



Contemporary forms of racism, racial discrimination, xenophobia and related intolerance and the internet

Submission to the United Nations Special Rapporteur on Contemporary forms of racism, racial discrimination, xenophobia and related intolerance (SRRX) from the Association for Progressive Communications (APC).

Introduction

1. APC welcomes the focus on the internet¹ as a priority thematic area for the Special Rapporteur. APC is an international network and non-profit organisation that believes the internet is a global public good. We advocate for everyone to have access to a free and open internet to improve our lives and create a more just world.² We encourage strategies that empower people to use technology, including the internet, to realise the full range of their human rights, combat discrimination and protect themselves from violence, and to take part in framing policies that govern use of such technologies, including internet governance discussions, legislation, policy and regulatory proposals.
2. As part of its Internet Rights are Human Rights initiative, APC advocates for the recognition of information and communication technology in facilitating human rights; documenting and analysing trends, violations and impacts on freedom of expression, freedom of association and the right to information on the internet at national, regional and global levels. APC also works to build the capacity of women human rights defenders to use the internet safely and securely, facilitating the development of learning and advocacy networks.
3. APC notes the SRRX focus on “governance of racist and xenophobic content on the Internet”, and research into “the appropriate balance between the protection of freedom of opinion and expression and the control of racist and xenophobic content and incitement to violence through the Internet.” Concerns about regulation of online content have been raised in a number of human rights and policy spaces in recent years, including the United Nations Human Rights Council and by the Human Rights Committee (including in the Universal Periodic Review)³. Issues of internet governance more generally have been under consideration in the UN Commission on Science, Technology and Development and in the multi-stakeholder Internet Governance Forum. We reiterate the importance of the multi-stakeholder model for internet governance and the WSIS principles and Tunis Agenda.

¹ APC defines the “internet” as a set of interconnected networks operated by government, industry, academia, and private parties which allow computers and other electronic devices in different locations to exchange information. The internet includes services such as the world wide web, electronic mail, file transfer (FTP), chat and remote access to networks and computers.

² <http://www.apc.org>

³ Association for Progressive Communications: Internet rights at the 13th session of the UPR, 2012
<https://www.apc.org/en/news/internet-rights-13th-session-universal-periodic-re>

4. Our work in these areas caused us to find the SRRX reference to “governance of racist and xenophobic content on the Internet” somewhat confusing. We assume it refers to the various human rights obligations of States in their governance role and how these are taken into account in developing legislative, policy and other measures to combat racism and related issues, rather than governance or control of the Internet or governance of online content more generally.
5. To that extent, this focus by the SRRX both builds on and extends the internet related work aspects of United Nations mechanisms, including human rights and internet governance. APC welcomes this development and calls for these various initiatives to be collaborative and integrated so that human rights and fundamental freedoms are respected, protected, promoted and fulfilled across all UN mechanisms that consider internet related issues. In this respect we note the planned thematic discussion of the CERD Committee scheduled for 28 August 2012.

Human rights and the internet: core concepts

6. The Human Rights Council has recently adopted, by consensus, an historic resolution affirming a profoundly simple concept: the same rights people have offline must also be protected online.⁴ This concise conceptual framing of human rights and the internet must be the foundation for the work of treaty bodies and special mandate holders, including the SRRX. More consideration is needed to understand how this conceptual foundation sits with the other universal and inalienable human rights and freedoms, including the right to be free from racial discrimination and States obligations as duty bearers to respect, protect and promote human rights. More consideration is also needed of the equal roles of all stakeholders (including governments, civil society, the technical community and the private sector) in upholding human rights online.
7. We note that Article 4 of the International Convention for the Elimination of All Forms of Racial Discrimination (CERD) requires States parties to penalize racist hate speech, including dissemination of ideas based on racial superiority or hatred, incitement to racial hatred, acts of racially motivated violence and incitement to such acts. Article 7 allows special measures ‘particularly in the fields of teaching, education, culture and information’ to combat prejudices that may lead to racial discrimination, and measures to promote a climate of tolerance. These articles must be interpreted in light of the Convention as a whole, including for example Article 5 which protects the right to freedom of opinion and expression. The Committee for the Elimination of Racial Discrimination has noted that racist hate speech occurs in the media, including the internet, in political discourse and other areas of public and social life. Racist hate speech has been a persistent concern of the Committee and has been raised by it in concluding observations and recommendations to States parties reporting to it. We therefore welcome the attention of the SRRX on the internet.
8. Originating from developed world technology, the internet and its many communication tools are now increasingly becoming available in the developing parts of the world, including in countries with repressive regimes where democratic rights are urgently needed. Internet users per 100 inhabitants in developing countries have more than doubled since 2007⁵ and are increasing more rapidly than in developed countries.

⁴ HRC resolution A/HRC/20/L.13 “The Promotion, Protection and Enjoyment of Human Rights on the Internet.”

⁵ ITU Statistics (2012), <http://www.itu.int/ITU-D/ict/statistics/> (12% of population in 2007 to 26.3% in 2011)

9. Taking these matters into account this submission has three parts: (a) Key issues, dilemmas and challenges in combating the use of the internet to propagate racist and xenophobic content and incitement to violence, (b) country specific cases highlighting new and emerging issues and (c) recommendations.

Key issues, dilemmas and challenges in combating the use of the internet to propagate racist and xenophobic content and incitement to violence

Key Issues

Access to the Internet

10. The internet as a communication technology is not new and telecommunications as a means to exercise the rights to freedom of expression and of peaceful assembly and association have been available for a long time. In the last few years, however, we have seen an unprecedented development in possibilities to communicate and interact online. With almost 2.5 billion internet users⁶, of which 800 million interact on Facebook⁷, “the Internet is one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies”⁸.
11. In reality, access to the internet is unequally distributed and as a result online communities do not yet reflect the full diversity of humanity, including racial and ethnic diversity. The potential of the internet to enable the rights to equality, dignity and freedom from discrimination for all is therefore far from being fully realised. The SRRX’s 2012 report drew attention to the dangers of unequal access to the internet, including the exclusion of the victims of discrimination from digital conversations, due to the intersection of poverty and discrimination. We echo this point and note, for example, the inequality of internet access in South Africa, where internet penetration is at approximately 20%. White South Africans account for 64% of all users, despite only representing 9% of the country’s total population⁹.
12. Access rates amongst countries vary widely, as do uptake projections, so that the trajectory for diversity of users increasing over time is by no means linear. For example, the uneven nature of the distribution of internet penetration is worrying and has both race and gender dimensions. Again, in relation to South Africa for example, only 31 per cent of South African internet users are women¹⁰. Rural internet penetration rates remain very low and distribution of internet users among provinces is extremely uneven. South Africa’s two most urbanised provinces, Gauteng and the Western Cape, account for 73% of all internet users in the country.¹¹ South Africa is by no means unique in this respect, but comprehensive disaggregated data about internet access rates in relation to race, ethnicity, gender and other variables that would allow comparisons between and among Member States does not appear to be available.

⁶ ITU Statistics (2012), <http://www.itu.int/ITU-D/ict/statistics/> (estimate for 2011)

⁷ Facebook statistics (2012), <https://www.facebook.com/press/info.php?statistics>

⁸ United Nations document A/HRC/17/27, (2011) para 2.

⁹ South African Press Association, ‘Internet use in SA growing’, 10/05/2012, accessed from <http://www.news24.com/SciTech/News/Internet-use-in-SA-growing-20120510#> on 19/05/2012.

¹⁰ Research ICT Africa, <http://www.researchictafrica.net/countries.php?cid=19>.

¹¹ See also: Statistics South Africa, <http://www.statssa.gov.za/publications/P0302/P03022011.pdf>

13. The World Internet Project¹² is one initiative which gathers quantitative data on internet use in 16 countries. The 2012 report shows, for example, that more men than women use the internet in all countries surveyed with very large gender gaps in Mexico (18%) and Colombia (16%).¹³ But few participating countries gather race and ethnicity data. In one, Hungary, the inequalities between the Hungarian Roma and non-Roma populations are stark: 45 per cent of non-Roma use the Internet, but only 1 in five Roma does so.¹⁴
14. We recommend that internet access rates be a key indicator in human rights reporting and that the SRRX encourage best practice among Member States to improve collection of disaggregated data. In addition, States should develop and report on national internet access plans, as suggested by the Special Rapporteur on Freedom of Expression.

Access to Content

15. While mobile technology has increased access to the internet by marginalised communities, there are still substantial gaps in capacities to create and access relevant content¹⁵. A study in Kenya found that mobile internet users are primarily accessing international news and services, often because of the limited availability of local content, because local news outlets have not formatted content to be accessible via mobile handsets and because local content is not as easy to licence¹⁶. As the internet becomes a growing source of education and awareness-raising it is crucial that production of content includes content created by and for diverse racial and ethnic groups.
16. The diversity of online content can also be restricted for ideological, racial, religious and cultural reasons. In July 2012 the Pakistan Telecommunication Authority banned the official website of a religious minority group, Ahmadiyya, citing blasphemous content on the website.¹⁷ A week later, another ban was imposed on a watchdog website in Pakistan, for publicly propagating religious views.¹⁸ In Indonesia, the anti-pornography bill was recently used to block a website that features information on the rights of lesbian, gay, bisexual and transsexual people.¹⁹ It is vital that the very real issues of racial hate speech and incitement to racial violence are not also used as an excuse to block lawful online content for political or other spurious reasons.
17. Democratizing access to the internet is therefore a key issue both in terms of access to infrastructure and access to content. Access to the internet should become a human rights indicator and reported on by States, so that their progress in ensuring equality of access can be monitored. States must also develop and implement national internet access plans using multi-stakeholder processes which ensure participation by all, including racial and ethnic minorities and other groups.

¹² www.worldinternetproject.net

¹³ "World Internet Project 2012 International" Report Third Edition, 2012.

¹⁴ Ibid, at page 31.

¹⁵ http://www.apc.org/en/system/files/LisaHomer_MobileInternet-ONLINE.pdf

¹⁶ Eric Hersman "The potential of mobile web content in East Africa" in Vodafone Making Broadband Accessible for All (London: Vodafone Group, 2011).

¹⁷ PTA bans official Ahmadi website: Report <http://tribune.com.pk/story/404509/pta-bans-official-ahmadi-website-report/>

¹⁸ Ahmad, Zafar, Internet Rights in Pakistan, GISWatch Special Edition, forthcoming; Ban on Shia website: Police disperse protest rally in Karachi <http://tribune.com.pk/story/409505/ban-on-shia-website-police-disperse-protest-rally-in-karachi/>

¹⁹ SM Kee, Moolman, 2011. Sexuality and women's rights. Global Information Society Watch

Dilemmas

18. The power of the Internet as a space for enabling human rights has been undermined by cases of hate speech and incitement to hatred and violence against racial and religious minorities, women, and LGBTQI communities, among others. Concerns about incitement to racial and religious discrimination on the internet have been raised in the HRC, for example, by China, Poland, Bangladesh, Malaysia, Algeria, Germany, India and Estonia at UPR13. A key dilemma for governments is how to balance their obligations to protect citizens from such actions and, at the same time, not to react repressively or negatively, for example, to act out of fear or without lawful authority or to regulate, especially over-regulate, too far and too quickly. Another dilemma for States is to resist the temptation to treat the internet and regulation of online content in the exactly the same way as they do offline or traditional media. Unfortunately, many States have not responded well to these dilemmas and have resorted to censorship, takedown of lawful internet content, repressive online registration systems, internet shutdowns and telecommunications blackouts, perhaps the most famous being that which occurred in Egypt in 2011.²⁰
19. The possibility for such actions highlights the critical vulnerability of those who may be the targets of racist hate speech and incitement to violence and the dilemmas States face in acting according to human rights standards. On the one hand, shutdowns of internet access or other telecommunications may be used to avoid very real prospects of escalation of sectarian, communal or inter-racial violence and therefore may be justified in a narrow range of exceptional circumstances. On the other hand, experience in the Middle East, the United Kingdom and in the USA shows that such blanket shutdowns are a blunt instrument for dealing with such issues and may in fact exacerbate problems, heighten community tensions, or unfairly impact on innocent people putting them at risk.²¹ In the long term they do nothing to address the underlying causes of racial discrimination, views about racial superiority or to address xenophobia. We call for all States to prohibit such blanket internet shutdowns and communication black outs.
20. The amount of racist hate speech and xenophobic material online is of increasing concern and is being brought to the attention of various human rights bodies. For example, national human rights institutions in various countries are dealing with a growing number of complaints related to allegations of hate speech communicated online – through websites, social networks and other online platforms²². A further dilemma is how to balance concerns about such racist hate speech with human rights standards on limitations on acts of speech.
21. Limitations on freedom of expression are permissible, including restrictions “on hate speech (to protect the rights of affected communities), defamation (to protect the rights and reputation of others against unwarranted attacks), direct and public incitement to commit genocide (to protect the rights of others), and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (to protect the rights of others, such as the right to life)”²³. With regard to technical measures taken to regulate types of prohibited

²⁰ For a useful timeline of the communications shutdown in Egypt see Ramy Raouf “The internet and social movements” Global Information Society Watch (APC and Hivos, 2011) at 36 - 39.

²¹ Alex Comninou “New Challenges to Freedom of Peaceful Assembly and Freedom of Association on the Internet” (APC, publication forthcoming 2012).

²² SAHRC Email Communication June 29, 2012; Petrova, D. 2011. Incitement to National, Racial or Religious Hatred: Role of Civil Society and National Human Rights Institutions

²³ United Nations document A/HRC/17/27, (2011) para 25.

expression, such as the blocking of content, the Special Rapporteur on Freedom of Expression has reiterated that “States should provide full details regarding the necessity and justification for blocking a particular website and that the determination of what content should be blocked must be undertaken by a competent judicial authority or a body that is independent of any political, commercial or other unwarranted influences in order to ensure that blocking is not used as a means of censorship.”²⁴

22. Yet there are many cases where States limit freedom of expression and freedom of association on the internet in the name of protecting citizens from racist hate speech or xenophobia but in ways that do not comply with international standards such as Articles 21 and 22 of the ICCPR, nor Article 5 of CERD. At the February 2012 HRC Panel on freedom of expression and the internet, some countries, including China, Iran, and Thailand, called on measures to prevent perceived misuses of the internet such as: undermining national security, terrorism, extremism, racism, xenophobia, violence, political gain, criminality, pornography, intellectual property rights, cultural affront, Islamophobia and hate speech. While some of these are legitimate concerns, in reality civil society groups and human rights defenders, especially women’s human rights defenders, report that in many countries these claims of “misuse” are frequently used to limit lawful and legitimate political speech and democratic participation (see also country studies below).
23. States obligations to protect citizens’ rights online also come into focus with the increase of online attacks against independent media and human rights groups, which have proven to be an effective way of silencing voices and groups at critical times²⁵. It is therefore appropriate to consider whether States’ positive obligations include obligations to take reasonable measures of protection for peaceful assemblies and associations from attacks especially where these are racially motivated. States must also refrain from interfering with their own citizens’ rights through the use of such technical measures.
24. States need more guidance and assistance, perhaps from the SRRX or by way of new General Comments from the Committee for the Elimination of all Forms of Racial Discrimination, on best practice in this area. APC developed the Internet Rights Charter to help guide the application of human rights to the internet and information communication technologies²⁶ along with the “Connect Your Rights! Internet Rights are Human Rights” and other campaigns.²⁷ We encourage the SRRX to consider these and other civil society initiatives such as the Charter of Internet Rights and Principles, developed by the Internet Rights and Principles Coalition as helpful reference points in his work.²⁸

Challenges

25. There is an important distinction between the outer limits of permissible speech and other speech which falls inside these limits. The boundaries for hate speech are tolerably clear. But the more difficult areas are racial discrimination, harassment, and xenophobia that fall short of being incitement to hatred or violence, but are nonetheless inconsistent with human rights

²⁴ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression <http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf>

²⁵ Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, John Palfrey, *Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites*, The Berkman Center for Internet & Society at Harvard University (2010), <http://cyber.law.harvard.edu/node/6521>

²⁶ Internet Rights Charter available at <http://www.apc.org/en/node/5677/>

²⁷ Connect your Rights: <http://rights.apc.org>

²⁸ www.irpcharter.org

standards in particular contexts (such as public places). This is also an issue in relation to, for example, discrimination and violence against women, an area on which APC has been working for some time. Technology-related discrimination acts as a significant barrier to meaningful engagement with the internet by people in vulnerable communities. APC research on sexuality and women's rights suggests that women and girls who use the internet increasingly face online content that depicts, promotes and normalises violence against women. This creates a hostile online environment for women's voices and contributes to the creation of a communication culture that is discriminatory and tolerant of violence against women²⁹.

26. Some parallels exist with the communication culture in relation to racial and xenophobic content and the way in which this can create a hostile online environment for racial and ethnic minorities. This can also occur where online discourse is dominated in particular ways. In Saudi Arabia, for example, strong religious fundamentalism in online communities can create a chilling effect for those wishing to highlight diverse perspectives, with the result that many online users practice considerable self-censorship out of fear.³⁰ Self-censorship also has an alarming effect if it allows majority views to be perpetrated in ways that create hostility against racial, religious or other minorities. A challenge for governments is to strike the appropriate balance between acting to restrict access to such content through lawful limitations and positively acting to protect rights and freedoms, and the implications of leaving the online discourse alone. For example, one commentator has noted:³¹

“The Saudi Arabian government has often responded to external calls to change its heavily censored system by suggesting most censorship is self-regulated by citizens, and, in doing so, suggesting a quasi-democratic self-imposed regulation is in place. However, this response is too simple, as there is no policy in place to protect minorities from the wider religious community, led and often fuelled by far religious “scholars”.

27. Government actions to address racist hate speech and incitement to racial hatred must be lawful, in particular rational and proportionate. Too readily some government resort to arbitrary or unreasonable censorship, repressive control of online content, unlawful surveillance or website blocking (including denial of service attacks).³² More research is needed to understand the range of ways in which racial and ethnic groups experience these forms of discrimination, harassment and xenophobia while online and the strategies that they are using to combat them. We recommend the SRRX continue his work to document and collate best practice and the experiences of diverse groups in this area.

Privacy and Anonymity

28. A further challenge is to protect privacy and rights, including the right to online anonymity. Despite recognition by the Special Rapporteur on freedom of expression that “the right to privacy is essential for individuals to express themselves freely”³³, including the use of pseudonyms on message boards and chat forums, some governments and corporations have policies that prevent anonymous monikers online, or require users to register with personally identifying information. This can be particularly problematic for those in racial and ethnic

²⁹ SM Kee and Moolman, 2011. Sexuality and women's rights

³⁰ Rafid Fatani “Internet Rights in Saudi Arabia” (Association for Progressive Communications publication forthcoming in 2012).

³¹ Ibid.

³² For examples of these see

³³ Frank La Rue, HRC 17, April 2011 Paragraph 53. <http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/17/27&Lang=E>

minorities who are targets of hate speech or racial violence, since anonymous speech may be a critical component of their secure online communication.

Internet intermediaries

29. The unique multi-stakeholder nature of the internet and the operation of the internet ecosystem mean that private international law governs many public online spaces. There is considerable debate about human rights and the role of private providers or internet intermediaries. This includes their responsibility, if any, for the content their users share in public online platforms, such as Facebook, YouTube or Twitter, their role in “policing” online content and their human rights responsibilities under their terms and conditions of use and online content and behaviour policies.³⁴ Many human rights advocates consider such intermediaries should not be interfering with online content, are not law enforcement and should only act under due process of law. At the same time difficulties of accessing lawful remedies means that complaints under these policies may be the only remedies available to internet users who are harmed by acts of racist or xenophobic speech and who want to take action to mitigate or prevent harassment.
30. Internet intermediaries include internet service providers, internet cafes, blog hosts, mobile operators, social networking platform providers, and search engines. These play critical roles in supporting online communication and upholding freedom of expression and freedom of association by providing access to networks, and enabling online participation, including by diverse racial and ethnic groups and individuals. State activities which interfere with fluid online activity are growing, such as increasing licensing conditions requiring collection of user data, provision of user account information, requiring control of online content and behaviour, and the erosion of protection from liability for third party content. In many developing countries, significant portions of the population access the internet in public places, such as cyber cafes. These factors and activities can put individuals and groups which are the victims of racial discrimination and violence at risk, especially where personal data is required to be collected and stored.
31. We strongly recommend that in addition to following good practices when blocking or removing content (especially due process, such as lawful order by an independent court or other judicial body), that internet intermediaries regularly report on requests for content removal, and their response, in the interests of transparency and due diligence. Where companies provide a mechanism for dealing with complaints on their website and publishing regular statistical reports on complaints received and their response, the SRRX could usefully inquire whether any of these relate to content that is racist hate speech or incitement to racial violence and document the experiences of victims of online racist attacks.
32. The work of the Special Representative on Business and Human Rights, in particular the “Respect, Protect and Remedy” framework, including the requirement for corporations to undertake human rights due diligence is also useful.³⁵ We encourage the SRRX to consider how this framework might be useful in relation to the particular concerns of racial hate speech and incitement to racial hatred and violence.

³⁴ See for example Joe McNamee “Internet Intermediaries: the new cyber police?” Global Information Society Watch (APC and Hivos, 2011), at 25.

³⁵ See also the Report of the Special Representative on the issue of transnational corporations available at <http://www.ohchr.org/documents/issues/business/A.HRC.17.31.pdf>

Country Studies

These are provided to highlight just a few examples of the range of ways in which racist hate speech and incitement to violence is experienced online and its link to what occurs offline. There are many more examples available and we would be happy to provide the SRRX with these.

33. **BULGARIA:** Local research reveals that online forums and social networks are becoming dominated by extremist groups, for example, in 2011 hate speech flourished in reaction to a street murder by the driver of a crime boss who had been linked for years to political corruption. Online and offline protests against “Roma crime” began, and calls for the “protection of Bulgarians against Roma” have increased.³⁶ At the same time, other social groups are pushed away as they are not protected enough from such hate speech.³⁷ This has provoked official reaction against that speech, with a focus on the internet. According to Articles 162 and 163 of the Bulgarian Criminal Code, hate speech and provocation of aggression in written or oral form, including online communication, is a criminal offence, subject to a fine of EUR 2,500 to 5,000 and incarceration of two to four years. As in any policing of assemblies, there is a delicate balance between protecting an assembly and allowing free speech of others. Local online advocacy groups have called for public debate and regulation of freedom of speech and its limitations to better protect this balance. The Bulgarian government has sponsored online forums to help exercise people exercise their rights. This is a good example of how States can provide safe spaces for online consultation and services which help citizens exercise their rights.

34. **ESTONIA:** In 2005, an Estonian internet service provider refused to respond to requests from Moscow human rights organizations to close down the website of a neo-fascist group in Russia that promoted national hatred and issues instructions on bomb-making. The Estonian Institute of Human Rights subsequently informed relevant state authorities, including the Office of the President, and the website was taken down³⁸. This case demonstrates the importance of involvement by human rights organisations and NHRIs both nationally and internationally to prevent discrimination and incitement to violence.

35. **INDONESIA:** Local research shows the mainstream discourse in the Indonesian online sphere is tainted by incitement to discrimination and hate-speech due to its capacity to accommodate a diversity of expressions. The government has failed to respond in an individual and proportionate fashion to these threats, such as by regulation which requires establishing a direct and immediate connection between the expression and the threat. Over-generalising efforts to regulate the dissemination of “hate speech” via the internet, for example, by the introduction of the Defamation Codes in the ITE Law did not solve the problem and even created a trajectory of its own abuses.³⁹

36. **PAKISTAN:** APC member Bytes For All Pakistan has been following government censorship of the internet since 2003, including recent attempts by the Pakistan Telecommunication

³⁶ english.aljazeera.net/news/europe/2011/09/201192653812872853.html; www.turkishweekly.net/news/124179/170-arrested-in-bulgaria-after-second-39-roma-protests-39-night.html

³⁷ Vera Staevska, “Is freedom of expression and association on the net working on the street?” GISWatch 2011, <http://giswatch.org/en/country-report/freedom-expression/bulgaria>

³⁸ Dimintrina Petrova, 2011. Incitement to National, Racial or Religious Hatred: Role of Civil Society and National Human Rights Institutions (OHCHR, Vienna 9-10 February 2011)

³⁹ Ferdiansyah Thajib *The internet and freedom of expression in Indonesia* (APC forthcoming 2012).

Authority (PTA) to ban the use of certain words in SMSs,⁴⁰ to set up an Internet Filtering System along the lines of the Great Firewall of China and to employ a kill switch on digital communication in Balochistan⁴¹ and Gilgit-Baltistan. Limitations to freedom of expression are in many cases done on the grounds of 'religious morality' and 'national interest'. Articles 19 and 19-A of the Constitution of Pakistan provide for freedom of expression and right to information for citizens, but include vague language on reasonable restrictions, including "the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, commission or incitement to an offence"⁴². The increasing use of these provisions to take unreasonable action against ethnic and religious minorities is of concern.

37. **SOUTH AFRICA:** As with Indonesia and Pakistan, concerns have been raised over vague language with respect to content censorship, in this case involving actions by internet service providers (ISPs). For example, there have been adverse impacts from policies by ISPs such as iBurst, which prohibits content that "...could be deemed objectionable, offensive, indecent, pornographic, harassing, threatening, embarrassing, distressing, vulgar, hateful, racially or ethnically offensive, or otherwise inappropriate, regardless of whether this material or its dissemination is unlawful"⁴³. While aspects of the policy may be human rights compliant, the power to take down lawful content violates permissible limitations on freedom of expression.
38. **UNITED KINGDOM:** In March 2012 a man was sentenced to a jail term of 56 days after making racist remarks on Twitter about a football player, Fabrice Muamba⁴⁴. While these remarks are atrocious, it is not clear that the law under which they were prosecuted met the standard required by article 20(2) of the International Covenant, which stipulates that States shall prohibit any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence⁴⁵. The case highlights the importance of developing clear regulatory frameworks and international best practices to determine the appropriate response to acts speech that constitute racism, racial discrimination, xenophobia and related intolerance online.

Conclusions and Recommendations

39. We urge the SRRX to take a comprehensive approach to the issue of racism online, which recognizes the interconnection between multiple forms of discrimination and the generation of different forms of violence, a move we have also welcomed in relation to information communication technologies and violence against women⁴⁶. In this respect, we urge the SRRX to support the continued focus on full implementation of the Durban Programme for Action by

⁴⁰Filtering SMS: PTA may ban over 1,500 English, Urdu words <http://tribune.com.pk/story/292774/filtering-sms-pta-may-ban-over-1500-english-urdu-words/>

⁴¹Communication siege in Balochistan to mark Pakistan Day 2012 <http://content.bytesforall.pk/node/45>

⁴²The Constitution of Pakistan and Fundamental Rights http://www.sdpi.org/know_your_rights/know%20you%20rights/The%20Constitution%20of%20Pakistan.htm

⁴³ iBurst, 'Acceptable Use Policy', accessed from http://www.iburst.co.za/documents%5Clegal%5Cdocument_2.pdf on 18/05/2012 cited in Jane Duncan internet rights in South Africa (APC, publication forthcoming 2012),

⁴⁴ <http://www.bbc.co.uk/news/uk-wales-17515992>

⁴⁵ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression <http://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf> paras 26-28.

⁴⁶ This approach is echoed in the work of the SRRX outlined in *Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*, (United Nations, 2012, A/HRC/20/33 available at http://www.ohchr.org/Documents/Issues/Racism/A.HRC.20.33_en.pdf)

all States which calls for a comprehensive approach to addressing the root causes of racism, racial discrimination, racially motivated violence, xenophobia and related forms of intolerance.

40. We note the view, recently stated by the Maldives which endorsed the Declaration on Freedom Online (2011) in commenting at the HRC Panel on Freedom of Expression and the Internet, that:

The best way to respond to internet content which is objectionable to society at large, whether that is content on extremist religious views or racism, is by freeing up the internet so that extremist opinions can be defeated through argument and the power of numbers.

41. We endorse that general approach and consider that more can be done to develop best practice in responding to this critical issue, including prevention and active response strategies. For example, NGO campaigns (there are many) which encourage victims to assert themselves and, where possible, to self-advocate should be supported.
42. National action plans for internet access should be developed through multi-stakeholder processes with a particular focus on uptake by diverse groups. These action plans should include key indicators for internet access across all racial groups and disaggregate data on access by racial and ethnic groups and gender.
43. Where appropriate, special temporary measures permitted under ICERD should be undertaken to foster access to diversity of content in multiple languages including creating safe online spaces for particular groups.
44. We endorse the SRRX call for States to focus on these issues in the UPR and also call for this to be done in ICERD and ICCPR reporting. In doing so, States must consult with women and girls and include a focus on the specific for different groups of women and girls, particularly given their low rates of internet access.
45. The very nature of the networked internet, together with language and various jurisdictional issues suggests that international best practices should be developed in multi-stakeholder ways which are inclusive of civil society, media and the private sector. These should be offered widely to help guide how best to respond to racism and racial discrimination on the internet. We note that national human rights institutions may also have a helpful role to play in relation to monitoring this issue and dealing with complaints.
46. Legislation that protects against racist hate speech and incitement to racial hatred and violence should extend appropriately to the internet, but regulatory measures need to be light-handed and based on existing human rights standards with the clear understanding that internet users have the same human rights and freedoms online that they do offline. Technological developments are moving too fast for “fixed line” regulatory measures. Such an approach risks being quickly ineffective if regulatory measures are overly prescriptive or simply assume that current legislative frameworks will work online in the same way.
47. Instead, human rights, including the right to be free from racial discrimination need a “wireless network” approach to the practical application of core human rights standards so that citizens can connect their rights wherever they are and whenever they are online.

48. We further recommend

- *States support the development of a clear framework for respecting human rights online which underscores the protection of individuals from hostility, discrimination or violence, rather than to protect belief systems, or religious, political or other institutions from criticism.*
- *Access to the internet should become a human rights indicator and be monitored and reported on by States.*
- *States develop and implement national internet access plans using multi-stakeholder processes which ensure participation by all, including racial, ethnic and other minority groups.*
- *The Special Rapporteur to seek opportunities for collaboration with other special mandate holders on issues in relation to the internet. In particular, the mandate holders on the right to freedom of expression, on violence against women, on the situation of human rights defenders, on the right to health and on the right to education, to ensure they are addressing the internet aspect of their mandates collaboratively.*