Freedom of assembly and association online in India, Malaysia and Pakistan

Trends, challenges and recommendations

By Gayathry Venkiteswaran

APC
IMPACT
India . Malaysia . Pakistan
Advocacy for Change Through Technology

EXECUTIVE SUMMARY

Freedom of assembly and association (FoAA) online refers to peoples' use of information and communication technologies (ICTs) to exercise their rights to peaceful assembly or association, either offline or online. Civil society groups or interest groups have used communication technologies for social and political causes. These include tools like websites, email groups, mailing lists and social media platforms that are used to share information, organise protests or issue joint statements. There are many examples of like-minded citizens rallying for a cause or coming together informally, whether in a geographical location or across borders, utilising growing access to the internet. The widespread use of ICTs during the Arab Spring and the Occupy movement in New York, London and elsewhere has prompted global discussions on the rights to FoAA online.

Over a dozen resolutions from the UN General Assembly (UNGA) and UN Human Rights Council (UNHRC) as well as thematic reports from UN Special Rapporteurs have affirmed that rights and protections enjoyed offline should also be afforded online. The guarantees in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) provide the overarching framework in which these rights are to be applied offline and online.

This paper is part of the Association for Progressive Communications (APC) project entitled "Networking for freedom online and offline: protecting freedom of information, expression and association on the internet in India, Malaysia and Pakistan." It frames the discussions of FoAA online, focusing on the challenges, trends, recommendations and areas for further study in India, Malaysia and Pakistan. This research paper draws upon the work previously done by APC in providing guidance to the interpretation of these rights in the digital age through briefing papers and submissions to the UN human rights bodies, as well as the important contributions made by the special rapporteurs on rights to FoAA and rights to freedom of expression and opinion.

The paper was prepared based on literature and desk reviews, as well as interviews with partner organisations and experts. These were conducted between September and November 2015. The examples and cases highlighted are by no means exhaustive. Instead, the paper attempts to identify the key issues and framework that can be used by individuals and groups to further the research in their respective countries.

The study of the three countries showed that civil society groups, human rights defenders, marginalised groups, political parties and youth were major users of the internet for gathering and organising social and political movements, benefitting from the wider reach, the networks created and the ability to quickly mobilise online. For some, the internet offered possibilities to come together in relative safety, compared to physical gatherings which are more dangerous. Using social media platforms like Facebook and Twitter, mobile chat applications, online petitions and hacking, groups have organised protests, attracted participants to gatherings, shared information, and conducted forums and meetings. Often, offline and online tools or mediums were used in combination, with street mobilisation and online lobbying of legislators on FoAA. Through campaigns on net neutrality, anti-corruption

and stronger anti-rape laws, digital activism has led to legislative and executive responses in India. In Malaysia, Bersih, a movement for electoral reforms, capitalised on an active social media community to counter state threats and mobilise thousands of people to join street rallies since 2011. In Pakistan, concerned citizens mobilised over Twitter to stop evictions of people living in slums in Islamabad and to organise people in major cities to demand the arrest of a radical cleric following the deadly attack on a school in December 2014.

Not all experiences have been positive, as the internet has also made it possible for non-democratic forces, including state and non-state actors, to occupy the spaces at the same time. In some cases, the aim was to disrupt online social movements or to target individuals for their identities and beliefs. Political parties and religious groups use the internet to mobilise supporters and in the process to dominate the online public sphere, and offline threats have been replicated and intensified online. Across the three countries, the common threats include surveillance, censorship, filtering, network shut downs, cyber bullying, stalking, gender-based violence, hacking, privacy violation and corporate control, and misinformation.

Responses by organisations and individuals to such threats vary. Some have used strategic litigation as in the case of state surveillance or to challenge interpretations of assembly laws, while others have submitted cases and complaints to UN bodies and improved some of their own digital security practices. There are also those who opted to keep a low profile on social media or made no responses to the attacks.

When it comes to guaranteeing rights to assembly and association offline, governance, laws and practices are more restrictive in Malaysia and Pakistan, compared to India. The national constitutions provide guarantees, but at the same time include limitations on grounds of national security, integrity of the country, public order and public morals. These limitations have been translated into laws on national security, foreign funding to non-governmental organisations, criminal defamation, sedition, blasphemy and anti-terrorism that restrict assembly and association.

Many laws would not meet the ICCPR's strict test of legality, necessity, and proportionality. No laws specifically address the exercise of these rights online, but internet-related laws, as well as penal codes and other laws, contain strict content regulations and permit arbitrary acts of surveillance that leave individuals at risk of persecution for their actions.

Clearly, there is work to be done to ensure that people can exercise their rights to assembly and association online. States should take a more proactive role in implementing their obligations to protect these rights and to be more transparent and accountable in developing internet-related policies. The legislatures and courts should seek guidance from international human rights instruments and apply public interest considerations in enacting or reviewing laws and hearing cases. The private sector should engage civil society more actively and apply human rights standards in their business practices as more and more people rely on their platforms for communication and mobilisation. Civil society should seek support to enhance their digital security practices, raise public awareness on the importance of digital access and security, build alliances to advocate legal reforms, and utilise international mechanisms to seek remedies. The relevant international human rights mechanisms should reaffirm and sustain their focus on FoAA online by condemning violations where they occur, highlighting the issue in their reports and through joint statements.

ACKNOWLEDGEMENTS

This research would not have been possible without the information on laws, incidents and contacts from APC partner organisations, in particular, Ritu Srivatsa (Digital Empowerment Foundation - DEF), Haroon Baloch (Bytes for All, Pakistan) and Serene Lim (Persatuan Kesedaran Komuniti Selangor - EMPOWER).

Thanks also to the experts and stakeholders in the three countries who responded to the questionnaires sent out.

They are:

- Syahredzan Johan, Bar Council Committee member, National Young Lawyers Committee chair, Malaysia
- Fadiah Nadwa Fikri, human rights lawyer, Bersih steering committee member, Malaysia
- Hazlan Zakaria, journalist, Malaysia
- Zoe Randhawa and Izmil Amri Ismail, secretariat staff, Bersih, Malaysia
- Thilaga Sulathireh, LBGT activist, member of the Justice for Sisters campaign, Malaysia
- Sevan Doraisamy, executive director, Suara Rakyat Malaysia (SUARAM), Malaysia
- Mishi Choudhary, legal director, Software Freedom Law Centre
- Gayatri Khandhadai, human rights activist, India
- Yasser Hamdani, Lahore High Court lawyer, Pakistan
- Sadaf Khan, media activist and director of programmes, Media Matters for Democracy, Pakistan.

Appreciation also goes to APC's Deborah Brown and Debbie Budlender for providing inputs and guidance during the research.

INTRODUCTION

In September 2015, a leaked document from Thailand's military regime discussing the proposal for a single internet gateway for all international internet traffic led to an immediate online protest using a distributed denial of Service (DDoS) attack that was done over a few hours.[1] Asked about the attack on the website of the Ministry of Information and Communications Technology, the government spokesperson was quoted by the media as saying, "It's like a symbol [of protest]."[2] The government reluctantly recognised the protests of Thai citizens over a plan for a single gateway, which many saw as an attempt to control citizens' access to information and expression.

There are many more examples of like-minded citizens utilising growing access to the internet to rally for a cause or to come together informally, whether in a geographical location or across borders. The widespread use of the internet during the Arab Spring and the Occupy movements in New York, London and elsewhere[3] has prompted global discussions on the rights to freedom of assembly and association online. In Asia, the internet has been used to mobilise and organise political responses, among them the online protest to defend net neutrality in India, known as SavetheInternet.in campaign, which saw the country's telecom regulator receiving the largest number of emails sent over a single weekend in 2015.[4] There was also the global mobilisation for electoral reforms in Malaysia by the Coalition for Clean and Fair Elections (Bersih).[5]

The motivations for online mobilisation are not confined to internet-specific issues. They include articulating social and economic concerns and defending political positions. Yet, the enabling features of the internet have also introduced an element of risk, including counter narratives and threats that at times endanger individuals. In its Freedom on the Net 2015 report, Freedom House found that

1. Distributed denial of service (DDoS) attacks refer to attacks that involve the continuous flooding of a website by many users with requests, which can then cause the website to slow down or go offline. A large number of computers needs to be used for the attacks to be effective.
For more, see: Comninos, A. (2012). *Freedom of Peaceful Assembly and Freedom of Association and the Internet*. www.apc.org/en/pubs/freedom-peaceful-assembly-and-freedom-association

2. Pornwasin, A. (2015, 30 September). Angry Thai internet users 'bring down ICT website'. *The Nation*.

3. The links between these movements are interesting as a global phenomenon. Occupy London began outside the London Stock Exchange in 2011, sparked by the Occupy Wall Street in New York, to challenge the political and economic systems to put "people, democracy and the environment before profit". The Occupy Wall Street organisers say it used the "revolutionary tactics of the Arab Spring" to achieve its goals. The websites of the occupy movements can be seen here: occupylondon.org.uk/ and occupywallst.org/.

4. Jayadevan, P. (2015, 13 April). 1.5 lakh mails and counting: India lodges one of its biggest online protests over net neutrality. *The Economic Times*. articles.economictimes.indiatimes.com/2015-04-13/news/61103013_1_neutrality-data-charges-internet-service-providers

5. Postill, J. (2013). *A critical history of internet activism and social protest in Malaysia*, 1998-2013. RMIT University, Melbourne. rmit.academia.edu/JohnPostill/Papers

digital activism (such as calls to protests, online petitions and campaigns for social or political action) was one of the main topics censored in 17 of the 65 countries studied.[6]

Various international institutions, specifically the UN Human Rights Committee, the UN Human Rights Council (UNHRC) and the UN General Assembly (UNGA), have affirmed that the rights and protections enjoyed offline should be afforded online. Among others, the UNHRC resolution on the promotion, protection and enjoyment of human rights on the internet adopted in June 2012 articulated the need to extend the protection of rights that are exercised using information and communication technologies, including the internet.[7] In addition, the resolution also encouraged "special procedures to take these issues into account within their existing mandates, as applicable."

UN special rapporteurs have raised these in their reports to the UNHRC, including the special rapporteur on freedom of peaceful assembly and association (FoAA).[8] Over time, the maturity and depth with which actors within the UN system are exploring the online aspects of human rights through reports is increasing. The proliferation of resolutions – such as the resolutions on the protection of journalists (2013), women human rights defenders (2013) and ending violence against women (2015) – reflects the recognition that technology creates new threats and opportunities across a range of rights.[9] These developments are not coincidental. The prevalence of the internet and mobile technologies shifts many traditionally offline causes and movements online, not as separate forces, but in ways significant enough to warrant inquiries on how such shifts take place and with what impact.

This regional research paper frames the discussions of FoAA online, focusing on the challenges, trends, recommendations and areas for further study in India, Malaysia and Pakistan. It is part of the Association for Progressive Communications (APC) project entitled "Networking for freedom online and offline: protecting freedom of information, expression and association on the internet in India, Malaysia and Pakistan" also known as India, Malaysia, Pakistan, Advocacy for Change through Technology (APC-IMPACT).

The research element of the project ensures that information exists on how internet policy hampers and/or facilitates the enjoyment of human rights in the target countries. The research focuses on how the internet impacts

6. Freedom House. (2015). *Freedom on the Net 2015*. freedomhouse.org/report/freedom-net/freedom-net-2015

7. United Nations General Assembly, Human Rights Council. (16 July 2012). *The promotion, protection and enjoyment of human rights on the Internet.* (A/HRC/20/8). ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8

8. United Nations General Assembly. (7 August 2013). *Rights to peaceful assembly and of association*. (A/68/299). freeassembly.net/wp-content/uploads/2013/09/UNSR-elections-report-to-UNGA-Aug.-2013.pdf

9. United Nations General Assembly. (18 December 2013). *The safety of journalists and the issue of impunity Resolution 68/163.* (A/RES/68/163) www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/163 United Nations General Assembly. (18 December 2013). *Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: protecting women human rights defenders.* (A/RES/68/181). www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/181; United Nations General Assembly, Human Rights Council. (1 July 2015). *Accelerating efforts to eliminate all forms of violence against women: eliminating domestic violence* . (A/HRC/29/L.16/Rev.1) documents-dds-ny.un.org/doc/UNDOC/LTD/G15/140/16/PDF/G1514016.pdf

the exercise of freedom of assembly and association in the three countries and the threats and risks to users from surveillance, harassment, intimidation and other threats to privacy. India, Malaysia and Pakistan were selected because of the clear challenges to internet rights in these countries and the existence of strong partners well placed to promote and protect human rights on the internet. The three country partners are Digital Empowerment Foundation (India), Empower (Persatuan Kesedaran Komuniti Selangor, Malaysia) and Bytes for All (Pakistan).[10]

The paper draws upon the work previously done by APC in providing guidance to the interpretation of these rights in the digital age through briefing papers and submissions to the UN human rights bodies, as well as the important contributions made by the special rapporteurs on rights to FoAA and rights to freedom of expression and opinion.

The paper was prepared based on literature and desk reviews, and interviews with partner organisations and experts. These were conducted between September and November 2015. The examples and cases highlighted are by no means exhaustive. Instead, the paper attempts to identify the key issues and framework that can be used by individuals and groups to further the research in their respective countries.

The paper consists of five sections. Section I provides an introduction to FoAA online. Section II discusses the legal framework for understanding these rights and their application in the countries under study. Section III discusses the trends of FoAA online in the three countries. Section IV highlights threats, opportunities and remedies related to the exercise of FoAA online. Section V provides recommendations for the various stakeholders.

10. A description of the project is available on the website of the Association for Progressive Communications at: www.apc.org/en/projects/advocacy-change-through-technology-india-pakistan

Section I.

WHAT IS FOAA ONLINE?

FoAA online refers to peoples' use of ICTs to exercise their rights to assembly and association, either offline or online. While the offline rights are well developed within international human rights instruments, the online rights are still evolving. Nevertheless, numerous examples show how groups and individuals have used the internet to mobilise, and to come together on specific issues or interests where physical gatherings have been impossible or dangerous. Gathering and mobilising online or the use of ICTs for social and political causes began at the turn of the millennium, and even earlier in some countries. Civil society groups or interest groups have used email groups and mailing lists to share information and increase their outreach, organise protests or issue joint statements. With blogging and social networking tools, these initiatives reached wider audiences, encouraged interactivity and garnered more public support, both locally and internationally.

Some of the more notable examples of people exercising FoAA online in recent years have been the online protests in 2012 against the United States Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA), the use of social media during the Arab Spring, which started in Tunisia in 2010 and spread across to Egypt, Libya, Syria, Yemen and elsewhere in 2011, the anti-austerity *indignados* movement across 58 cities in Spain, and the Occupy protests in New York and London. Communication tools used by thousands of protestors and campaign supporters included social media sites Facebook and Twitter, video sharing platform YouTube, and streaming sites like Livestream.

In Asia, examples include LGBT-India, established in 1999 as an e-group, which then transitioned to Yahoo! Groups.[11] According to Software Freedom Law Centre legal director Mishi Choudhary,[12] the mailing list is still being used for discussion among middle-class, English-speaking Indians, and websites like LGBT-India and GayBombay function as online resources for the local and national readership.

In 1998 in Malaysia, a group of campaigners used the internet to disseminate information and mobilise support for a protest against the construction of the Sungai Selangor Dam, which was expected to have negative consequences on the indigenous peoples in the area and the environment. The campaign was ultimately unsuccessful but "it was the first concerted effort by civil society groups that made a conscious and effective use of the Internet to lobby support."[13]

In analysing the incidents of protests and mass movements that relied on or used ICTs, W. Lance Bennett and Alexandra Segerberg describe the digitally networked actions that are personalised and spread through social media, where the tools and spaces are not just communication channels. As the exam-

11. See: groups.yahoo.com/group/lgbt-india/

12. Email interview with Software Freedom Law Centre legal director Mishi Choudhary, 2 October 2015.

13. Randhawa, S., & Venkiteswaran, G. (2010). Civil Society use of media and ICT: A case study of the SOS Selangor Campaign. In Y. Seng Guan (Ed.), *Media, Culture and Society*. Routledge.

ples of the Put People First (PPF) in the UK and the *indignados* protests in Spain show, they "are flexible organisations in themselves, often enabling coordinated adjustments and rapid action aimed at often shifting political targets, including crossing temporal boundaries in the process."[14]

Studies and analyses lend support to the impact of social media on social movements, arguing that even if the results have been mixed, a "global protest movement based on social networks is here to stay"[15] or that social media provided the opportunities "for large-scale mobilisation and the organisation and implementation of social movements."[16]

The euphoria of the online revolution has come under criticism as well, for the exaggeration of the powers of the technology. In this context, it is worth reflecting on Evgeny Morozov's arguments that caution against blind faith in the liberating features of the internet, and to recognise that the "real effects of digital activism would most likely be felt only in the long term rather than immediately"[17] and that internet mobilisation must take into account the kinds of activism that would be able to yield the intended results.

Also noteworthy is that not all online activities and assembly carry messages of social justice or the promotion of human rights. UNESCO stresses in its 2015 framework study on a vision of internet-enabled knowledge societies that the outcome of the use of the internet is not always positive:

> The Internet is designed, implemented, and used by people. Its potential implications for supporting human rights, greater equity in access to information, education and knowledge, including gender equality, make it one of the most promising technologies of the information age. Yet public policies and regulation of the Internet, and patterns of Internet use, are not always positive in their outcomes.[18]

This regional paper recognises that while opportunities abound, particularly for groups and individuals who faced challenges in expressing their identities and political positions, the internet or online platforms have deepened the fault lines and threats against those already in a disadvantaged position. The research also notes that political structures that are more open have slightly more encouraging responses compared to the ones that are more repressive.

Several assumptions have been made while conducting this research. Firstly, the exercise of FoAA online is not solely confined to the internet. Long term and ad hoc associations or assemblies may originate online and move to the physical domains and vice versa, and more often than not, the role and use of the internet happen at different points of any given movement. This is reflective of how pervasive the internet is in the lives of many who

14. Bennett, W. L., & Segerberg, A. (2012). The logic of connective action: Digital media and the personalization of contentious politics. *Information, Communication and Society*, 15(5), 753.

15. Mason, P. (2013, 5 February). From Arab Spring to Global Revolution. *The Guardian.* www.theguardian.com/world/2013/feb/05/arab-spring-global-revolution

16. Eltantawy, N., & Wiest, J. B. (2011). Social media in the Egyptian Revolution: Reconsidering resource mobilization theory. *International Journal of Communication, 5*(18), 1207-1224. ijoc.org/index.php/ijoc/article/view/1242/597

17. Morozov, E. (2011). The net delusion: The dark side of Internet freedom. *Public Affairs, 198*.

18. UNESCO. (2015). *Keystones to foster inclusive Knowledge Societies: Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet.* unesdoc.unesco.org/images/0023/002325/232563E.pdf

use it for communicating with one another and to conduct transactions, organise, plan and share. In other words, people go in and out of the spaces depending on the cause or interest, target groups, strategies, and to a lesser extent, results expected. This then explains why responses to the movements or groups online can occur both online and offline.

Secondly, the exercise of the rights to FoAA online is not always strategically considered based on the clear articulation of goals, objectives or impact. As such, this paper does not assess the quality of the actions, but examples are used to highlight how the internet is used and if any results were recorded.

Thirdly, for people to be able to organise online, the minimum requirement is access to the content and technologies,[19] digital literacy and the ability to differentiate the platforms, benefits, risks and threats. The cases and discussions assume the users have some level of access and literacy, but it became obvious in the research that this assumption should not be treated as a given.

Definition of terms

Based on the international standards and for the purpose of this research, FoAA online refers to the rights of all persons to express their opinions on, join together with other individuals and engage in activities related to civil, political, economic, social, and cultural rights. It also refers to the right to be part of, or form associations. These rights are enabled or enhanced through new technologies, including the internet, and the limitations to these rights must be permitted by international human rights law. The research recognises two aspects of the rights: one where the exercise of FoAA is carried out online such as online petitions and protests – including virtual protests and "hacktivism"[20] – and one where technology is used to enable FoAA online and offline.

Maina Kiai, United Nations special rapporteur on the rights to freedom of peaceful assembly and of association, noted in his first thematic report to the UNHRC in 2012 that while rights to form associations and to assemble have been used interchangeably, they are two separate rights that are governed by different laws and have different sets of challenges.[21]

19. In his report to the UNHRC in 2011, Frank La Rue, the former UN Special Rapporteur on the freedom of expression and opinion, proposesd the importance of access to the internet with as little restriction as possible and the availability of necessary infrastructure as a human right.
See: LaRue, F. & United Nations Human Rights Council. (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. Geneva: United Nations. www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

20. According to ARTICLE 19, "hacktivism is defined as a collective action of technologically-skilled individuals through the use of digital technologies to protest without gathering in person. Most are considered a form of electronic civil disobedience due to related violation of the law. The organisation argues that international law allows for consideration of these actions as forms of freedom of expression and assembly. See ARTICLE 19 for their background paper on right to protest: right-to-protest.org/wp-content/uploads/2015/06/Right-to-Protest-Background-paper-EN.pdf

21. Kiai, M., & United Nations Human Rights Council. (2012). *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai.* Geneva: United Nations. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-27_en.pdf

Associations online refers to the act of forming groups, including informal ones, online, with or without moderators or group leaders, based on the definition provided by Kiai, who said that:

> Association refers, inter alia, to civil society organisations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions, foundations or even online associations as the Internet has been instrumental, for instance, in "facilitating active citizen participation in building democratic societies."

Associations could be ad hoc, for a specific cause or issue, or over a long term.

Peaceful assembly online refers to an intentional and temporary gathering in a private or public space for a specific purpose that includes the acts of coordinating, organising, gathering, planning or meeting on platforms available online such as instant messaging, voice over internet protocol, chat applications, email groups and mailing lists, among others. In his 2012 report to the HRC, Kiai "noted the increased use of the Internet, in particular social media, and other information and communication technology, as basic tools which enable individuals to organise peaceful assemblies."

Internet and *online* are used interchangeably to refer to the network or interconnected ICTs including the web, social media, mobile based internet, cloud computing and big data.[22] The term "digital activism" is also used where the internet and mobile tools are used in organising actions and movements. The lines can be unclear when an online communication is one of expression, association, for the purposes of assembly, or some combination of multiple rights. As an example, the use of a social media platform like Facebook to share ideas about a campaign or to call for participation reveals overlaps in the exercise of the two rights specifically (association and assembly) and with others like freedom of expression generally. An online petition is relatively clearer and can be categorised as a form of protest, but the use of mobile chat applications by protest organisers is more difficult to distinguish. This conundrum is dealt with by Alex Comninos who writes that:

> The intricacy with which the concepts of association and assembly are intertwined, and the difficulty in cleaving them apart perhaps suggests that these two rights need to be dealt with by means of an integrated approach which acknowledges their similarities and interdependence, and that the exercise of these rights face the same challenges and opportunities.[23]

Some of the distinctions between online and offline FoAA, for example, how online associations are not bound by geographical boundaries like their offline counterparts or whether limitations in the public space will apply online, are elaborated on in a training curriculum on "Internet Rights Are Human Rights" by APC.[24]

22. UNESCO. (2015). Op. cit., 14.

23. Comninos, A. (2012, June). Op. cit., 9.

24. Souter, D., & APC. (2013). Multimedia Training Kit: Freedom of Association and Freedom of Assembly Handout. itrainonline.org/itrainonline/mmtk/APC_IRHRCurriculum_FOA_Handout.pdf

Section II.

LEGAL FRAMEWORK

This section outlines the legal frameworks and application of rights and freedoms in international human rights conventions and within the national contexts. It begins with some of the main UN resolutions related to the internet and human rights as well as FoAA, the Universal Declaration of Human Rights (UDHR), and the International Covenant on Civil and Political Rights (ICCPR). It is followed by a discussion of the national laws in the three countries and a brief overview of the country contexts regarding the state of human rights and governance and access to the internet.

Rights offline must be protected online: International frameworks

The first UN resolution on the impact of the internet on human rights was adopted by the United Nations Human Rights Council (UNHRC) in 2009[25] in the context of freedom of opinion and expression. In 2012, the UNHRC adopted resolution 20/8 on the promotion and protection of human rights on the internet. This resolution is particularly useful to contextualise discussions in this research paper as it is one of the key human rights commitments recognising the importance of the internet and its links with the enjoyment of other human rights. In particular, the resolution affirms that the same rights that people have offline must also be protected online, calls on states to promote and facilitate access to the internet, encourages the UN special procedures to take the issues related to internet rights into account within their mandates, while deciding to continue its consideration of the promotion, protection and enjoyment of human rights on the internet and other technologies.[26]

Another important development in the promotion and protection of FoAA was the creation of the United Nations Special Rapporteur on the rights to peaceful assembly and of association by the UNHRC through resolution 15/21 in 2010 to examine, monitor, advise and publicly report on the rights worldwide. UNHRC resolutions 21/16 and 24/5 specifically remind states of their positive obligations to promote and facilitate access to the internet and online spaces for individuals "including persons espousing minority or dissenting views or beliefs, human rights defenders, trade unionists and others, including migrants, seeking to exercise or to promote these rights" to be able to exercise their rights to peaceful assembly and association online and offline, including in the context of elections.[27] They emphasise the role of

25. United Nations General Assembly, Human Rights Council. (2009). (A/HRC/12/16). *Freedom of opinion and expression*. documents-dds-ny.un.org/doc/RESOLUTION/GEN/G09/166/89/PDF/G0916689.pdf?OpenElement

26. UNHRC. (2012). (A/HRC/20/8). Op. cit.

27. United Nations General Assembly, Human Rights Council. (2012, 27 September). *The rights to peaceful assembly and association.* (A/HRC/RES/21/16). freeassembly.net/wp-content/uploads/2013/11/AHRC2116-2012.pdf; United Nations General Assembly, Human Rights Council. (2013, 8 October). *The rights to peaceful assembly and association.* (A/HRC/RES/24/5). freeassembly.net/wp-content/uploads/2013/08/A-HRC-RES-24-5-ENG.pdf. This resolution sought to renew the mandate of the Special Rapporteur, Maina Kiai, for another term.

states to "take all necessary measures to ensure that any restrictions on the free exercise of the rights to freedom of peaceful assembly and of association are in accordance with their obligations under international human rights law."[28]

It is important to highlight the link between freedom of association and freedom of expression as well as the significance of internet freedom[29] in the context of FoAA online. One document that expresses this link is the Declaration on Human Rights Defenders of 1998.[30] Frank La Rue, the former special rapporteur on the promotion and protection of the right to freedom of opinion and expression, recognised the opportunities of access to information online as crucial for individuals and reiterated the important links between the right to demonstration in the context of rights to participation in public affairs (Article 25 of the UDHR).[31] In its 2015 report on the right to protest, ARTICLE 19, a human rights organisation, also suggests that online protests – namely virtual protests and "hacktivism" – should be recognised as forms of freedom of expression and assembly.[32]

The issues around which people have rallied online relate to other rights that have been affected, such as land rights, access to justice, women's rights, end to gender based violence, political participation and the right to religious freedom. As such, other instruments that are relevant to the discussions on FoAA online include the International Covenant on Economic, Social and Cultural Rights (ICESCR), the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), and the International Convention on All Forms of Elimination of Racial Discrimination (ICERD), which provide the human rights framework regarding the rights of women, minority communities etc., in exercising their rights in public and private spaces, without fear of discrimination and violence.[33] Though not specifying the use of the internet, these conventions obligate states to respect the rights of the individuals and groups to use other rights, such as access to all forms of media, freedom of opinion and expression, to come together and to assemble, to exercise their specific rights.

28. See paragraph 1 of: United Nations General Assembly, Human Rights Council. (2010, 6 October). *The rights to peaceful assembly and association.* (A/HRC/RES/15/21). www.icnl.org/research/resources/dcs/UNHRCResolution.pdf

29. Internet freedom refers to an internet that is free of censorship, has universal access and affordable networks; is open; has freedom of innovation; and where privacy is protected (these are among the global principles adopted by civil society in demanding for internet freedom).

30. United Nations General Assembly. (1999, 8 March). *Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms.* (A/RES/53/144). www.ohchr.org/Documents/Issues/Defenders/Declaration/declaration.pdf

31. Human Rights Council. (2014, 2 July). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. daccess-dds-ny.un.org/doc/UNDOC/GEN/G14/071/50/PDF/G1407150.pdf?OpenElement

32. ARTICLE 19. (2015). *The "Right to Protest": Background paper*. right-to-protest.org/wp-content/uploads/2015/06/Right-to-Protest-Background-paper-EN.pdf

33. For the list of the nine core international human rights instruments, see www.ohchr.org/EN/ProfessionalInterest/Pages/CoreInstruments.aspx

TABLE 1

Selected UN resolutions with specific provisions on protections and rights offline that should be applied online, cutting across different rights

16 July 2012	UNHRC Resolution 20/8: The promotion, protection and enjoyment of human rights and the internet ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8
11 October 2012	UNHRC Resolution 21/16: The rights to peaceful assembly and association freeassembly.net/wp-content/uploads/2013/11/AHRC2116-2012.pdf
26 September 2013	UNHRC Resolution 24/5: The rights to peaceful assembly and association freeassembly.net/wp-content/uploads/2013/08/A-HRC-RES-24-5-ENG.pdf
27 September 2013	UNHRC Resolution 24/21: Civil society space: creating and maintaining, in law and in practice, a safe and enabling environment ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/24/L.24
18 December 2013	UNGA Resolution 68/163: The safety of journalists and the issue of impunity www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/163
	UNGA Resolution 68/167: The right to privacy in the digital age www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167
	UNGA Resolution 68/181: Protecting Women Human Rights Defenders www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/181
14 July 2014	UNHRC Resolution 26/13: The promotion, protection and enjoyment of human rights on the internet www.apc.org/en/system/files/G1408283.pdf
1 July 2015	UNHRC Resolution 29/L14: Accelerating efforts to eliminate all forms of violence against women: eliminating domestic violence ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/L.16/Rev.1
1 October 2015	UNHRC Resolution 30/9: Equal participation in political and public affairs ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/30/L.27/Rev.1

International conventions

Guarantees for freedom to peaceful assembly and association are articulated in the UDHR 1948, where Article 20 states that "everyone has the right to freedom of peaceful assembly and association" and no one shall be compelled to be part of an association.[34] The three countries, as all UN members, are parties to the UDHR, and even though not directly binding on states, the guarantees are accepted as customary international law and have made their way into the respective constitutions. The ICCPR, which imposes formal obligations on states that have ratified the convention, further elaborates on these rights under Articles 21 (peaceful assembly) and 22 (association).[35]

Article 21 reads:

> The right of peaceful assembly shall be recognised. No restrictions may be placed on the exercise of this right other than those imposed in conformity with the law and which are necessary in a democratic society in the interests of national security or public safety, public order (*ordre public*), the protection of public health or morals or the protection of the rights and freedoms of others.

Article 22 states that:

> 1. Everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of his interests.
>
> 2. No restrictions may be placed on the exercise of this right other than those which are prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others. This article shall not prevent the imposition of lawful restrictions on members of the armed forces and of the police in their exercise of this right.
>
> 3. Nothing in this article shall authorise States Parties to the International Labour Organisation Convention of 1948 concerning Freedom of Association and Protection of the Right to Organise to take legislative measures which would prejudice, or to apply the law in such a manner as to prejudice, the guarantees provided for in that Convention.

Restrictions to the rights are permitted within the ICCPR, but as outlined in the UNHRC resolution 15/21, these should be exceptions and only used in the last resort. They should be prescribed by law, necessary and proportionate, on grounds of national security or public safety, public order and the protection of public health or morals, or in order to protect the rights and freedoms of others.

The UN Human Rights Committee, which issues authoritative interpretations of the ICCPR, further elaborated that:

> ...the mere existence of reasonable and objective justifications for limiting the right to freedom of association is not sufficient. The State party must further demonstrate that the prohibition of an association is necessary to avert a real and not only hypothetical danger to national security or democratic order, and that less intrusive measures would be insufficient to achieve the same purpose.[36]

34. For the full text of the UDHR, see: www.un.org/en/universal-declaration-human-rights/index.html

35. For the full text of the ICCPR, see: www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

36. United Nations Human Rights Committee. (1999, 1 November). *General Comment No. 27*. (CCPR/C/21/Rev.1/Add.9). Paragraph 14. tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.9&Lang=en

On the right to assembly, Maina Kiai, United Nations special rapporteur on the rights to freedom of peaceful assembly and of association, has suggested that notifications to the authorities about a gathering should be adequate instead of having to seek approval, while rights to association should also include protections for those that are unregistered.[37]

National legal frameworks for India, Malaysia and Pakistan

While there are no specific laws relating to the exercise of FoAA online, the rights are articulated in the respective constitutions and national laws for the traditional enjoyment of the rights and permissible limitations. A brief look at the laws is relevant insofar as more and more physical gatherings are planned, organised and mobilised online. In addition, it is important to understand how other laws that directly or indirectly relate to the internet have been applied particularly in restricting FoAA online, as the examples will show in the later sections.

The three countries in focus share a background in common law and have similar constitutional and legal traditions, which primarily draw upon the British colonial history, making the comparisons convenient. The provisions for civil and fundamental liberties in the respective constitutions as well as the criminal codes tend to share similar language.

Yet, the political traditions and cultures are diverse, as is the role of the courts in setting standards when it comes to the protection of fundamental liberties. Discussions of FoAA and the application of laws in Pakistan also need to be seen in the context of the ongoing threat of terrorism and government/military responses to counter-terrorism and human rights violations.[38] This is also true, to a lesser extent, in India, where it is spurred by the ongoing border conflict with Pakistan, the separatist movements in the northeast and other internal security-related challenges. The defence of Sunni Islam by the state in Pakistan and Malaysia also plays a major role in how rights to expression and FoAA, offline and online, are affected by the laws and courts.

National constitutions of India, Malaysia and Pakistan

The constitutions of the three countries provide citizens with guarantees for the rights to assemble peacefully and without arms, and to form associations (Article 19 in India; Article 10 in Malaysia and Articles 16 and 17 in Pakistan).[39] Restrictions to these rights are subject to compliance with laws, in the interest of national sovereignty or security, or the integrity of the country, and public order.

The protection of public morality is specifically mentioned as a restriction to the rights to association in all countries. The Constitution of Malaysia provides for restrictions on associations by laws on labour and education (Article 10(3)), while the Constitution of the Islamic Republic of Pakistan imposes condi-

37. The United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association has produced factsheets on the rights, permissible limitations and how the rights apply online. They can be accessed at: www.freeassembly.net

38. For an updated status of human rights in Pakistan and information regarding Baluchistan, see: Human Rights Commission of Pakistan. (2015). *State of Human Rights in 2014*. Lahore, Pakistan: Human Rights Commission of Pakistan. hrcp-web.org/hrcpweb/data/HRCP%20Annual%20Report%202014%20-%20English.pdf

39. For the full text of the Constitution of India, see: lawmin.nic.in/olwing/coi/coi-english/coi-indexenglish.htm

For the full text of the Constitution of Malaysia, see: en.wikisource.org/wiki/Constitution_of_Malaysia

For the full text of the Constitution of Pakistan, see: www.pakistani.org/pakistan/constitution

tions on political parties deemed prejudicial to the federation (Article 17(2)) and requires parties to declare their sources of funding (Article 17(3)).

The constitutions in all three countries allow for the governments to impose "reasonable" restrictions, some of which have negatively impacted on individuals' fundamental rights. Article 148(3) of the Pakistani constitution provides for the protection of its provinces from external aggressions and internal disturbances, which is particularly relevant in cases relating to the rights of people in provinces such as Baluchistan. The respective legislative bodies have used the constitutional provisions to enact laws to control expression and public gatherings, or introduce stricter requirements and penalties for offenders.

National laws of India, Malaysia and Pakistan

Freedom of peaceful assembly

The Code of Criminal Procedure, 1973 in India and the penal codes of Pakistan and Malaysia contain provisions that regulate assemblies, including defining what is a public assembly and prohibitions on use of weapons during assemblies and participation in an unlawful assembly.

The two relevant Pakistan Penal Code provisions are as follows:[40]

> Section 144: Whoever, being armed with any deadly weapon, or with anything which, used as a weapon of offense, is likely to cause death, is a member of an unlawful assembly/shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

> Section 145: Whoever joins or continues in an unlawful assembly, knowing that such unlawful assembly has been commanded in the manner prescribed by law to disperse, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

Important in the context of Pakistan is the prohibition imposed on religious minorities, especially Ahmadi Muslims who are not allowed to identify themselves as Muslims, gather for prayers or use any references to Islam, the prophet or the *Adzan* (call for prayers), among others. This prohibition was introduced in 1984 under Sections 298B and 298C of the Penal Code.

Section 129 of India's Code of Criminal Procedure, 1973 authorises the police to disperse any unlawful assembly which may cause disturbance to public peace, while Sections 130 and 132 contain provisions on use of armed forces to disperse assembly and protection against prosecution for acts done under the preceding sections.[41] Section 144 can be used by the government in certain areas to make the assembly of five or more people an unlawful assembly. Interestingly, this was used by the Gujarat state government and endorsed by the Gujarat High Court to ban access to websites in the state in 2015.

In Malaysia, in addition to provisions in the Malaysia Penal Code,[42] the government in-

40. Pakistan Penal Code (Act XLV of 1860), §144-145, 298 (1860). www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html

41. The Code of Criminal Procedure, §144 (1973). www.icf.indianrailways.gov.in/uploads/files/CrPC.pdf

42. Malaysia Penal Code, Act 574 §124B (1936). www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Penal%20Code%20%5BAct%20574%5D2.pdf

troduced a Peaceful Assembly Act in 2012[43] which replaced provisions in the Police Act, to regulate public assemblies. Section 124B of the penal code (which was also introduced in 2012) on unlawful assemblies was used for the first time in August 2015 against activists and organisers of an anti-government rally. The section reads:

> Whoever, by any means, directly or indirectly, commits an activity detrimental to parliamentary democracy shall be punished with imprisonment for a term which may extend to twenty years.

Freedom of association

A host of laws exist in all three countries to regulate the existence and operations of associations, including societies, clubs, trade unions, professional bodies, charity groups, non-governmental organisations and others. Limitations have been prescribed on collectives and groups for reasons of anti-terrorism, dissenting politics, religious "deviancy" and breaching the hegemonic social norms such as sexual and gender orientation.

For example, in India, the formal establishment of non-governmental organisations or trusts will be subject to laws such as: the Societies Registration Act, 1860,[44] the Charitable and Religious Trusts Act, 1920[45] and the Religious Endowment Act, 1863.[46] The Foreign Contribution Regulation Act, 1976[47] that governs the foreign funding of NGOs has also proved controversial. It bars use of foreign funding for those indulging in political activities, and a 2010 amendment includes carrying out political actions such as the *bandh* or *hartaal* (protest, strike) in support of public causes.

Civil society groups have long questioned and challenged the act and its arbitrary application as a tool to curb dissent and threaten deregistration.[48] A similar trend is expected in Pakistan with controls on foreign funding as a draft Foreign Contributions Act is being considered.[49]

Other laws that exist in Pakistan to govern formal organisations include:

- The Societies Registration Act, 1860[50]
- The Charitable and Religious Trusts Act, 1920[51]
- The Mussalman Wakf Act, 1923[52]

43. The Peaceful Assembly Act, Act 736 (2012). www.federalgazette.agc.gov.my/outputaktap/20120209_736_BI_JW001759%20Act%20736%20(BI).pdf

44. The Societies Registration Act (1860). www.mca.gov.in/Ministry/actsbills/pdf/Societies_Registration_Act_1860.pdf

45. Charitable and Religious Trusts Act (1920). cconpo.icai.org/wp-content/uploads/2012/05/Charitable-and-Religious-Trusts-Act-1920.pdf

46. Religious Endowment Act (1863). cconpo.icai.org/wp-content/uploads/2012/05/The-Religious-Endowment-Act-1863.pdf

47. The Foreign Contribution Regulation Act (1976). www.fcraforngos.org/pdf/1976act.pdf

48. The case of Greenpeace International in India is an example, where the government cancelled its registration under the Foreign Contribution Registration Act, 1976. The decision was challenged and the court granted an interim stay of the cancellation, at the time of writing.

49. For a detailed and updated overview of the NGO registration process in Pakistan, see: www.icnl.org/research/monitor/pakistan.html

50. Societies Registration Act (1860). punjablaws.gov.pk/laws/1.html

51. The Charitable and Religious Trusts Act (1920). cconpo.icai.org/wp-content/uploads/2012/05/Charitable-and-Religious-Trusts-Act-1920.pdf

52. Mussalman Wakf Act (1923). indiankanoon.org/doc/188677788

- The Companies Ordinance, 1984[53]
- The NWFP Local Government Ordinance, 1984.[54]

A Malaysian human rights organisation, Suara Rakyat Malaysia (SUARAM), says that at least five laws in the country are known to restrict citizens' rights to association:

- The Societies Act 1966[55]
- The Trade Unions Act 1959[56]
- The Universities and University Colleges Act 1971[57]
- The Legal Profession Act 1976[58]
- The Prevention of Terrorism Act 2015.[59]

Human rights organisations encounter obstacles when registering themselves and many have signed up as companies under the Companies Act 1965[60] to circumvent the arbitrary regulation of the Registrar of Societies, and still be able to legally raise funds. Progressive organisations like SUARAM and a coalition of human rights organisations in the United Nations Universal Periodic Review Process, COMANGO, have been threatened by the authorities with action because of the nature of their work that challenged establishment politics. The state has not taken any specific actions but the cases highlight the difficult climate for "anyone or any group trying to offer a critique of the human rights and government situation in the country."[61]

Most of the laws mentioned above, with the exception of those on receiving foreign funding, may not be relevant for groups that are created and maintained online, over platforms such as Facebook, Google, email or mobile applications. Instead, these private companies and service providers could directly and indirectly be subject to legal and financial requirements by governments wishing to curtail the activities of users, or liable as intermediaries that fail to regulate content.

In other countries with similar legislative histories such as Singapore, online communities perceived to be rallying around political issues have been legislated through a law called the Political Donations Act 2001 which was used to gazette human rights NGOs and online media, as political associations.[62]

Internet-related laws

The existing internet-specific laws lie within the framework of telecommunications policy, computer related crimes, and facilitating investigations including allowing for intercept-

53. Companies Ordinance (1984). www.secp.gov.pk/corporatelaws/pdf/CO1984_%20Feb09.pdf
54. NWFP Local Government Ordinance (1984). www.khyberpakhtunkhwa.gov.pk/Gov/files/v9_0094.htm

55. The Societies Act, Act 335 (1966). www.scribd.com/doc/55591930/Akta-Pertubuhan-1966

56. Trade Unions Act (1959). aseanhrmech.org/downloads/malaysia-Trade_unions_act.pdf

57. Universities and University Colleges Act (1971). apps.ideal.upm.edu.my/website/master/rules2003_rev2012.pdf
58. Legal Profession Act (1976). www.lawyerment.com.my/library/doc/laws/casecode/profs/lpa

59. Prevention of Terrorism Act (2015). www.federalgazette.agc.gov.my/outputaktap/akta-BI_20150604_Act769(BI).pdf

60. Companies Act (1965). www.scribd.com/doc/3333802/Companies-Act-1965-revised-1-January-2006

61. SUARAM. (2014). *Malaysia Human Rights Report 2014: Civil and Political Rights.* Malaysia: Suara Inisiatif Sdn Bhd.

62. Political Donations Act (2001). statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A%22d9bac77b-5520-435b-9325-101373ac9acf%22%20Status%3Ainforce%20Depth%3A0;rec=0

ing communications and surveillance, among other responses.

Sections 69A and 69B of the Information Technology Act of India, 2000[63] provide for the take down of websites or blocking access to websites. According to digital law expert Mishi Choudhary, these provisions give power to the government to block public access to any information through any computer resource for cyber security and that together with the Code of Criminal Procedure, this can be used to restrict the right to assemble.

In Malaysia, Section 211 of the Communications and Multimedia Act 1998[64] criminalises the dissemination of information considered "indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten, or harass any person" while Section 233 penalises those who misuse the network facilities to disseminate the content.

Pakistan's Telecommunications (Re-organization) Act, 1996[65] allows for the government to authorise anyone to intercept communications, and to suspend or modify conditions of telco license holders or suspend the operations or functions of any licensees for any period. In addition, the Electronic Transaction Ordinance 2002[66] makes it a non-bailable offence to damage information systems or breach privacy of information, which could be used against hackers or those conducting online protests, including DDoS attacks.

As this report was written, the Pakistan National Assembly was deliberating the Prevention of Electronic Crimes Bill, which activists and experts say will undermine individuals' civil liberties in the name of combating terrorism.[67] David Kaye, the current United Nation Special Rapporteur on freedom of expression, has expressed his concern that the draft law, if passed, would among others, criminalise legitimate expression and threaten rights to privacy and lead to self-censorship within the media.[68]

Other laws

A cursory scan across the three countries found that laws governing content regulation and national security, *sharia*[69] laws and cybercrime laws will most likely impact on the exercise of FoAA online. Civil society groups and experts point to the frequent use of non-internet based laws, some dating back a century or more, against activities and expression online.

63. Information Technology Act of India §69 (2000). deity.gov.in/content/view-it-act-2000

64. Communications and Multimedia Act §211, 233 (1998). www.skmm.gov.my/Legal/Acts/Communications-and-Multimedia-Act-1998-Reprint-200.aspx

65. Pakistan's Telecommunications (Re-organization) Act (1996). www.pta.gov.pk/media/telecom_act_170510.pdf

66. Electronic Transaction Ordinance (2002). legaladvicepk.com/electronic-transactions-ordinance-2002-1238.html

67. Ashraf, G. (2015, 17 December). Prevention of Electronic Crimes Bill 2015: Vaguely worded law may result in censorship. *Express Tribune*. tribune.com.pk/story/1011418/prevention-of-electronic-crimes-bill-2015-vaguely-worded-law-may-result-in-censorship/

68. OHCHR. (2015, 14 December). UN expert urges Pakistan to ensure protection of freedom of expression in draft Cybercrime bill [Press release]. www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=16879&LangID=E

69. Sharia (or spelt as syariah in Malaysia) refers to the body of Islamic law that regulates public and some private aspects of life based on Islam.

Activists in Malaysia cite the Sedition Act 1948,[70] Section 505 of the Penal Code[71] and the legislated Securities Offences (Special Measures) Act 2012,[72] which replaced the controversial Internal Security Act (ISA), a law on detention without trial, as the legal tools used by the state to restrict expression and mobilisation.

In 2015, the Sedition Act was amended to include a provision that empowers the Session Court to prohibit a person from accessing any "electronic device" with no definition as to what would constitute an "electronic device". This disproportionate penalty has the potential to be used to restrict FoAA online, freedom of expression, and the right to full participation in public life.[73] Section 505 of the Penal Code deals with criminal defamation and incitement, and is used as an alternative provision to the Sedition Act to restrict FoAA offline and online. Any forms of mobilisation that are seen as questioning the government, institutions of royalty, Islam and Malay rights are quickly acted upon.

Preventive detention is also contained in the Protection of Pakistan Ordinance 2014[74] which could affect citizens' right to assemble. It vaguely includes crimes such as internet offences and other offences related to information technology, which critics said impact greatly on individuals and NGOs that rely on the "multiplier effect of social media and digital news outlets to highlight issues of injustice and human rights."[75] The Penal Code of Pakistan criminalises sedition (Section 124A) as well as blasphemy (the related provisions are Sections 295A, 295B, 295C, 298 and 298A).[76] The latter offence carries a death penalty. Lawyer Yasser Hamdani explains that in terms of limitations to FoAA online, the provision on blasphemy is the most likely to be used, and even then, it would result from complaints by private individuals, rather than the state.

The Investigation for Fair Trial Act 2013[77] in Pakistan gives security agencies the authority to collect evidence using modern techniques and devices, in others words to conduct surveillance and to intercept communications, enhancing the provisions in the Pakistan Telecommunications (Re-organization) Act.

In Malaysia, Section 114A of the Evidence Act, which was introduced in 2012, holds internet account holders and intermediaries liable for any content published or shared through their services (such as ISPs, cafes offering broadband connections and web-

70. Sedition Act (1948). www.icnl.org/research/library/files/Malaysia/sedition.pdf

71. Malaysia Penal Code, Act 574 §505 (1936). www.agc.gov.my/agcportal/uploads/files/Publications/LOM/EN/Penal%20Code%20%5BAct%20574%5D2.pdf

72. Securities Offences (Special Measures) Act (2012). www.federalgazette.agc.gov.my/outputaktap/20120622_747_BI_Act%20747%20BI.pdf

73. Persatuan Kesedaran Komuniti Selangor (EMPOWER). (2015, 10 April). *Sedition Act Amendments a Betrayal of Democratic Process* [Press release]. docs.google.com/a/hum.uc3m.es/file/d/0B2lgLcnoRb1QUzNsWXMzWWdRdTg/

74. Protection of Pakistan Ordinance (2014). www.na.gov.pk/uploads/documents/1391322775_795.pdf

75. PPO's cyber crime clauses inhibit on online freedom of speech, privacy: Rights group. (2014, April 16). *Express Tribune*. tribune.com.pk/story/696489/ppos-cyber-crime-clauses-inhibit-on-online-freedom-of-speech-privacy-rights-group/

76. Pakistan Penal Code (Act XLV of 1860), §124A, 295, 298 (1860). www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html

77. Investigation for Fair Trial Act (2013). www.scribd.com/doc/232439480/Pakistan-Investigation-for-Fair-Trial-Act-2013

site owners).[78] This means, if an anonymous person posts content deemed offensive using another person's account or services, it will be the latter who will be responsible for the content, unless they can prove otherwise.[79] Critics in both these cases have pointed to the threats on freedom of expression, and by extension, to individuals using the devices and services for online organising and gatherings.

Activists focused on LGBT rights say that restrictions on rights and freedoms in relation to sexual and gender identities are used to further curb their rights to associate and assemble. Activist Thilaga Sulathireh, who also represents the Justice for Sisters campaign in Malaysia for the rights of the *Mak Nyah* community,[80] says the criminalisation of identities has created an adverse impact on the participation of "LGBTQ persons in spaces, including private, public, online, offline spaces with dignity, and freely."[81] She cited the penal code criminalising sodomy (which exists in the codes of almost all of Britain's former colonies, including India, Malaysia and Pakistan) and *sharia* laws that prohibit same sex relationships as the official justification.

Similarly, in 2013, the government of Pakistan shut down the first and only openly gay website, Queer Pakistan, which was started as an online support platform for the LGBT community, on grounds of religious and social values.[82]

Further explorations will be required regarding the practices of FoAA online as some of the rules and procedures that exist for offline assemblies and associations may not be applicable in the digital context. The exception is Section 144 of India's Code of Criminal Procedure, which has been applied for the internet.[83] On the other hand, the growing use of the internet to exercise rights could prompt reforms of the laws that currently govern offline rights to be in line with international standards.

Country contexts for India, Malaysia and Pakistan

Freedoms and governance

Of the three countries studied, India ranks higher in terms of democratic practices and enjoyment of freedoms, compared to Malaysia and Pakistan.

The U.S.-based Freedom House considers India a "free" country, while Malaysia and Pakistan are "partly free".[84] Most indices on

78. Evidence (Amendment) (No. 2) Act (2012). www.federalgazette.agc.gov.my/outputaktap/20120622_A1432_BI_Act%20A1432%20BI-evidence%20(amendment)%20(no.%202).pdf

79. Centre for Independent Journalism (CIJ). (2012). Frequently Asked Questions on Section 114A of the Evidence Act 1950, "Presumption of Fact in Publication" [Press release]. stop114a.files.wordpress.com/2012/08/stop114a-faq-english.pdf

80. *Mak Nyah* refers to the Malay term for the male-to-female trans women in Malaysia. The Justice for Sisters campaign is aimed at raising awareness about the violence and persecution against the *Mak Nyah* community in the country. See their blog at: justiceforsisters.wordpress.com

81. Email interview with LGBT activist, Thilaga Sulathireh, 16 October 2015. Thilaga chose to mention LGBTQ in the example to highlight the information she had obtained from the different communities, but had no data on the experiences on intersex persons. The acronym LGBT is used elsewhere based on the references made in reports or interviews.

82. Nazish, K. (2013, 21 December). Queer Pakistan Under Attack. *The Diplomat.* thediplomat.com/2013/12/queer-pakistan-under-attack

83. The Code of Criminal Procedure, §144 (1973). www.icf.indianrailways.gov.in/uploads/files/CrPC.pdf

84. For profiles, see: Freedom House. (2015). India. freedomhouse.org/country/india; Freedom House. (2016). Malaysia. freedomhouse.org/country/malaysia; Freedom House. (2015). Pakistan. freedomhouse.org/country/pakistan

TABLE 2

Selected indices related to rights, freedoms and governance

Indices/ Countries	Ratification of UN conventions relevant to FoAA online	Freedom on the Net (Freedom House, 2015)	Press Freedom Index (Reporters Without Borders, 2015)	Corruption Perception Index (Transparency International, 2015)	UN Human Development Index (2014)
India	ICCPR (except the Optional Protocols), ICESCR (with declarations), ICERD, CEDAW (with reservations)	Partly free	136	85	130
Malaysia	CEDAW (with reservations)	Partly free	147	50	62
Pakistan	ICCPR (with reservations and not the Optional Protocols), ICESCR (with reservations), CEDAW (with reservations)	Not free	159	126	147

Notes: Freedom House assessed 65 countries for the report on internet freedom for 2015. Countries are classified as either Free, Partly free or Not free.

The Reporters Without Borders press freedom index is a global ranking out of 180 assessed in 2015; the lower the press freedom, the lower the rank. See: freedomhouse.org

Transparency International's tool measures perceived levels of public sector corruption in 168 countries. This index is for 2015. See: www.transparency.org/cpi2015

The UN Human Development Index is a composite index measuring average achievement in three aspects of human development – a long and healthy life, knowledge and decent standard of living. It ranks the countries based on a number of indicators including levels of gender inequality. See: hdr.undp.org/en

democratic indicators like freedom of the press place India among the more established democracies. Freedom House's Freedom in the World report measures the practice of civil and political liberties based on the UDHR, using 24 indicators. Relevant to this discussion are the levels of electoral processes, political pluralism and participation, freedom of expression, associational and organisational rights and rule of law in the country.

In its annual global democracy index, which also measures electoral processes, function of government, political participation, political culture and civil liberties, the Economist Intelligence Unit (EIU) ranked India 27th in 2014. Malaysia was 65th and Pakistan was 108th. The EIU considers India and Malaysia as having "flawed democracies", while Pakistan is a "hybrid" regime that has more irregularities in the political processes and weak rule of law, among others.[85]

International NGO Human Rights Watch, in its annual report on the state of human rights, defenders in the three countries, threats to freedom of association and assembly as well as freedom of expression, and discrimination and repression by state and non-state actors against religious minorities and sexual orientation and gender identity minorities.

Table 2 presents a snapshot of the indices that reflect the levels of human rights and the quality of governance in the three countries.

Of the three countries, Pakistan and India have ratified the ICCPR but not the Optional Protocols, and the ICESCR (with declarations and reservations), while Malaysia has yet to sign on to the instruments. Both Malaysia and Pakistan have not signed on to the ICERD, and while all ratified CEDAW (with reservations), gaps remain in the translation of the rights to national laws and implementation.

Malaysia has been subject to questions and recommendations for review of its laws and practices in relation to FoAA. During the second cycle of the Universal Periodic Review (UPR) at the UNHRC in 2013, at least four countries made recommendations to the Malaysian government to review, amend or repeal legislation seen as restricting FoAA, among them, the Peaceful Assembly Act, Sedition Act, and also a host of laws related to free expression. All of these were merely noted (not opposed or rejected) by the government of Malaysia.

Recommendations were made in the second cycles for India and Pakistan in 2012 on removing restrictions to access and exercise freedom of expression on the internet, in line with international standards. The governments' positions and responses to queries on their obligations as per the human rights conventions reflect their general attitude to reject international scrutiny and recommendations on civil liberties.

85. The EIU uses a scoring system to categorise the countries as either full democracies, flawed democracies, hybrid regimes and authoritarian regimes. The definition of flawed democracies is "countries have free and fair elections and even if there are problems (such as infringements on media freedom), basic civil liberties will be respected. However, there are significant weaknesses in other aspects of democracy, including problems in governance, an underdeveloped political culture and low levels of political participation." In hybrid regimes, "elections have substantial irregularities that often prevent them from being both free and fair. Government pressure on opposition parties and candidates may be common. Serious weaknesses are more prevalent than in flawed democracies - in political culture, functioning of government and political participation. Corruption tends to be widespread and the rule of law is weak. Civil society is weak. Typically, there is harassment of and pressure on journalists, and the judiciary is not independent."
The Economist Intelligence Unit. (2015). *Democracy Index 2014: Democracy and its discontents*. www.sudestada.com.uy/Content/Articles/421a313a-d58f-462e-9b24-2504a37f6b56/Democracy-index-2014.pdf

TABLE 3

Summary of recommendations during the Universal Period Review of India, Malaysia and Pakistan

Country	Summary of recommendations	Government responses
India (2008, 2012)	There were no specific recommendations related to FoAA online, but during the second cycle, a recommendation from Sweden was made to ensure that measures limiting freedom of expression on the internet were based on clearly defined criteria in accordance with international human rights standards. In other related rights, India received, during both cycles, recommendations on improving rights of women and to extend invitations to several special rapporteurs.	The government tended to note the recommendations made, including the one on freedom of expression on the internet. India has not made any comments or recommendations on FoAA online or freedom of expression to other countries under review.
Malaysia (2009, 2013)	Numerous recommendations were made on rights to assembly and association, for example, to review and amend laws such as the Peaceful Assembly Act, to allow full enjoyment of rights. Recommendations were also made to lift restrictions on free speech and expression in relation to peaceful assembly and organisation. During the second cycle, five recommendations were made on improving freedom of expression, of which two touched on the amendment to the Evidence Act that would hold intermediaries of online services liable for crimes.	The Malaysian government noted all the recommendations (from the United States, Czech Republic, Canada, Switzerland, Netherlands, United Kingdom, Australia, Poland, Denmark and Austria) that called for reviews of its laws and to bring them in line with international standards, but accepted the recommendations by Russia and Indonesia that called for Malaysia to continue encouraging the right to peaceful assembly according to national legislation. Malaysia has not made any comments or recommendations on FoAA online or freedom of expression to other countries under review.
Pakistan (2008, 2012)	No recommendations were made with regard to FoAA (online or offline) but Pakistan received a specific recommendation on removing restrictions on accessing the internet in the country, while several countries recommended reviews and amendments of the blasphemy laws, to be in line with principles of freedom of thought, conscience and religion (relevant obligations under the ICCPR). In the first cycle, Canada made a recommendation to decriminalise defamation. General recommendations were made on invitations to special rapporteurs, women's rights (in particular, to address violence against women in all its forms), and the protection of human rights defenders.	The Pakistan government noted the recommendations on freedom of expression, and accepted those in relation to the rights and protection of women, human rights defenders and journalists. Pakistan has not made any comments or recommendations on FoAA online or freedom of expression to other countries under review.

Note: The information was obtained from UPR Info, an organisation that monitors the UPR process and works by raising awareness, providing tools to monitor the process and bridge the different actors. Reporting requirements are contained in Human Rights Council resolution 5/1 on the Universal Period Review. The online resource is available at: www.upr-info.org States cannot reject recommendations and their responses are recorded by the HRC as well as independent monitors. UPR Info explains that recommendations that are clearly stated as "accepted" means the State under Review (SuR) will follow up on them, while responses not committing or rejecting are recorded as "noted". The SuRs can choose to follow up on recommendations they "noted" and report on them at the following cycle. For more information, see: www.upr-info.org/database/files/Database_Methodology_Responses_to_recommendations.pdf

Table 3 shows the recommendations relevant to FoAA made to the respective states during their reporting at the UPR. All three countries have completed two cycles at the time of writing of this report. There were no specific recommendations on FoAA online, but similar or related rights and freedoms were selected based on possible relation with the laws and practices of FoAA online – freedom of expression, rights of women, rights of human rights defenders, freedom of the press, religious freedoms and invitations to special rapporteurs – to gauge the official responses. It should also inform civil society on strategies that can and need to be used for international advocacy.

Access to the internet in India, Malaysia and Pakistan

India, Malaysia and Pakistan have different levels of access to, and affordability of, the internet and mobile technologies. According to the International Telecommunication Union (ITU) estimates, India, with a population of 1.2 billion as of July 2014, has an internet penetration of 18% while Pakistan is lower at 13.8% for a population of 185 million, and Malaysia's internet penetration rate was 67.5% for a population of 30 million.[86]

Disaggregation of these indicators also shows that a majority of those with access in many parts of the world live in or closer to the urban centres and are men. A study by the World Wide Web Foundation in nine cities across nine developing countries (including India) has found that women are 50% less likely than men to access the web in poor urban areas and between 30% and 50% less likely to use the internet to increase their income or participate in public life.[87] Nevertheless, the study notes that the gender disparities are more complex in nature as they are also influenced by the levels of education, age, income, civic engagement and political participation. Notably, the study found that when women do gain access to the internet, the divide narrows among the users in terms of digital empowerment.

86. International Telecommunication Union. (2015). ICT Facts and Figures 2015. www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

For the raw data, see: www.itu.int/en/ITU-D/Statistics/Documents/statistics/2015/Individuals_Internet_2000-2014.xls

87. World Wide Web Foundation. (2015). *Women's Rights Online: Translating Access into Empowerment*. webfoundation.org/wp-content/uploads/2015/10/womens-rights-online_Report.pdf

Section III.

TRENDS OF FOAA IN INDIA, MALAYSIA AND PAKISTAN

Data on access to the internet, mobile telephony and social networking sites show a growing online community across the board, but the growth continues to reflect inequities and disparities that exist in societies. Access to high speed broadband infrastructure is still concentrated in the cities and urban areas, but mobile networks are providing more ICT access in the rural areas, or possibilities for a wider segment of the population to get connected.[88] The internet has provided the platform for a number of large and small scale campaigns and created social movements within Asian societies. This section examines the use of the internet for assembly and association in India, Malaysia and Pakistan, but examples from other countries are also cited where similar trends or issues were noted.

Given the diversity of the users, country contexts and issues, it is difficult to generalise on the kinds of issues that people will rally around online, either in the form of networks or actions. However, a few recurring themes include:

- Political participation
- Promotion and protection of women's rights
- Land rights and the environment
- Rights of gender and sexual minorities
- Expression by religious minorities
- Rights and freedom on the internet
- Access to information
- Defence of human rights
- Media freedom and responsibility.

Three groups of users stand out: civil society organisations, political parties and marginalised communities or groups. The main actors responsible for imposing restrictions, challenges and threats to the exercise of FoAA online are the state and large political parties. Although in the past, the internet was often the space for opposition politicians, activists, CSOs and independent media in countries with strong restrictions on political opponents and the media, the trend has changed and in the last five years, large, dominant and conservative political parties and interest groups have stepped up their presence online, using the platforms for mobilisation. Both ruling and opposition political parties now invest heavily in their social media strategies and hire or engage individuals, known as cybertroopers, to carry out online propaganda against their opponents or critics.[89]

Table 4 lists some of the more common users of FoAA online, and the main sources of threats. These only provide a general picture

88. Haque, J. (2013). *Pakistan's Internet Landscape, A Report by Bytes for All*. Pakistan: Bytes for All. content.bytesforall.pk/sites/default/files/MappingReportFinal%20-%20Published.pdf

89. Thien, V. V. (2012). The Struggle for Digital Freedom of Speech: The Malaysian Sociopolitical Blogosphere's Experience. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. MIT Press. access.opennet.net/wp-content/uploads/2011/12/accesscontested-chapter-03.pdf

TABLE 4

Profiles of FoAA online

Profiles	Actors
Users	• Civil society organisations • Human rights defenders • Political parties and associations from different ideological backgrounds • Women and women human rights defenders • Marginalised or disadvantaged groups such as religious minorities, sexual and gender minorities • Journalists • Student activists and youth
Sources of violations	• State bodies and institutions • Political parties and associations • Religious groups • State-supported NGOs and individuals

of the groups across the countries and do not prioritise or rank them. However, it is important to note that the users may not always be those seeking to strengthen civil and political liberties or those promoting social justice. Many also involve political groups that use online tools to promote discrimination or parochial views, and in some cases, incitement to hatred.

Across India, Malaysia and Pakistan, the examples on the use of the internet to mobilise assemblies, which range from organising online petitions for a cause to sharing information about and organising online and physical protests, outnumber those where the internet is used to form associations. However, fewer examples of associations formed online is not proof of the low incidence levels. Many are overlooked as often they are informal and circumvent the need for official registrations, or are considered acts of expression.

The paper identifies the most common tools and methods of FoAA online – social media, web resources including online petitions and emails, mobile applications and DDoS attacks – which show how the different rights are exercised. Clearly, a more thorough context analysis is needed to study the intersection of rights across platforms and communities. The topics below, which are platform-oriented, are not meant to be technologically deterministic; instead they relate to Bennet and Segerberg's postulation that the forms of communications are essential to the online social networks and movements, and to some extent, Marshall McLuhan's theory of the medium being the message.[90]

90. McLuhan, M., and Fiore, Q. with Agel, J. (1967). *The Medium is the Massage: An Inventory of Effects*. New York: Random House.

Social media

The most common platform cited across the three countries is social media, mainly Facebook and Twitter. Here, pages are created for specific causes and campaign or advocacy hashtags are created to coordinate conversations, raise awareness and generate support.

India has the world's second largest user base for Facebook with about 130 million active users. As early as 2009, the Pink Chaddi campaign in India to counter conservative and right wing activism made use of Facebook to coordinate responses and raise awareness. Despite attacks by internet trolls who hacked the page and set up other fake pages, the Facebook group has about 59,000 supporters. The public in India rallied over Facebook and Twitter to support veteran social activist Anna Hazare in early 2011 on the issue of anti-corruption, getting real time updates and tracking the movement. The movement demanded the enactment of an anti-corruption law (Jan Lokpal Bill) that will give wider powers to the ombudsman.[91]

There are 18 million Facebook subscribers in Malaysia.[92] During the rally on electoral reform in Malaysia on 29 and 30 August 2015, the Bersih organisers' Facebook page peaked at 3.2 million fans.[93] A research firm that analyses social media, Politweet, documented that over the two-day rally, more than 96,000 users tweeted about the rally using the hashtag #Bersih4.[94] Online meetings and gatherings via Twitter are also examples of FoAA online as participants of a group or issue "meet" at designated times to discuss problems and actions on a given topic. The media community and civil society responded to the suspension of a newspaper in Malaysia by holding two protests at its office organised online and conversations continued on Twitter using the hashtag #AtTheEdge.[95]

In the wake of the deadly attacks on the Army Public School in Peshawar in December 2014 and the endorsement given by a radical cleric, an online campaign with the hashtag #ReclaimOurMosques organised by activist Jibran Nasir got hundreds of people gathering in major cities and demanding the arrest of the cleric. Journalist Jahanzaib Haque notes the importance of social media in the context of Pakistan. In his report about the country's internet landscape for Bytes for All, he writes:

> Social media in particular has been leveraged by citizens to raise their voice against curbs on fundamental rights, to disseminate information and build a movement, to attract local and international attention – and resultant pressure – to an issue, and organise protests.[96]

Web resources, online petitions, emails

E-groups have been used since the 1990s to organise interest groups or around themes and causes. Blogs and websites that served

91. Times of India. (2013, 18 December). All you want to know about Lokpal Bill. *Times of India*. timesofindia.indiatimes.com/india/All-you-want-to-know-about-Lokpal-Bill/articleshow/27570010.cms

92. ASEANup. (15 February 2016). Mobile internet and social media in Malaysia. aseanup.com/mobile-internet-social-media-malaysia

93. Email interview with Bersih media and communications officer Izmil Amri Ismail, 15 October 2015.

94. Politweet.org. (2015, 2 September). Twitter statistics and crowd measurement of the Bersih 4 rally. politweet.wordpress.com/2015/09/02/twitter-statistics-and-crowd-measurement-of-the-bersih-4-rally

95. Interview with journalist Hazlan Zakaria, 8 October 2015.

96. Haque, J. (2013). Op. cit. 24

as a resource base were used to raise public awareness and encourage actions like signing a petition or sending letters to the leaders or authorities, using campaign images on personal social media tools and sharing information about meetings and gatherings.

LGBT-India, which started as an e-group and transformed into a Yahoo! Group, still operates and non-governmental organisations in Malaysia promoting freedom and human rights continue to discuss, share information and coordinate responses via a Yahoo! Group that was set up in January 2001.

The Save the Internet campaign for net neutrality was initiated to mobilise the public to send in suggestions on retaining net neutrality to the Telecommunication Regulatory Authority of India.[97] By the last day of submission, a month after the process was started in April 2015, over one million emails had been sent in support of net neutrality. The campaign was reported to be one of the biggest online protests in India, combining the use of a website as a resource page, and Twitter (using the hashtag #savetheinternet), Facebook, a petition, and emails to the authorities as action tools.

The Malaysian campaign to stop the controversial amendments to the Evidence Act used WordPress to collate information, awareness materials and actions that could be taken by individuals and companies.[98] In Pakistan, religious minorities, including different Muslim sects, have used websites and online forums where they raise awareness about threats against them and register protest on different issues. An example is *The Rabwah Times*, which started as a community project in 2006 in the mainly Ahmaddi town of Rabwah, and now operates as an online news website.[99]

Online petitions, such as those hosted by change.org and avaaz.org, are also widely used for numerous issues, and can form a base of a movement. Following the heinous rape of a young woman in New Delhi in December 2012, an online petition on change.org was created and received 65,000 signatures to seek the intervention of the president and chief justice of India. Other petitions were also created, adding to the extensive campaigning over Facebook ("Delhi for Women's Safety", "Gang Raped in Delhi") and Twitter (hashtags #Damini #Nirbhaya #Delhirape #DelhiProtest #RapeFreeIndia), together with street mobilisation.

A government plan to introduce a single gateway for all international internet traffic in Thailand, which was leaked to the public in September 2015, saw thousands of people organise online using petitions and attacks on government websites. In the span of a month, a petition against the plan garnered more than 150,000 signatures and a Facebook page called "Anti-CAT Tower Mob" received 129,420 page likes.[100] The government responded by saying that it was merely considering the plan, but later disclosures showed it was still keen to implement the single gateway.

Mobile applications

Organisers of protests and rallies, including the pro-government ones, rely heavily on chat applications like WhatsApp to plan, coordinate and mobilise their activities. It is easy to invite and add people to conversations and have real time discussions. However, because the authorities can monitor the participants

97. The campaign website acts as a resource tool but also shares action items. See: blog.savetheinternet.in

98. See: stop114a.wordpress.com

99. See: www.rabwah.net

100. See: www.facebook.com/antimobcattower

and their involvement, activists have said they moved important discussions to relatively more secure platforms like Telegram due to security risks. This chat application is available for mobiles and desktops and offers encryption of messages and options to delete conversation history. The organisers at the Bersih secretariat said they used Telegram when details like location, persons in charge or secure strategies were being discussed, even though they were aware of its limitations.[101]

For more sensitive discussions, face to face meetings are considered to be the only safe option available. To counter misinformation, which featured during the earlier electoral reforms rally, the Bersih organisers collaborated with independent news portal, Malaysiakini.com to create Prime, an application that would allow the organisers to send out official and verified information to rally goers. According to the organisers, the application was installed on 30,000 devices in the days leading up to the rally. The election campaign in India in 2014 saw the Bharatiya Janata Party (BJP), now the ruling government, create an app, Mission 272+, referring to the number of seats the party needed to form a majority in parliament, to get voters to register in the party database. BJP's team of volunteers also used WhatsApp to reach out to the wider population to promote the Mission 272+.

DDoS attacks

Distributed denial of service (DDoS) attacks are a form of online protest where protesters attempt to disrupt the availability of an online service by overwhelming it with traffic from different sources. The attacks are often carried out by bots (networks of infected computers) or manually by getting large numbers of people to visit a website and DDoS attacks are seen as a form of protest akin to street protests. The hacktivist community Anonymous is credited for many of the global attacks against governments and corporations by taking down their websites and hacking customer information. In October 2015, it targeted Thailand's telecom operator CAT following disclosures of government plans to install a single internet gateway. Prior to this attack, thousands of Thais had organised a manual attack on several government websites. The group hacked records of customer data and exposed that the government had failed to ensure that personal data were encrypted and secure. Here, the privacy of data was clearly compromised as a result of the attack.[102]

On the other hand, pro-government groups have targeted independent media and individuals, whose private information has been exposed and subject to further risks of attacks. Independent media outlets in Myanmar and Malaysia have come under DDoS attacks for coverage of certain topics, such as the general elections (*Malaysiakini.com* in Malaysia) and the plight of the Rohingya Muslims (*The Irrawaddy* and *Mizzima News* in Myanmar). Both countries have a tightly controlled media environment and restrictions for the public to access independent information critical of the establishment. The source of attacks was not obvious but believed to be pro-government. Clearly the impact was to disrupt public access to information and

101. In its scorecard of secure messaging, the Electronic Frontier Foundation, a non-profit organisation defending civil liberties in the digital world, highlights that Telegram is not the most secure platform but that its private chat feature offers more protections. See: Electronic Frontier Foundation. (2014, 6 November). Secure Messaging Scorecard. www.eff.org/secure-messaging-scorecard

102. For Anonymous statements on the attack, see: Waqas. (2015, 18 October). Anonymous Targets Thai Govt, Leaks Data from State-owned Telecom Firm. *Hackread*. www.hackread.com/anonymous-targets-thai-govt-telecom-firm

to intimidate the media in what is seen as a new form of censorship. In the ongoing border conflict between India and Pakistan, cyber attacks by hackers, sometimes believed to be state sponsored, target the other side's official communication infrastructure.

The trend is for states to react against DDoS attacks as criminal activities when they are the targets. The response of the Thai government that it would invoke provisions of the Computer Crimes Act against those involved is a case in point. But there are few legal remedies available when non-state actors are subject to such attacks. The media, for example, usually step up security of their websites and data if they can afford to, while the absence of data protection laws means personal data is easily exposed.

A mixed bag of benefits and reservations

The cases that saw substantial results that could be due to the overwhelming public support online and offline were in India. The "Save the Internet" campaign led to several online companies pulling out of Internet.org, a zero-rated online service[103] provided by Facebook in the country. In the anti-corruption campaign led by activist Anna Hazare, the Parliament passed a resolution for the Jan Lokpal Bill to set up the ombudsman, but the draft law has not been passed. The anti-rape protest led to the government introducing specific anti-rape provisions in the Code of Criminal Procedure 1973 (Criminal Law (Amendment) Act 2013).[104]

In terms of mobilisation, the experiences emphasise the importance of ICT tools to raise awareness and encourage participation. The rallies for free and fair elections in Malaysia, particularly since Bersih 2.0 in 2011, rely heavily on the spread of information via the internet. Some of the largest rallies created in Malaysia make use of mobilisation tactics such as the use of picbadges on Facebook and Twitter and coordination not just of the organisers but also among small groups of participants.[105]

The lower costs and logistical barriers of the internet have made it possible for a wider spectrum of people to come together on a single issue. In Pakistan, the eviction of people living in Islamabad slums by the Capital Development Authority saw protests organised and announced online with many generating attention on Twitter using the hashtag #StopEvictions. Groups and communities that are marginalised and had few spaces for communication and organising, have been important beneficiaries of the internet. From religious and political minorities to women and LGBT persons, the internet has provided opportunities for safe spaces to come together and engage in discussions, and Mishi Choudhary says the relative anonymity provided by the internet allows people to associate on sensitive matters.

According to Digital Empowerment Foundation (DEF), several websites and cyber campaigns focusing on gender-specific issues have aided in increasing people's sensitivity to issues of violence against women and have garnered massive support and participation

103. Zero-rating involves mobile carriers offering users free access to some websites but charging others, in what critics say is a form of preferential treatment that would violate the principle of net neutrality, mainly benefit large companies, and could negatively impact freedom of expression.

104. Criminal Law (Amendment) Act (2013). indiacode.nic.in/acts-in-pdf/132013.pdf

105. Carmen Leong, P., Nge, C., & Wong, P. (2012). *From PicBadge to Street Protest: Social Media and Youth Activism in Bersih 2.0.* Paper presented at Friedrich Ebert Stiftung Expert Meeting: "From Online Activism to Offline Action: Digital Media and Democratic Space in Asia", Bangkok, 26-28 August.

in India. Some examples of campaigns include *Must Bol* (Youth Collective), *Bell Bajao!* (Breakthrough) and *Stop Acid Attacks* (Saraswati Siksha Samiti).

In the case of the I-Am-You campaign to be a trans ally in Malaysia, activist Thilaga Sulathireh said that the internet:

- Helped increase awareness regarding gender and sexuality.
- Increased engagement offline and online with people of diverse gender identity, sexual orientation and gender expression.
- Acted as a resource centre for people to learn about issues, ask questions, seek assistance, connect and engage.
- Allowed crowd-sourced information and consistent dissemination of information and amplification of messages and news.

It can be generalised that state and corporate responses to public networking and mobilisation online seem to be more encouraging in India, and less so in Pakistan and Malaysia, where public pressure has resulted in more restrictions by the government. This reflects the level of democratic freedoms in the countries, as discussed in Section II.

While not all FoAA online cases saw negative responses or threats to individuals using the spaces, the research shows challenges for specific communities in using the internet, often exposing people and communities to more vulnerabilities. Those who have found the online networking and groups useful also experienced intimidation and harassment online. Among others, LGBT persons, liberal Muslims and human rights activists now find themselves subject to cyber bullying and threats over the same platforms that provided them the spaces to engage and mobilise.

In addition, the research reveals that FoAA online can have a weak translation of online voices into "real world" actions and change, or as some have criticised, online mobilisation can sometimes result in mere "slacktivism". Media rights activist Sadaf Khan notes that the Pakistan experience of using digital media to facilitate offline protests has produced references of "keyboard activists", "drawing room activists" and "*mon batti mafia*" (translated as "candle mafia"). She adds that there is a sense of dependency among those who have access to the internet to be satisfied with making their stand online but there is no will to participate in street protests against the injustices.[106]

Another important consideration that arose from the research is that the platforms selected by many are owned by private companies and are governed by proprietary regulations, which disenfranchises users as they are bound by commercial interests. The dependency on commercial platforms leaves users of FoAA online under their rules on intellectual property, permissible content, data retention and sharing as well as disclosure of their data to state enforcement agencies (as shown by the Google Transparency Report and the Facebook Government Request Reports). Such threats are discussed in more detail in the next section.

106. Email interview with media activist and director of programmes at Media Matters for Democracy, Sadaf Khan, 14 October 2015.

Section IV.

ISSUES: CHALLENGES, VIOLATIONS, PROTECTIONS AND REMEDIES

Challenges and violations

This section highlights the threats against FoAA online, based on the documented cases and reports by non-governmental organisations that monitor digital rights such as APC, Citizen Lab, the Electronic Frontier Foundation, Privacy International, Freedom House, and work done by groups like Tactical Technology Collective in the area of digital security.

Surveillance, censorship and the shutdown of networks are among the threats that have been well documented globally, as these impact on the exercise of rights related to expression, assembly and privacy. Concerns of mass government surveillance drew international attention following revelations by former NSA contractor and whistleblower, Edward Snowden, of the extent of the programmes, which have also targeted journalists and human rights defenders.

The hacking of the surveillance technology company, Hacking Team, revealed the list of state clients of equipment used to intercept communications. According to a technology expert who works in the region and requested anonymity, the exposé essentially demonstrates that many governments have the aspirations to install and operate NSA-level surveillance. Based on his mapping of threats faced by civil society groups in Asia, he believes the states were interested in the technologies because "governments do not want people to organise on any issue."[107]

Surveillance

State surveillance is one of the biggest threats to internet freedoms, including freedom of association and assembly. According to Bytes for All, while communities and individuals in Pakistan enjoy the right of online freedom of assembly and association, they are constantly being monitored. Under the guise of national interest and security, the Pakistani government exercises its power to ban or accuse or arrest the individuals or groups.

This concern is based on the findings by Toronto-based Citizen Lab, together with Bytes for All, which released a report in 2013 documenting the presence of FinFisher, a commercial network intrusion malware developed by a UK company, on the Pakistan Telecommunication Company Limited (PTCL) network. Citizen Lab's research has found 36 active command and control servers "used for surveillance beyond suspected criminal activities" and targets in

107. Interview with expert, who chose to remain anonymous, 4 October 2015.

some countries have included human rights organisations.[108]

The malware was also detected in Malaysia during the 2013 elections targeting Malay-language speakers, though it is not clear who purchased or used it.

Yasser Hamdani, a Lahore High Court lawyer, is of the opinion that both the Pakistani government and other foreign states mine data from the country, and that the government is "definitely interested in keeping tabs on activists from across the political and social spectrum." He adds that laws like the Investigation of Fair Trial Act 2013, Protection of Pakistan Act 2014 and the 21st Constitutional Amendment have empowered the spy and law enforcement agencies to collect data on individuals, with the possibility of prosecuting elements involved with terrorism-related activities.[109]

Mishi Choudhary says the existence of legal provisions that empower the government to intercept communications makes the threat of surveillance a significant one in India. This is supported by research showing the extent of India's surveillance technology industry and concerns that it could be as intrusive as the controversial PRISM programme in the United States.[110]

Censorship, filtering and network shutdown

Public mobilisation using the internet and mobile communication have come under attack through government orders to operators to shut down networks, dubbed the kill switch, in Pakistan and India. The kill switch refers to the complete shutdown of cellular and mobile services and internet traffic. Governments use it as a measure to counter cyber attacks and enforce it through network operators, but critics say the measure is subject to abuse and threatens fundamental rights.

In Pakistan, the kill switch was first used during the violence in the province of Baluchistan in 2005, and it has since been imposed during major events or festivals like Ashura.[111] Bytes for All monitors the use of the kill switch in Pakistan on www.killswitch.pk. The kill switch usually happens across all major cities like Islamabad, Rawalpindi, Lahore, Peshawar, Quetta and Karachi though at times the shutdown is localised. The reasons cited have primarily been to prevent terrorist groups from using the technology to organise attacks.

A report by the Institute for Human Rights and Business on shutdowns implemented by international telecommunications company Telenor recorded 23 such incidents in Pakistan since 2012. The report said that over time, the scope of the shutdowns has broadened to include internet access via wireless networks. The report concluded that the kill switch was neither necessary nor proportionate to the

108. Marquis-Boire, M., Marczak, B., Guarnieri, C., Scott-Railton, J., Citizen Lab., Canada Centre for Global Security Studies., & Munk School of Global Affairs. (2013). *For their eyes only: The commercialization of digital spying*. Toronto: Citizen Lab. citizenlab.org/2013/04/for-their-eyes-only-2

109. Email interview with Lahore High Court lawyer Yasser Hamdani, 10 October 2015.

110. Xynou, M. (2014, 10 February). Big democracy, big surveillance: India's surveillance state. *Open Democracy*. www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance-state

111. Ashura is a Muslim festival that falls on the 10th day of the Muharram and is observed by the Shia and Sunni practitioners. But for the Shia Muslims, Ashura is also celebrated to commemorate the assassination of Imam Husayn, a Shia leader, and the grandson of Prophet Mohammad. Shia followers, who make up about 20 percent of the Sunni-dominated population in Pakistan, have been targeted for violent attacks during the celebrations.

problem at hand and that it had more risks of violating fundamental human rights.[112]

In India, the governments of the states of Jammu, Kashmir, Gujarat, Nagaland and Manipur imposed bans on mobile internet services over different periods, largely due to public protests and threats of violence. According to DEF, in addition to access, some governments also blocked networking sites like Facebook, Twitter and WhatsApp on some of the service providers. Shut downs continue to happen in Pakistan and India despite major UN and international human rights experts declaring that kill switches are impermissible under human rights law, even in times of conflict.[113]

Jahanzaib Haque writes that there is pressure on the 50 ISPs operating in Pakistan to act as intermediaries and to comply with requests to filter and block websites based on orders of the Pakistan Telecommunications Authority (PTA), an example of which is the blocking of the *Baloch Hal* website that hosts content focused on the Baluchistan crisis.[114]

Similarly, in Malaysia, ISPs are subject to takedown and blocking orders issued by the regulatory body, the Malaysian Communications and Multimedia Commission (MCMC). The electoral reform group, Bersih, had its website blocked days ahead of the major rally in August 2015. MCMC was quoted by the media as saying that the move under Sections 211 and 233(1) of the Communications and Multimedia Act was necessary to block information deemed threatening to national security. Bersih organisers however said that most of the rally participants relied on their Facebook page and Twitter accounts, so the impact of the blockade was minimal.

Google has reported in its transparency report that they received five requests from the Indian Computer Emergency Response Team during the second half of 2012 to remove content from Google+, blogs, and YouTube. For YouTube, the requests were about videos and comments on the disturbance in the northeast region. The company responded by removing one of the videos and restricting the others from local view.

For the period between 2009 and 2015, Google received 1,517 requests for take down from various agencies and courts in India, 31 from Malaysia and 18 from Pakistan. The reasons commonly cited were adult content, defamation, government criticism, privacy and security, impersonation, national security, hate speech, copyright, violence, religious offence, obscenity/nudity, geographical dispute, trademark, bullying/harassment, suicide promotion, electoral law and drug abuse.[115] The motivations for the requests have not been analysed as detailed information is not available for each request. But the take down of websites could have the net effect of denying the public its right to access information about issues and events, given that India, Ma-

112. Institute for Human Rights and Business. (2015). *Security v Access: The Impact of Mobile Network Shutdowns. Case Study: Telenor Pakistan*. London, United Kingdom: IHRB. content.bytesforall.pk/sites/default/files/2015-09-Telenor-Pakistan-Case-Study.pdf

113. Article 19. (2015, 4 May). Joint Declaration on Freedom of Expression and Responses to Conflict Situation. www.article19.org/resources.php/resource/37951/en/joint-declaration-on-freedom-of-expression-and-responses-to-conflict-situation

114. Haque, J. (2013). Op. cit.

115. Google Transparency Report. www.google.com/transparencyreport

The bulk of the requests in Pakistan were related to the YouTube video of the "Innocence of Muslims" in 2012. Following this, the government banned access to the website, hence the zero requests to Google in the subsequent periods. The ban was only lifted in January 2016.

laysia and Pakistan have all been criticised for not applying international standards in imposing restrictions to civil liberties.

Cyber bullying, stalking and gender-based violence online

"Space should be seen as a continuum, and spaces are also connected," says LGBT activist Thilaga Sulathireh, who aptly describes the day-to-day and organised threats faced by marginalised individuals and groups online. "Often, an experience in offline space could also continue in online spaces, and vice versa."[116]

In other words, the physical violence and threats experienced for expressing one's identity are replicated and intensified online given the speed and reach of the internet. The ability to exist and interact online anonymously can be a double-edged sword. On the one hand, it can offer protection to those engaging in sensitive or controversial issues. However, it can also protect abusers hiding behind anonymity. A study on the violence experienced by LGBT persons included cyber bullying as one of the threats.[117] Malaysian lawyer Syahredzan Johan says the internet has made it easier for individuals to be tracked down and attacked for the stands which they take, especially in relation to religion and specifically Islam. He said individuals who associate themselves with groups which are seen to be "liberal" have been attacked online.[118]

Cases from the three countries also highlight incidents of cyber bullying and threats of violence against women netizens, gender and sexual minorities and those perceived to be supporting liberal Muslim ideas. Some of the incidents shared by APC partners and other respondents include:

- Bersih chairperson, Maria Chin Abdullah received sexist remarks and threats of violence over Facebook and mobile chat apps ahead of and during the two-day mass rally in August 2015 in Malaysia. Several women volunteers also said they were subject to harassment on their Facebook accounts.[119]
- The case in Lahore in 2014, where a man made contact with gay men online through their digital communities, met them, and murdered them after having sex. When arrested, he said that he wanted to teach them a lesson for being homosexual.[120]
- Hate speech, harassment and incitement by trolls from political parties such as the Pakistan Tehreek e Insaaf (PTI) party, whose followers openly "wish" or "pray" for supporters of other parties to be killed, maimed, raped or worse. Those criticising PTI online also face coordinated attacks.[121]Azwan Ismail, a gay man in Malaysia, received death threats after sharing a video on YouTube entitled "Saya gay, saya okay" ("I'm gay, I'm okay") in conjunction with the North American "It Gets Better" campaign.

116. Email interview with LGBT activist Thilaga Sulathireh, 16 October 2015.

117. International Gay and Lesbian Human Rights Commission. (2014). *VIOLENCE: Through the Lens of Lesbians, Bisexual Women and Trans People in Asia* (Rep.). New York: IGLHRC. www.outrightinternational.org/content/violence-through-lens-lbt-people-asia

118. Email interview with Malaysian lawyer Syahredzan Johan, 30 September 2015.

119. Interview with Bersih advocacy and education officer Zoe Randhawa, 22 September 2015.

120. Email interview with media activist and director of programmes at Media Matters for Democracy Sadaf Khan, 14 October 2015.

121. Ibid.

> The video was hosted locally by organisers of a festival called *Seksualiti Merdeka* (loosely translated as Sexuality Independence) and went viral within five days. Ismail was accused by the religious authorities of insulting Islam and the minister in charge of Islamic affairs called for the authorities to monitor the activities of "gay groups" and take action where necessary, as these were seen as hurting the image of Islam.[122]

Hacking – DDoS attacks

Hacking can serve as a form of public protest, but at the same time it has the potential to cause harm against rights such as freedom of expression, access to information and rights to privacy. An example of disruption occurred during the World Conference on Information Technology (WCIT) in November 2012 where the International Telecommunication Regulations (ITRs) were being negotiated. Hackers attacked the conference website, which then made it difficult for those attending the event, including civil society, to follow deliberations and work towards a better outcome.[123]

When the hacktivist community Anonymous targeted Thailand's telecom operator in October 2015 following disclosures of government plans to install a single internet gateway, the attack targeted the government but also partly revealed customer identification and details. Activists are divided over whether to endorse cyber attacks as a form of protest even when the collective action is targeted at unjust or undemocratic actions. This form of protest would require further research as it involves rights to FoAA online and free speech but at the same time, potentially causes harm to individual privacy and access to information.

In discussing this contentious action, Comninos suggests that "while DDoS should not be criminalised as a form of protest, it may need to be balanced against other rights in assessing the effects of such protests."[124]

Privacy violations and private sector control

Privacy breaches occur at various points of threats. For example, hacking has the potential to reveal personal data, unchecked surveillance by states and corporations can expose individuals to profiling and threats of criminal prosecution, and cyber bullying and surveillance by family members or the public can lead to violence against women and minorities online and offline. On state surveillance, US and UK security agencies have been criticised for weakening encryption of online communication such as emails and social media, which could undermine public safety.[125] Controversial US. surveillance programmes have been found to have compromised the safety of human rights defenders in other countries.[126]

The exercise of FoAA online is dependent to a large extent on platforms owned and managed by the private sector. From the tools to

122. Email interview with LGBT activist Thilaga Sulathireh, 16 October 2015.

123. Kerner, S. M. (2012, 6 December). WCIT ITU Conf Site Disrupted – Hackers Claim Responsibility. *InternetNews.com*. www.internetnews.com/blog/skerner/wcit-itu-conf-site-disrupted-hackers-claim-responsibility.html

124. Comninos, A. (2012). Op. cit.

125. Arthur, C. (2013, 16 September). Academics criticise NSA and GCHQ for weakening online encryption. *The Guardian*. www.theguardian.com/technology/2013/sep/16/nsa-gchq-undermine-internet-security

126. Privacy International. (2015, 14 September). Human Rights Watch legal challenge to NSA/GCHQ intelligence sharing. www.privacyinternational.org/node/651

the infrastructure, users are subject to the conditions and practices of corporate entities, and the handing over of personal data to government agencies and the decisions on censorship implemented by the companies remain contentious. A project to monitor corporate disclosure of policies and practices that affect users' freedom of expression and privacy, Ranking Digital Rights, has found that many large internet and telecommunications companies fail to disclose key information about practices affecting users' rights.[127]

Cyber stalking or gender-based violence complaints submitted to companies like Twitter and Facebook are considered based on internal or community guidelines, which have shown lapses in terms of adhering to human rights standards. On data, although full disk encryption is being offered by some device operating systems, others like Android went back on earlier decisions to offer disk encryption for mobile devices, which could affect individuals who cannot afford costlier options like Apple phones.[128]

Misinformation

The danger associated with misinformation or attempts at disruptions that come with large-scale and public mobilisation using the internet continue to be problematic. Some of these are attributed to state-supported cybertroopers, openly admitted by states like Malaysia, Thailand, Vietnam and China.

Organisers and participants of Malaysia's Bersih 4 rally have encountered false or misleading information spread by fake Facebook pages, Twitter accounts and WhatsApp messages, causing confusion. The Bersih organisers said they spent too much time verifying information shared on social media, and also dealing with the Bersih counter-narratives. "They used the Bersih hashtags but they were basically anti-Bersih," said a member of Bersih staff.[129]

Misogynist attacks against APC's Take Back the Tech Twitter campaign are also an example of counter-narratives hijacking a cause that essentially promoted free expression. According to the organisers of that campaign, the scale of the attack "involved more than 20,000 tweets and memes containing anti-feminist, racist, violent and abusive content, which has also been targeted at those who expressed support for the #TakeBacktheTech campaign."[130]

Protections and remedies

International experts and human rights advocates have called for rights afforded offline to be promoted and protected online, and resolutions at the UNHRC and the UNGA recognise this. However, the legal frameworks on civil liberties offline are currently below standards in some countries. These have been called into question at the UPR where Pakistan and Malaysia received a series of suggestions to review, amend and repeal laws or provisions related to FoAA, freedom of expression and the internet. It will not be adequate to extend the protections online without also ensuring that the fundamentals

127. Kumar, P. (2016, 1 March). Ranking Digital Rights: Improving Corporate Transparency Reporting. rankingdigitalrights.org/2016/03/01/improving-corporate-transparency-reporting

128. Simonite, T. (2015, 3 November). Why Google Trailing Apple on Encryption Support is a Human Rights Issue. *MIT Technology Review*. www.technologyreview.com/news/543161/why-google-trailing-apple-on-encryption-support-is-a-human-rights-issue

129. Interview with Bersih advocacy and education officer Zoe Randhawa, 22 September 2015.

130. Association for Progressive Communications. (2015, October). Facts on #TakeBacktheTech www.apc.org/en/pubs/facts-takebackthetech

of those protections offline are strengthened across the board.

Few groups or individuals have sought for remedies for threats or violations of FoAA online in the three countries. However, the examples that are mainly related to FoAA in general and online freedom of expression could be used as potential strategies to fight against violations of FoAA online.

Legal recourse

Despite challenges, civil society and individuals have used legal instruments where possible to seek justice, or, at a minimum, to raise public awareness. Strategic litigation is seen as an important method of pressuring courts and governments to review standards.

When the Toronto-based Citizen Lab, together with Bytes for All, released a report in 2013 documenting the presence of FinFisher, a commercial network intrusion malware developed by a UK company, on the Pakistan Telecommunication Company Limited (PTCL) network, the two organisations involved in the research filed a public interest litigation case in the Lahore High Court, and in the process drew public attention to the issue. In the United Kingdom, Privacy International led a litigation effort against the government's surveillance programme, and saw the courts declare that the UK had illegally spied on human rights groups and that all intelligence shared with the US National Security Agency (NSA) before December 2014 was unlawful. In both cases, Bytes for All was a petitioner.[131]

The Supreme Court in India struck down Section 66(A) of the Information Technology Act, 2000 following a constitutional challenge, and invalidated the provision as violating guarantees to freedom of expression. This section provided for the punishment of any person who sent through a computer resource or communication device any information that is grossly offensive, or with the knowledge of its falsity, where the information was transmitted for the purpose of causing annoyance, inconvenience, danger, insult, injury, hatred, or ill will. The challenge stemmed from the arrests of two women for posting allegedly offensive and objectionable comments about whether it was proper to shut down the city of Mumbai after the death of a political leader. In the judgement, the Supreme Court judge made reference to the market place of ideas and the importance of free speech and assembly for political discussions.[132]

Human rights lawyer Fadiah Nadwa Fikri says that legal options can be beneficial even though they can be tedious. In Malaysia, legal challenges or even seeking legal solutions is seen as ineffective given the double standards by the enforcement agencies.

"Filing police reports in the case of harassment and intimidation, or challenging the constitutionality of certain laws can help raise public awareness of the injustices," says Fadiah Nadwa Fikri. "Through the process, even if we know there will be no action, we are able to explain to the public how the laws do not protect our rights to FoAA."[133]

In India, the case of the trolling experienced by a woman television journalist in Delhi who lodged a police report for stalking, defama-

131. Bytes for All. (2015, 6 February). GCHQ-NSA Intelligence Sharing Unlawful, says UK Surveillance Tribunal [Press release]. content.bytesforall.pk/node/160

132. The full judgment of the Supreme Court in the case: *Singhal v. Union of India*, (2013) 12 S.C.C. 73 can be read here: supremecourtofindia.nic.in/FileServer/2015-03-24_1427183283.pdf

133. Interview with human rights lawyer Fadiah Nadwa Fikri, 8 October 2015.

tion and outraging the modesty of women showed that existing laws in the penal code could offer legal remedies. The relevant provisions are Section 507 that deals with criminal intimidation by anonymous communication, Section 499 on using words, signs, visible representations, making or publishing any imputation concerning any person intending to harm, Section 509 which outlines words, gestures or acts intended to insult the modesty of a woman, and Sections 354A and 354D which deal with sexual harassment and stalking, including harassment via electronic communication.

Similarly in Pakistan, a research paper on technology-based violence against women, published by Bytes for All in 2014, noted that in the absence of internet laws, other legal provisions in the Penal Code and the Electronic Transaction Ordinance (ETO) could be used in some of the cases, bearing in mind that similar provisions in the ETO are used to also restrict liberties and freedoms.[134]

In a report on how women deal with sexist and abusive comments online, Richa Kaul Padte of the India-based Internet Democracy Project concluded that users who face some form of trolling and cyber stalking adopt different strategies but rarely take a legal approach.[135] Similar findings were made in a seven-country research project by APC released in March 2015.[136] In some of the cases, civil society groups have documented the violations or threats for possible investigations by the authorities but the experiences of harassment among marginalised communities by enforcement bodies means that following the legal path can expose victims to further abuse. More people choose to retain a low profile, removing themselves from online discussions or disabling their social media accounts.

The research papers by Bytes for All and Internet Democracy Project cited above, on how women in India and Pakistan have responded to online attacks, are good resources on which to build further documentation on options and strategies available.

Digital security practices

Exposure to some threats, such as surveillance and hacking, can be minimised through better digital security practices. Organisations focused on this have worked with groups in the region to provide assistance and support to enhance digital and information security, given the low state of awareness or priority assigned to online security.

According to a technology expert who has worked with CSOs in Southeast Asia, there is little in terms of awareness, capacity and resources among human rights defenders and civil society organisations to establish information security practices. They often become frustrated with the tools or are not given enough support and training for changes in behaviour to take hold. Others think since their work is above ground and widely publicised, the government would have already

134. Bytes for All. (2014). *Access to Justice for Technology driven violence against women: Case Studies 2014*. content.bytesforall.pk/sites/default/files/CaseStudies-TechnologyDrivenViolence-AgainstWomen.pdf

135. Padte, R. K. (2013, 29 June). *Internet Democracy Project: Keeping women safe? Gender, online harassment and Indian law*. internetdemocracy.in/issues/freedom-of-expression/gender-and-censorship/

136. Association for Progressive Communications. (2015, 2 March). GenderIT.org: From impunity to justice: Exploring corporate and legal remedies for technology-related violence against women. www.genderit.org/node/4258

collected information about them. Only a handful have taken the cases to the companies that are the intermediaries or suppliers of spying tools.[137]

International advocacy

There are opportunities for recourse for human rights violations at the global level but as the APC briefing paper on FoAA online noted, these are underutilised by individuals and civil society. Most respondents did not identify the international mechanisms as top priority remedies, although the APC partner organisations have submitted cases of violations of FoAA and online expression to the UNHRC through complaints to the special rapporteurs and civil society submissions for the UPR.

137. Interview with expert, who chose to remain anonymous, 4 October 2015.

Section V.

RECOMMENDATIONS

The recommendations are based on trends of FoAA online as well as the threats and challenges documented. A number of the recommendations are drawn from the work of organisations cited in this research, which have developed principles and tools to defend digital rights. The recommendations are clustered into seven stakeholder categories – governments and legislatures, judiciary, national human rights institutions, civil society, the private sector, technologists and international human rights mechanisms.

Governments and legislatures

- State bodies should engage and consult with civil society and human rights experts to review existing laws governing the internet as well as FoAA to bring them up to international standards.
- Governments should voluntarily follow up on recommendations made at the UPR on improvements to human rights practices by repealing repressive laws or amending provisions that adversely affect the exercise of FoAA online.
- Governments and enforcement agencies should fulfil their positive obligations in human rights by ensuring protection for those made vulnerable by online threats. In relation to this, governments must immediately end the persecution and selective prosecution of activists and critics who have used the internet to express their rights and mobilised protests.
- State actions related to surveillance, internet blocking or network shut downs need to be in line with permissible limitations under international human rights law. The practices are currently arbitrary, indiscriminate and happen under limited judicial oversight. In this regard, states should reform their surveillance practices so they comply with the International Principles on the Application of Human Rights to Communications Surveillance,[138] which have widespread support from civil society groups worldwide.
- Governments should ensure the availability and affordability of internet infrastructure to all so that everyone will have access to the tools to exercise their rights to FoAA online and other rights (freedom of expression, participation in public affairs, education, etc.).

Judiciary

- The judiciary should uphold international human rights standards in cases involving the exercise of FoAA online and offline, including by refraining from providing orders permitting disconnection of communication services.

138. en.necessaryandproportionate.org

National human rights institutions

- National human rights institutions should include violations of human rights online within their purview and in particular address violations of FoAA online, as it falls within their mandate.

Civil society

- Civil society organisations (CSOs) should review their social media strategies (or outreach and communications) that rely heavily on third party platforms, as more and more concerns are raised over issues of privacy, corporate moderation of content that is in violation of human rights, and surveillance. At a minimum they should adopt and encourage partners and participants to opt for secure communications. CSOs should enhance their digital security practices and skills based on an assessment of risks and needs for organisations and individuals. Some references for digital security strategies include APC's Digital Security Kit for human rights defenders[139] and the tools and tactics for digital security developed by Tactical Tech Collective and Front Line Defenders called Security in-a-box.[140]
- CSOs should conduct more public awareness campaigns on the importance of digital access and security.
- CSOs should build alliances for advocacy targeting legislators to review laws to strengthen protections for FoAA online.
- CSOs should review the outcome of international advocacy efforts as remedies and where the potential for change exists. Priority should be given to capacity building and exposure for local groups and individuals to present their cases relating to violations of FoAA online.

Private sector

- The private sector should raise compliance of human rights standards in business practices where these could impact on the exercise of FoAA, freedom of expression and privacy online. This should be based on internationally accepted best practices, namely the UN Guiding Principles on Business and Human Rights.[141] The three core principles are that: 1. States have a duty to protect against violations by third parties, including businesses; 2. Corporate responsibility to respect human rights; and 3. Greater access for victims to judicial and non-judicial remedies and protections.
- ICT companies that have participated in the Global Network Initiative, such as Facebook, Google, Microsoft and Yahoo, should honour their commitments towards upholding principles of freedom of expression and privacy, jointly developed and agreed upon by companies, investors, CSOs and academics.[142]

139. Association for Progressive Communications. (2014). Digital Security First Aid Kit for Human Rights Defenders (Second edition). www.apc.org/en/irhr/digital-security-first-aid-kit

140. Front Line Defenders and Tactical Technology Collective. (2016). Security in-a-box: Tools and tactics for digital security. securityinabox.org/en

141. Business and Human Rights Resource Centre. (n.d.). UN Guiding Principles on Business and Human Rights. business-humanrights.org/en/un-guiding-principles

142. Global Network Initiative. (n.d.). Principles on Freedom of Expression and Privacy. globalnetworkinitiative.org/principles/index.php

- Specific measures should be taken by ICT companies to introduce and implement gender-sensitive and rights-based responses to gender-based violence online.
- Intermediaries and internet companies in the developed North should improve their engagement and communication with CSOs, particularly outside of the United States, where human rights defenders are under threat for using the internet for their work.

Technologists

- Technology experts and practitioners should work together with NGOs to develop secure platforms. Mobile applications are being developed for human rights defenders and journalists, who are among those at risk of state surveillance and attacks, which can be customised for activists and general users alike. Examples include *Muhafiz,* which will be available to journalists in Pakistan, and *Salama*, which has been tested in Mexico.

International human rights mechanisms

- Relevant international human rights mechanisms, such as the Human Rights Council and the UN special rapporteurs, should reaffirm and sustain focus on FoAA online, including by condemning violations where they occur and by highlighting the issue in their thematic reports and joint statements.

CONCLUSION

This paper set out to identify the legal framework and trends of FoAA online in three countries – India, Malaysia and Pakistan. So far, the UNGA and UNHRC resolutions calling for protection of offline rights to be applied online for the full enjoyment of rights have yet to be translated into national standards and practices.

The laws on peaceful assembly and on the internet are more restrictive and fall short in creating an enabling environment for the practice of FoAA online. This regional paper shows that the legal framework of FoAA online in the countries under study does not vary much, although there are obvious differences in how the judicial and political institutions respond to digital activism.

In this context and despite the differences in access to the internet, in which only some people or groups are using the technology for FoAA, people are gathering and mobilising online over a variety of issues, using different tools and sometimes in combination with offline actions. Civil society groups and individuals who previously had limited access to offline platforms to mobilise have benefited from the relative ease and anonymity of the internet. The results are mixed, as some online actions have seen real results (as shown in the Indian examples with responses from the government) and others have at least been able to push the issues to the public domain and draw wider support.

Not all experiences have been positive, as the internet has also made it possible for non-democratic forces to occupy the spaces at the same time. In some cases, this occurred with the deliberate aim of disrupting online social movements or targeting individuals for their identities and beliefs. Political parties and

religious groups are among the major users of the internet to mobilise supporters and in the process they have dominated the online public sphere where offline threats have been replicated and intensified.

Across the three countries, common threats have included:

- Surveillance
- Censorship, filtering and network shut down
- Cyber bullying, stalking and gender-based violence
- Hacking
- Privacy violation and corporate control
- Misinformation

Most examples shared or made available publicly show how citizens of a country have used the internet to exercise their rights. Yet most societies host a multitude of people, among them non-citizens, such as migrants and refugees who also rely on networks offline and online for their support. Internet shut downs or content regulations affect the ability of communities of non-citizens to access information and communicate across borders. As the definition of FoAA applies to all persons, it would also be useful and necessary to include their experiences in using the internet for FoAA.

Few seek legal remedies internationally or nationally, even though there were important court challenges on surveillance, content regulation online and the rights to peaceful assembly. Individuals facing harassment or intimidation chose to either confront the abusers or withdraw from public spaces. Seeking remedies is especially challenging for those with few resources or little access to legal support, particularly internet users among migrants and refugees who live in constant fear of deportation and would rather not seek legal remedies if they are victims of online threats.

The experiences of organisations with local and international advocacy vary across the countries and are particularly relevant to the APC-IMPACT project if stakeholders want to use the mechanisms to improve human rights practices.

It was not possible through this research to accurately state how different groups were affected by the threats and laws imposed on users online or offline. Nevertheless, the examples provide initial insights of how some individuals (women activists, LGBT persons and religious minorities) were specifically targeted for their identities and beliefs.

It is hoped that the research can be a useful tool to initiate conversations to clarify how the internet facilitates the exercise of the different rights. Future research could also benefit from a more detailed analysis of the relationship between online and offline actions, the impact of using the internet for FoAA, and how laws are used to promote or restrict these rights in the respective countries.

Internet and ICTs for social justice and development

APC is an international network of civil society organisations founded in1990 dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technologies (ICTs).

We work to build a world in which all people have easy, equal and affordable access to the creative potential of ICTs to improve their lives and create more democratic and egalitarian societies.

www.apc.org info@apc.org

Written by Gayathry Venkiteswaran

Commissioned by the Association for Progressive Communications (APC)

SUPPORTED BY THE EUROPEAN UNION UNDER THE INSTRUMENT FOR DEMOCRACY AND HUMAN RIGHTS (EIDHR)

Freedom of assembly and association online in India, Malaysia and Pakistan: Trends, challenges and recommendations

March 2016

ISBN 978-92-95102-59-0 APC-201603-CIPP-R-EN-DIGITAL-250