed and sometimes well known journalists and broadcast personalities become active online, e.g. in their own blogs, in their private capacities. And though this may give the respective media house some free publicity, such publicity is not always welcome, especially if opinions voiced in those forums are controversial or ethically problematic. One way to tackle this is to give the principle of transparency much more attention than it has been given in traditional codes of ethics. Employed journalists need to distinguish clearly online where they act and write in their private, where in their professional capacity as employees of a specific media house. They will also need to identify other interests or motivations influencing their online activities. Ideally though, individuals will adopt ethical standards, regardless of whether they work for media houses or not. And they may do so because it is in their own interest.

8. Ironically, to date censorship technologies as well as circumvention tools are mainly developed by Western companies.

9. https://www.cdt.org/files/pdfs/Cybersecurity_ITU_WCIT_Proposals.pdf (accessed 31st December 2012).

10. See for example »The Conficker Working Group Lessons Learned Document«(June 2010, published January 2011), http://www.confickerworkinggroup.org/wiki/ (accessed 31st December 2012), http://www.cleanitproject.eu (accessed 31st December 2012) and also http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf (accessed 31st December 2012) and http://blog.netsafe.org.nz/2011/11/15/review-of-the-london-conference-on-cyberspace-nov-12-2011/ (accessed 28th December 2012).

Self-regulation on social communication platforms, twitter, blogs and Co.

Most social media platforms and Internet companies, many Internet freedom and industry-based initiatives have developed charters, i.e. sets of principles or codes of ethics for their users, which reflect the professional codes of ethics developed by media houses and media councils, though often including a stronger focus on honesty and transparency.

There are several mechanisms and characteristics of Internet communication and social media that can help to make these platform charters but also self-regulation of individual online and mobile communication work:

- Most importantly, the general human desire to look good needs to be put to use. Bloggers, twitterers and other individuals, who post regularly, by and large value their online reputation and are interested in building credibility and trust in their product or online presence, and in gaining the respect of the online community, or that of their followers, »facebook friends« etc.

- Online communication gives individuals a greater opportunity than face-to-face communication to be actually judged on the basis of the quality of their writing as other determining factors, such as sex, ethnicity, looks, age etc., are less evident. This means that individuals interested in building online popularity have an interest in posting high quality content.

- Most people have a strong ethical sense. The two way communication of social media allows those users to flag problematic content, which may then be taken down. It also promotes the posting of comments, corrections and the sparking of debates, thus activating the name and shame mechanism. Or users – following the »do not feed the trolls« principle – will ignore and isolate inciting posts. Hence the very nature of the Internet does not only intensify some of the ethical problems encountered in communication but also offers mechanisms which allow self-regulation via two-way communication and feedback to work better.

- The greater focus on increased transparency, which asks users, who post content, to be honest about where they come from and what their motives are, will further promote the restraining function of a social framework and setting.[11]

These restraining mechanisms can be supported by calling on social networks to publicize their community guidelines more strongly and by promoting moderated forums where possible, since moderation, in the truest sense of the word, will prevent the most critical ethical lapses.

Information and media literacy for users

While codes of ethics and self-regulatory mechanisms target the providers of content, information and media literacy aim to equip the consumers of content with the tools needed to make sense of the masses of information the media and the Internet provide and to participate in that exchange.

Media literacy provides a framework and the skills that enable individuals to access information, analyse it in a critical and structured way, e.g. against one's ethical, moral and/or democratic principles, evaluate it on the basis of that analysis, and ultimately to produce messages using a variety of tools. Information and media literacy help to understand the role of information and media and build essential skills of inquiry and self-expression necessary for citizens to understand and participate in a society.[12]

In a world where not only conventional media but also mobile phones are ubiquitous and the Internet is already or fast becoming an everyday tool, introducing information and media literacy into schools' curricula makes a lot of sense. Due to the rapid changes in technology, teachers will act less like experts and more like facilitators and guides who provide the right questions and

11. It should be noted that the perceived anonymity of Internet, which may foster bad Internet ethics, is eroding fast. The use of spyware and other such tools now increase the dangers associated with the unauthorised release, analysis and use of private data by governments and companies, e.g. repressive governments access and use personal data to sanction and persecute politically opposing, critical opinions. Also note that while anonymity can promote unethical behaviour online, it is – as noted above – in many repressive contexts a necessary requirement to exercise freedom of expression effectively.

12. See http://www.medialit.org/ (accessed 31st December 2012), the definition by participants at the 1992 Aspen Media Literacy Leadership Institute in the USA, and http://mediasmarts.ca/digital-media-literacy-fundamentals/media-literacy-fundamentals (accessed 31st December 2012).

tools to students to become information and media literate.

In the context of assessing online contents, information and media literacy requires some degree of technical skills. More importantly however, media literacy activates the online responsibility of the individual by encouraging critical thinking, reflection, and ethical behaviour, which are invaluable for detecting bias of all sorts, falsities, and defamation, and for exposing incitement and hate speech. Individuals learn to evaluate sources, authenticate information and check for accuracy. They learn to distinguish between reality and fantasy, contextualise information, to discover and define agendas. It encourages users to become active and create the transparency (where it is not provided) necessary to expose dangerous partisanship, conflicts of interest, and ulterior motives.[13]

Information and media literacy promotes responsible media consumers who cannot be easily manipulated and who may even play a role in upholding ethical standards online. Media literacy hence provides yet another alternative to censorship, government controls and the violation of freedom of expression and other human rights.

Media diversity and debate

Promoting transparency in self-regulation on the one hand and information and media literacy on the other are likely to further more debate around contentious content. More users are likely to flag, contradict, discredit and argue against serious ethical breeches such as hate speech and incitement to violence. Media literate Internet users are also likely to contribute to creating more content diversity, thus giving other consumers a greater choice of opinions, perspectives and analyses.

Kenya's post-election violence of 2007/2008 demonstrates this point. While some politicians manipulated some vernacular radio stations and abused text messaging, the mainstream media, social networks and service providers in the latter stages of the conflict played a positive role in conveying messages of peace, providing viewpoints challenging aggressors and working against the spread and influence of hate speech.

A free Internet, governed by various stakeholders, including civil society, in an open and transparent manner, with inquisitive, informed, ethically aware and active users, which allows for vibrant discussions and a multitude of opinions will be an effective tool in the fight against its unethical or even some criminal manifestations; in the fight against false news, defamation, hate speech, incitement to violence and the online activities of extremists groups.

How do you convince governments?

While most democratic governments are convinced of the virtues of a free Internet, autocratic regimes tend to focus on how the Internet and social media can threaten their grip on power and demand national control over and ultimately the fragmentation of the Internet.

In an attempt to convince those regimes otherwise, various approaches can be employed. Governments should be reminded of their obligations under international and even national laws by other governments, international bodies and civil society initiatives. Support should be given to international and national civil society campaigns which lobby for the freedom and universality of the Internet, as well as for transparency and the participation of civil society in Internet governance. Pointing out the flaws or limited effectiveness of government controls and online censorship and the waste of state resources may also help. For this to work, the development and free provision of circumvention or anti-censorship software and technology need to be continued and increased. Finally, it could be helpful to focus on the benefits of a free Internet for social and economic development.

Some research puts the current contribution of the Internet to the national GDP of newly industrialising countries (though hard to measure) at somewhere between 1 and 2 per cent p.a., which – considering the rapid growth of Internet users in the developing world – is likely to increase in all developing countries over the next years.[14] Significant growth can be expected from mobile phone applications, which are especially useful to private individuals, small businesses, and farmers in facilitating various transactions and obtaining and exchanging vital

13. Occasionally authors of inciting online content are exposed as government agents, as agents provocateurs, revealing that government's insincerity with regard to Internet ethics.

14. See http://www.mckinsey.com/client_service/high_tech/latest_thinking/impact_of_the_internet_on_aspiring_countries (accessed 31st December 2012).

information. These economic considerations are of special importance to African countries, which recently have seen the highest growth rates in mobile telephony and the second highest economic growth as a region after Asia. Considering that scores for human development indicators in many African countries are still among the lowest worldwide, making good use of economic growth potentials is crucial.

Changes of Internet governance which give governments more controls and fragment the Internet are likely to result in barriers for new companies, slower transactions, higher costs, lower productivity and loss of business for established enterprises. Furthermore, the rate of innovation is bound to decrease as the exchange of ideas, collaborative knowledge creation and sharing work best in a free, transparent and unrestrained environment, uninhibited by national borders.

The Internet and mobile communication are also important tools for improving social services, health, education, and to help build more just societies. The citizens of some African countries, such as Kenya, have led the way in developing new sites and applications on Internet and mobile phone platforms that facilitate not only economic transactions but address social issues and issues of good governance. In 2011, the Kenyan government itself embarked on an open data initiative giving online access to public data across all sectors and thereby facilitating important monitoring and advocacy work of civil society organisations with respect to public services and development policies.

Research has shown that though social media *may* be used as a tool to incite violence, it is not the defining factor of that violence. Root causes are rather socioeconomic issues like poverty and inequality, and the lack of trust in government institutions and processes. If governments worry about staying in power, the most effective way to do so is by providing the public services, jobs and good governance their citizens need and have a right to.

About the Author

Mareike Le Pelley has been head of *fesmedia Africa*, the media project of the Friedrich-Ebert-Stiftung in Africa, since July 2010.

Imprint

Friedrich-Ebert-Stiftung
Division for International Cooperation | Africa Department
Hiroshimastraße 17 | 10785 Berlin | Germany

Responsible:
Michèle Auga, Head of Africa Department

Tel.: ++49-30-26935-7435 | Fax: ++49-30-26935-9217
http://www.fes.de/afrika

To order publication:
blanka.balfer@fes.de

The media project of the Friedrich-Ebert-Stiftung

fesmedia Africa, based in Namibia, promotes freedom of expression and freedom of information as well as media diversity throughout Sub-Saharan Africa to further the media's role in the democratic process. fesmedia Africa supports access to information campaigns on a continental level and in selected countries. It implements the African Media Barometer (AMB) panel discussions, a tool for assessing national media landscapes based on African standards, and publishes the resulting AMB reports as detailed sources of information and instruments for advocacy. fesmedia Africa promotes community broadcasting, the development of standards and independent media regulation. The project also contributes to the media development debate through its www.fesmedia-africa.org website and its publications.

EFQM Committed to excellence

ISBN 978-3-86498-452-5