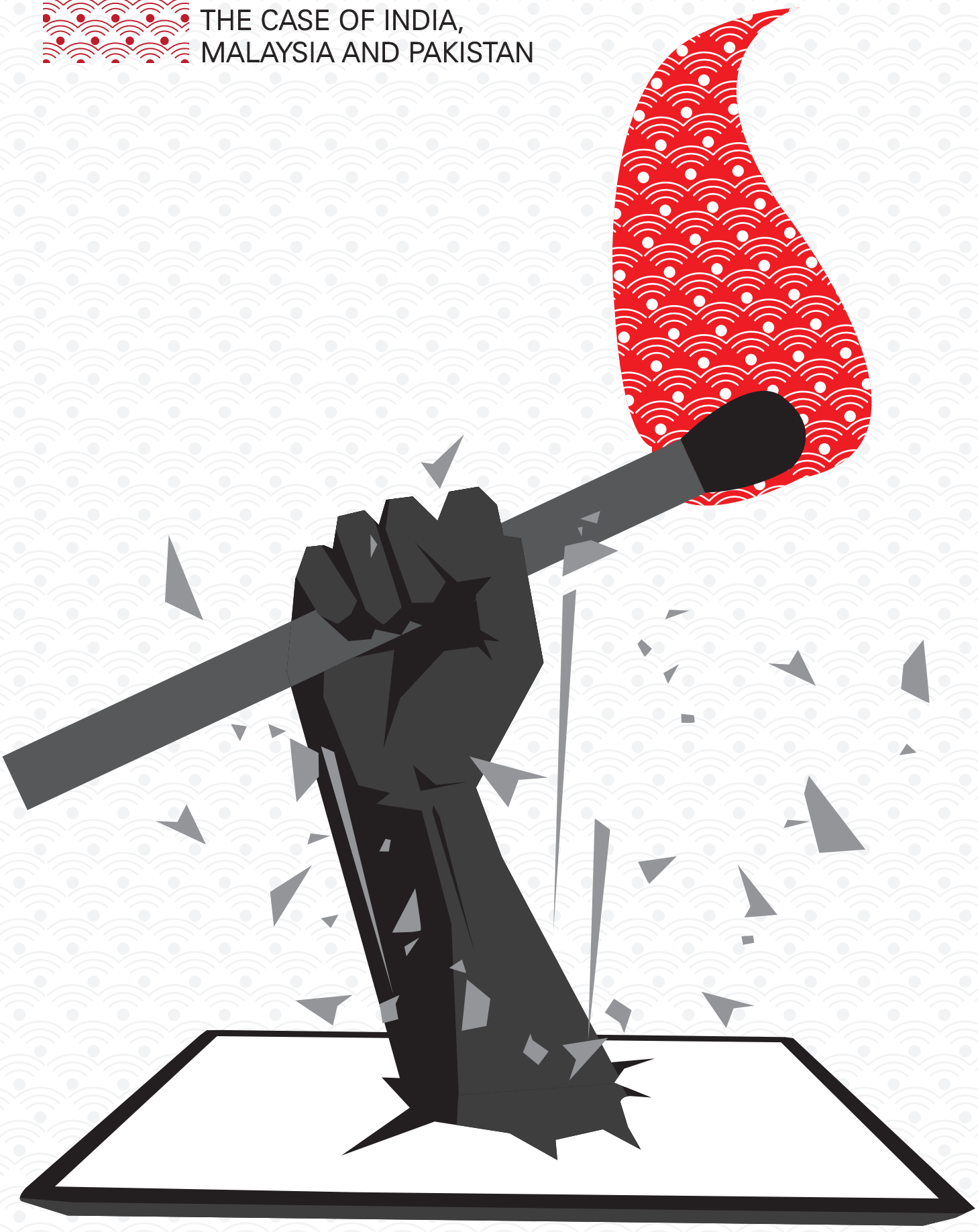
STATE OF THE INTERNET IN ASIA:
THE CASE OF INDIA, MALAYSIA AND PAKISTAN



ACKNOWLEDGEMENTS

This report would not have been possible without the information on laws, other research documents and data from monitoring of rights violations from APC partner organisations, in particular, Bytes for All Pakistan, the Digital Empowerment Foundation (DEF) and Persatuan Kesedaran Komuniti Selangor (EMPOWER); and APC. We thank the authors of the country chapters Geetha Hariharan (India), Umer Ali and Haris Bin Munawar (Pakistan), Yasmin Masidi (Malaysia) and Faheem Zafar who coordinated the research and compiled the regional summary.

We also wish to thank Ritu Srivastava (DEF), Tehmina Zafar (Bytes for All), Haroon Baloch (Bytes for All), Serene Lim (EMPOWER) and Gayatri Khandhadai (APC) who supported the research and publication. Special thanks to Fingerprints Creative (India) and Saakshita Prabakar for making this publication possible.

CONTENTS

CHAPTER 1

IMPACT: PROJECT SUMMARY REPORT

APC-IMPACT: PROJECT
SUMMARY 2014-2017

The APC-IMPACT (Advocacy for Change through Technology in India, Pakistan and Malaysia) programme consisted of four thematic areas and the project was based in three countries. The project was executed by the Association for Progressive Communications (APC) with local partners in India, Pakistan and Malaysia. In Pakistan, Bytes for All, Pakistan executed the project, in India it was Digital Empowerment Foundation (DEF), and in Malaysia, Persatuan Kesedaran Komuniti Selangor (EMPOWER).[1] Under the first thematic area of research and monitoring, partner organisations studied the state of online-freedom of expression and association, patterns of hate speech, digital security and violations of internet rights. A second component consisted of capacity building, which required contextualisation of digital tools and curriculum related to internet-rights and enabling human rights defenders to strategise their digital security through training and awareness raising exercises. The third component underscored strengthening institutions through organisation of regional workshops with national stakeholders, particularly civil society activists and groups from India, Pakistan and Malaysia. Lastly, networking and advocacy, required engagement in regional and international platforms for promotion of internet rights, domestic advocacy for freedom of expression, association and assembly right to information online, and participation in country consultation for the Universal Periodic Review (UPR) process.[2] The following subsections of the report look at the summary of the project activities and the outcomes achieved in India, Malaysia and Pakistan.

- **APC-IMPACT in India:**

Keeping in line with the objectives of the project, DEF submitted its UPR contribution for India's Third UPR cycle, 2017, to the United Nations Human Rights Council (UNHRC). [3]The UPR was authored in association with partner organisations, including APC. The UPR highlighted the restrictions imposed by the Government of India (GoI) on Freedom of Expression (FoE) and speech, consequences of the state-led crackdown on the internet.[4] These included censorship of the URL/websites and network shutdowns and arrests of citizens for engaging in online activities to form associations; including social media platforms such as Twitter, Facebook and digital communication apps such as WhatsApp. The report highlighted lack of adherence to transparency and compliance with national policies, domestic laws and international standards to blocking and censorship.[5] The report also cited proposed laws that could extend more powers to the state, especially intelligence agencies for surveillance with few or absence of any checks. Such proposed

1 www.apc.org/en/project/advocacy-change-through-technology-india-malaysia-and-pakistan
2 Ibid.
3 www.internetrights.in/wp-content/uploads/2017/03/Coalition-UPR-Report-2017_India_Full-Report.pdf
4 Ibid.
5 Ibid.

laws and policies include Privacy Bill, 2013; Draft National Encryption Policy, 2015 and DNA Profiling Bill, 2015. The UPR 2017 also cited concerns on barriers for women in accessing information and communications technologies (ICTs) courtesy of the socio-economic inequalities. The UPR also identified thematic areas such as access to internet, right to information, freedom of opinion and expression online, right to privacy, freedom of association and assembly online, gender and the internet, cybercrime and sexual exploitation, international mechanisms and recommendations to the GoI. DEF also published a summary document on the UPR 2017;[6] and published joint *Recommendations on the second UPR of India,* including participation in the Human Rights Council working group of the UPR – Thirteenth Session (Geneva 21 May-4 June 2012).[7]

The project also included an advisory committee which advised on planning, project outreach and promotion, implementation, meetings and sub-committees and other miscellaneous tasks.[8] Moreover, the project in total held five workshops; these consisted of the Internet Rights are Human Rights (IRHR) UPR Advocacy Workshop for Human Rights Organisations, IRHR eNGO Workshop, IRHR Workshop at CIRC, Internet Rights Human Rights Workshop, APC Women Human Rights Defenders Workshop, and Training of the Trainers (TOT) on IRHR Curriculum for Grassroots Beneficiaries.[9] Five consultations were held by DEF including Right to Access the Internet, Upholding a Human Right, Not Too inaccessible for Broadband: Connecting Remote Communities with Wireless Spectrum, Google India-DEF Launches Good to Know Campaign for Web Safety, National Consultation on Internet Rights, Accessibility, Regulation & Ethics Inauguration & Plenary: Right to Internet for Right to Information and Round Table Discussion on Internet Governance.[10] Moreover, for meeting its capacity building related objectives, DEF prepared and uploaded its entire IRHR curriculum on its website www.internetrights.in. The training curriculum consisted of four modules including resources translated in the Hindi language, with provision of presentation slides, handouts, and discussions and case-studies for the individual participants and trainers. Additional documents under the curriculum section also included *Internet Rights for NGOs, Pedagogy Document for Centers and Basic Human Rights under the Constitution of India.*[11] In tandem with the curriculum a digital security kit was uploaded for free-access and consumption of the public. This included a tool kit in both English and Hindi.[12]

A dedicated media related section is maintained by DEF for reporting on daily news significant to internet rights. The section included updates on interviews, events, books and publications. DEF also contributed to policy and advocacy related initiatives under this project. Among the country research reports, DEF published, *Limited Access Restricting Expression*[13]*, including Human Rights vs. National Security*[14] highlighting collateral damage to the internet rights as a consequence of the internet shutdowns and restrictions posed by the state to online expression and access to the internet. For promoting policy related discussion DEF also maintained a section called Information Communication

6 www.internetrights.in/wp-content/uploads/2017/02/Coalition_UPR-Report-2017_India_Summary.pdf
7 internetrights.in/human-rights-council/
8 internetrights.in/about-us/#AdvisoryCommittee
9 internetrights.in/capacity-building/#Training&Workshop
10 internetrights.in/capacity-building/#Consultations
11 internetrights.in/capacity-building/#IRHRCurriculum
12 internetrights.in/capacity-building/#digitalsecurity
13 internetrights.in/wp-content/uploads/2015/10/Country-Research-Report_September-2015.pdf
14 Srivastava, R., & Abraham, B. (2017). *Country Report: Anatomy of Virtual Curfews: Human Rights vs. National Security.* Digital Empowerment Foundation. docs.google.com/viewerng/viewer?url=internetrights.in/wp-content/uploads/2017/08/Internet-Shut-down.pdf&hl=en

Technologies for Development (ICT4D) Columns. Under this project, DEF participated at various national and international events.[15] Different policy recommendations were articulated under policy advocacy, including disaster risk management and ICT, DEF recommendations and stance on net neutrality, communications, surveillance and human rights in India,[16] and joint written statement submitted by APC to the 34th session of the Human Rights Council: Freedom of expression and religion in Asia/ Bangladesh and Pakistan.[17]

- **APC-IMPACT in Malaysia:**

The APC-IMPACT project started in Malaysia in 2014 in partnership with its local partner EMPOWER. EMPOWER held two meetings with prospective national level partners, on 12 August and 25 November 2014 respectively. The meetings led to constitution of National Steering Committee.[18] Issues to be covered by Committee included, increased surveillance by state on the internet users, harassment of internet users and confiscation of devices by law enforcement agencies and physical raids of offices, blocking content and restricting access to internet, prosecution of internet users over statements and remarks deemed as sedition and threatening to national security. Furthermore, EMPOWER incorporated the APC-La Rue Framework[19] to author and prepare its country report for Malaysia titled *Status of Freedom of Expression Online: A Country Report of Malaysia.*[20] In 2014, EMPOWER also organised a follow up event after the interim disruption when the Coalition of Malaysian NGOs (COMANGO) was declared illegal by the government. The follow up Consultation on Monitoring UPR Recommendations was held on 4 and 5 August 2014.[21] At the consultation, COMANGO endorsees agreed to submit a mid-term report in 2016 and to monitor Malaysia's implementation of UPR recommendations in five thematic areas, including civil and political rights, economic, social and cultural rights, groupings of people (women, indigenous, disabilities, asylum seekers), institutions and mechanisms, and freedom of religion and racism.

In 2015, EMPOWER obtained funding for monitoring UPR recommendations for Malaysia Project, the object of which was to monitor the implementation of the UPR recommendations received in Malaysia's second review cycle in 2013. To meet this object, EMPOWER in consultation with other NGOs in Malaysia constituted COMANGO to build and implement a common monitoring framework along with an action plan.[22]

EMPOWER organised pre-event and workshops on internet rights at the ASEAN Peoples' Forum, organised its first workshop based on APC's IRHR curriculum and the publication of the country research into freedom of expression in the same year. EMPOWER also initiated a twitter teach-in and campaign on internet rights and submitted a joint statement in June with APC to the Human Rights Council along with an oral statement on threats to online freedom of expression and opinion in Malaysia on behalf of EMPOWER and APC.[23] An APC-IMPACT regional Training of

15 internetrights.in/policyadvocacy/#participation
16 internetrights.in/policyadvocacy/#policyanalysis
17 *Association for Progressive Communications. (2017, February). Joint written statement submitted by the Association for Progressive Communications to the 34th session of the Human Rights Council: Freedom of expression and religion in Asia/Bangladesh and Pakistan.* APC. www.internetrights.in/wp-content/uploads/2016/09/DraftWrittenstatementonHRC34.pdf
18 . EMPOWER. (2014). *EMPOWER Annual Report* 2014.
19 *Association for Progressive Communications. (2013). APC-La Rue Framework for assessing freedom of expression and related rights on the internet.* https://www.apc.org/sites/default/files/APC-La_Rue_Framework_digital.pdf
20 EMPOWER. (2015a). *Status of Freedom of Expression Online: Malaysia.* empowermalaysia.org/impact/monitoring
21 EMPOWER. (2014). Op. cit.
22 . EMPOWER. (2015b). *EMPOWER Annual Report* 2015.
23 Ibid.

Trainers was organised from 29 May to 02 June 2015 by EMPOWER. Earlier that year EMPOWER produced research publications and held national consultation on Internet Governance, Human Rights and Democracy in Malaysia in April to present a draft of the country on FoE online in Malaysia. Following consultation a report was published in 2015 titled *Status of Freedom of Expression Online*.[24] The report adopted the APC-La Rue Framework and sought to assess Malaysia's record on arbitrary blocking or filtering of content, criminalising of legitimate expression, imposition of internet intermediary liability, the implications of disconnecting users from the internet, cyber-attacks, privacy and data protection, and internet access.[25] It covered events based on media reports that occurred from 1 January 2014 to 31 March 2015. The object of this research was to aid the advocacy strategy to improve the internet governance and introduce reforms to laws to improve people's internet rights.[26]

In 2016, EMPOWER conducted a training from 30 January to 2 February on Internet Rights are Human Rights and conducted a talk with university students under the same project on 18 February . On 27 February a separate training was conducted on UPR Writing Workshop. UPR related trainings were also held in June and July. Furthermore, training was delivered from 14 to 17 July, 2016 by EMPOWER on IRHR with women human rights defenders for raising awareness that Internet Rights are also Women's Rights.[27]

EMPOWER conducted secure online communications (SOC) regional training from 25 to 31 May 2016 under IMPACT. Furthermore, EMPOWER held and delivered two separate research studies in collaboration with APC. Their key theme was to highlight the issues faced by women in online freedom of information (FoI) and freedom of association and assembly (FoAA) in online spaces. The research will be used by EMPOWER to bridge the gap on misperceived separation of online and offline spaces.[28] The focus of this remained on highlighting barriers faced by women in exercising FoI and FoAA in Malaysia. The object of this study was to use it as an advocacy tool in future for guiding informed policies and legislation in securing equal rights for women in online and offline spaces for securing and exercising FOI and FoAA without any discrimination.[29] A six-day IMPACT Capacity Building Workshop was held by EMPOWER from 23 to 28h November 2016 and 16 days of online activism campaign was executed from 25 November to 10 December known as Internet Kita. Under this project, UN Special Rapporteur Maina Kiai delivered a public lecture on FoAA.[30]

In 2016 EMPOWER published a study on the *Freedom of Assembly and Association Online in Malaysia.* The research framework employed relied on case studies, particularly expert interviews and desk research. This expansive study sought to highlight three main areas. Firstly it sought to elucidate on the state of the online FoAA online in Malaysia, particularly by providing a historical context to it. Secondly it offered an insight into the diverse strategies employed by civil society activists to use ICT for their respective movements in Malaysia. And finally it contextualised the exercise of FoAA online to the broader struggles of human rights in the country.[31] To this end, the research also highlighted the threats and challenges faced by civil society organisations and activists while trying to exercise their right of FoAA online.[32]

24 Ibid.
25 EMPOWER. (2015a). Op. cit.
26 Ibid.
27 EMPOWER. (2016). *EMPOWER Annual Report* 2016.
28 Ibid.
29 Ibid.
30 Ibid.
31 EMPOWER. (2016). *Freedom of Assembly and Association Online in Malaysia.*
32 Ibid.

- **APC-IMPACT in Pakistan**

The APC-IMPACT project began in Pakistan in the year of 2014. APC partnered with Bytes for All, Pakistan to execute this project. Like other regional partners, Bytes for All, Pakistan raised awareness under the scope of this project particularly on FoE and FoAA in online spaces. Most notably Bytes for All, Pakistan made an important contribution to the process of Universal Periodic Reviews (UPR). To this end, in continuation of the stakeholders' submission made by Bytes for All, Pakistan under the Pakistan's UPR in 2012, the organisation carried out two consultations at Islamabad and Lahore respectively on 25 and 30 January 2016. This Mid Term Periodic Review was launched at a side event co-organised by Bytes for All, Pakistan, and Association for Progressive Communications and FORUM-ASIA at the 31st session of UN Human Rights Council on 10 March 2016.[33] As a stakeholder Bytes for All, Pakistan made a submission on areas of offline and online fundamental rights – particularly FoE and adverse impact of Pakistan Electronic Crimes Act, 2016 (PECA 2016) – right to privacy and surveillance and gender rights (particularly, ICT-Driven Violence against Women).

On PECA 2016, Bytes for All, Pakistan held a notable consultation on 31 May 2016 with members of the Pakistan National Assembly and journalists at Islamabad Press Club to mobilise support on concerning areas of the legislation which could infringe on people's civil liberties, including right to privacy, information and association and assembly.[34] The project team also highlighted concerns on PECA 2016 in different critical pieces since the bill was first tabled in the lower house (i.e. National Assembly) of the Parliament.[35]

In September 2015, Bytes for All, Pakistan published a research study titled *Expression Restricted: An Account of Online Expression in Pakistan*, the objective of which was to assess the status of FoE, FoI and FoAA in online spaces by applying the APC-La Rue Framework and checklist. The study also explored and "addressed the restrictions imposed on the internet by promoting and protecting internet rights."[36]

In October 2015, Bytes for All, Pakistan organised its first workshop with human rights defenders on the IRHR theme to raise awareness on FoAA, FoE and FoI in online spaces. The workshop also attempted to build participants understanding on impacts of the shrinking spaces on their online presence, work and activism.[37]

An Urdu curriculum was prepared under the theme of IRHR for access by the public, particularly human rights defenders, activists and the participants of workshop. A guideline for the UPR process was uploaded on the project website.[38]

Bytes for All, Pakistan also organised a two-day workshop in April 2016, with human rights defenders and members of civil society organisations from Pakistan to enhance their understanding on FoE, FoI and FoAA. The workshop also raised awareness on the secure online communications and on UPR by holding distinct sessions under the workshop. The workshop facilitated 20 human rights defenders working to promote gender, children, religious freedom and freedom of expression rights across Pakistan.[39]

33 Netfreedom.pk. (2016, 9 August). Pakistan Mid-term Universal Periodic Review: Summary of Information. www.netfreedom.pk/summary-of-information-mid-term-universal-periodic-review-pakistan

34 Netfreedom.pk. (2016, 10 June). Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill. www.netfreedom.pk/internet-rights-and-legislation-in-pakistan-a-critique-on-cyber-crime-bill-2016

35 For more information see www.netfreedom.pk/?s=Consultation and www.netfreedom.pk/?s=Prevention+of+Electronic+Crimes

36 Baig, A., & Khan, S. (2015). Expression Restricted: *An Account of Online Expression in Pakistan*. www.netfreedom.pk/wp-content/uploads/2015/09/Expression-Restricted.-An-account-of-online-expression-in-Pakistan.pdf

37 Baloch, H. (2015, 27 October). Bytes for All Pakistan: Internet Rights Are Human Rights workshop. Netfreedom.pk. www.netfreedom.pk/bytes-for-all-pakistan-internet-rights-are-human-rights-workshop/

38 www.netfreedom.pk/category/resources/upr-guidelines

39 www.netfreedom.pk/three-day-workshop-on-internet-rights-are-human-rights

To raise awareness on freedom of expression and right to privacy in online and offline spaces, Bytes for All, Pakistan organised a theatre performance on 3 May 2016. The theatre performance was staged to mark the World Press Freedom Day 2016. The performance highlighted three different issues related to misuse of social media and other online modes of communication resulting in physical threats and censorship issues, especially for marginalised groups including women and religion minorities.[40] This activity was also witnessed by the head of the European Union delegation in Pakistan H.E. Jean-François Cautain and his staff, who lauded the activity.[41]

The United Nations Human Rights Committee in January 2017 included a list of questions issued by Bytes for All, Pakistan, APC and Media Matters for Democracy for a detailed review of Pakistan concerning internet-related human-rights violations in the June-July session 2017.[42] These lists of issues were based on internet-related human rights issues from the recently enacted and implemented PECA 2016.[43]

In January 2017 under the thematic area of IRHR, Bytes for All, Pakistan published a report titled *Shrinking Spaces: Online Freedom of Assembly and of Association in Pakistan* in line with the objectives of the APC-IMPACT project.[44] This study aimed to understand the legal framework in Pakistan protecting and impacting the FoAA in Pakistan particularly, the areas which facilitate or hamper the FoAA in online spaces. Lastly the study recommended strategies for a course forward particularly for the journalists, human rights defenders and organisations and civil society organisations under the existing socio-political environment in Pakistan. [45]

Bytes for All, Pakistan organised another workshop in the city of Swat in February 2017 with local representatives of civil society. The object of the capacity building exercise was to raise awareness among the local representatives on the themes significant to an individual and a group's right to FoE, FoI and FoAA in online spaces. The workshop also aimed to pro*vide* locals with an opportunity to reclaim the use of digital media and tools to publicise their work and views.[46]

Bytes for All, Pakistan compiled a country report on *Effects of Surveillance on Journalists and HRDs is changed to state of Data Protection.* The study aimed to assess and understand the implications of disproportionate laws such as Investigation of Fair Trial Act, 2013, and PECA 2016 and the powers it gave to government authorities to intercept and monitor communications which could have an adverse impact on the FoE and FoAA in online spaces for journalists and human rights defenders and their activism.

40 Theatre of the Oppressed – privacy and expression rights online. www.netfreedom.pk/1224-2/
41 Ibid.
42 Zafar, T. (2017, 11 January). UN Human Rights Committee includes issues from B4A-APC submission. APC-IMPACT. www.netfreedom.pk/un-human-rights-committee-includes-issues-from-from-b4a-apc-submission
43 Ibid.
44 Khan, A. Z. ,& Baloch, H. (2017). Shrinking Spaces: Online Freedom of Assembly and of Association in Pakistan. www.netfreedom.pk/wp-content/uploads/2017/01/FoAA-Report_web.pdf
45 Ibid.
46 Zafar, T. (2017, 11 February). Swat workshop on Internet Rights are Human Rights. *APC IMPACT.* www.netfreedom.pk/swat-workshop-on-internet-rights-are-human-rights

APC-IMPACT: COUNTRY REPORT METHODOLOGY

For the purpose of its research associated with the APC-IMPACT programme, APC developed a broad methodology framework for assessing freedom of expression on the internet, by amalgamating the work of United Nations Special Rapporteur Frank La Rue and on General Comment 34 on Article 19 of the International Covenant on Civil and Political Rights ICCPR).[47] This framework is also applied to observe and report the internet-related human rights violations. This summary report sheds light on the salient features and trends noted in the Internet Landscape Report of Pakistan, India and Malaysia respectively, which have impacted the overall internet landscape and online freedom of expression.

47 APC. (2013). Op. cit.

COUNTRY REPORT SUMMARY
PAKISTAN'S INTERNET LANDSCAPE:

Under IMPACT, Bytes for All, Pakistan published a research report titled Expression Restricted in May 2015. Its focus was to monitor the restriction of the freedom of expression in the online spaces. While serving as an extension and update of *Expression Restricted*, the new report produced under IMPACT by country partner Bytes for All entitled *Internet Landscape of Pakistan* deals with wider set of issues prevailing in Pakistan. The study was compiled by the application of the APC-La Rue Framework. Given Pakistan's unique circumstances, by virtue of both patterns significant to human rights related conditions and genuine security needs, the country partner Bytes for All, Pakistan suggested to work on a research report which would look at the wider issues of FoE, FoAA and internet governance in Pakistan as existing and developing legislative framework and provision of powers to different government authorities were and are likely to create human rights related violations.

The current *Pakistan Internet Landscape Report* attempts to understand the changing patterns taking place under the lens of APC-La Rue Framework, to understand these developments in significance to impact on people's right to expression, right to information, and right to association and assembly online. It further takes an evolutionary look at growth and expansion of internet across Pakistan and its growth relative to regional countries. The report sheds light on the legislative contours which enables executive bodies to block content. It also highlights lack of transparency in public-private cooperation between intermediaries such as Google, Facebook, Twitter, etc. and the latter's compliance with the government. Interestingly, it reveals the extension of blasphemy related penalisation to online spaces under PECA 2016, and overlapping of religiously motivated physical and cyber violence. The report highlights role of executive bodies in cyber moral policing consequence of judicial compliance. However, a change has been in intermediary liabilities under PECA 2016. Among other notable highlights are lack of indiscriminate access to content of cellphone users and increase in surveillance by the state, absence of privacy related mechanisms to protect people's right to privacy in online and offline spaces, growth of digital journalism and internet for social and political activism among media, civil society, sexual minorities and political parties.

The report begins by discussing access to the internet, citing various sources on the gradual increase in the number of users' access to the internet, particularly 3G/4G and broadband

subscribers to stand at 41.7 million and 44.3 million[48] in 2017 as opposed to 31.78 million[49] and 34.4 million[50] in 2016 respectively. As per global internet penetration figures the internet penetration in Pakistan stands at 17.8%,[51] and as per Internet Telecommunication Union the internet penetration remains at 18%.[52] This progress is extremely low when compared with other Asian countries where, as of May 2017, penetration stands at 45.2%.[53] Some of the factors attributed for a higher digital divide are low literacy, difficult economic condition and cultural resistance.[54]

Blocking and filtering of the content over the internet in Pakistan is common, particularly content which is termed as pornographic, blasphemous and anti-state in nature. To this end, section 37 of the PECA 2016, serves as the legal cover for exercising the censorship by Pakistan Telecommunication Authority (PTA).[55] Prior to introduction of this act, Telecommunication Policy 2015 also used similar language (please read further Section 9.8.3 of the policy document).[56] Alarming developments include lack of transparency in the bilateral agreements reached between Google[57] and Facebook[58] with the government of Pakistan. Facebook's compliance to government requests from Pakistan has staggeringly increased. From June 2014 to December 2014 the compliance stood at 42% in comparison to 67.5% from July 2016 to December 2016.[59] Recently, then interior minister Chauhdry Nisar met with Facebook's management on latter's visit to Pakistan. During this visit Facebook management did not hold any meetings with members of the civil society or private stakeholders. In 2014, Twitter also blocked "blasphemous content" on Pakistan's request only to have the decision revoked later after criticism from rights activists.[60] Earlier in 2017, a justice of the Islamabad High Court threatened to ban Facebook if it failed to remove the sacrilegious content.[61] After Islamabad High Court's order, the power to block and online content have been delegated to PTA[62] from Inter-Ministerial Committee for Evaluation of Web Sites (IMCEW). The previous body IMCEW was controversial for the secrecy of its operations and lack of transparency, and personnel.[63]

Witch-hunting of users under the pretext of blasphemy has caused internet users in Pakistan to exercise self-censorship over the internet as much as they do in offline spaces. The current legal provisions penalising blasphemy (including Section 295-A of Criminal Procedure Code and Section 37 of PECA 2016) are rampantly subject to abuse by the general public for settling personal scores against innocent victims. Notable persecution under this allegation involved the act of

48 Pakistan Telecommunication Authority Indicators. www.pta.gov.pk/index.php?Itemid=599
49 Chaudhry, H. (2016, 24 August). 3G and 4G mobile internet users cross 30m milestone. *Dawn.com*. www.dawn.com/news/1279886
50 Pakistan Telecommunication Authority Indicators. www.pta.gov.pk/index.php?Itemid=599
51 Internet World Stats. www.internetworldstats.com/stats.htm
52 Attaa, A. (2016, 25 July). Pakistan among Countries with Lowest Internet Penetration: ITU. *Propakistani*. https://propakistani.pk/2016/07/25/pakistan-among-countries-with-lowest-internet-penetration-itu
53 Internet World Stats. www.internetworldstats.com/stats.htm
54 Freedom House. (2016). Freedom on the Net 2016 – Pakistan Country Profile. freedomhouse.org/report/freedom-net/2016/pakistan
55 The Prevention of Electronic Crimes Act 2016. www.na.gov.pk/uploads/documents/1470910659_707.pdf
56 Freedom House. (2016). Op. cit.
57 BBC. (2016, 18 January). Pakistan unblocks access to YouTube. BBC. www.bbc.com/news/world-asia-35345872
58 govtrequests.facebook.com/country/Pakistan/2016-H2
59 Ibid.
60 Dawn. (2014, 18 June). Twitter restores access to block content in Pakistan. *Dawn.com*. www.dawn.com/news/1113542
61 Shehzad, R. (2017, 7 March). Blasphemy: IHC directs authorities to block all social media if necessary. *Express Tribune*. https://tribune.com.pk/story/1348784/ihc-directs-authorities-block-social-media-necessary
62 Also read further on the powers given to PTA in Haider, M. (2015, 21 March). PTA given powers for content management on internet. *The News*. www.thenews.com.pk/print/30534-pta-given-powers-for-content-management-on-internet
63 Haque, J. (2016). *Pakistan's Internet Landscape*. Bytes for All. www.gp-digital.org/wp-content/uploads/2016/09/Pakistan_Internet_Landscape_2016.pdf

abduction of five activists earlier in 2017 for their alleged administration of a social media page, "Bhensa".[64] All of them went missing in the first week of January. Other notable cases from 2017 include lynching of Mashal Khan by a rabid mob in Mardan,[65] arrest of a 16-year-old minor from Sheikhupura for sharing a derogatory picture of a Muslim holy place[66].

Moreover, pornographic websites and content is the most blocked content over the internet in Pakistan. Until January it is reported PTA[67] has directed Internet Service Providers (ISPs) to block over 400,000 "offensive" websites at the domain level.[68] The report also cites a case where blocking of websites such as Tumblr, which contains diverse content, incurred collateral damage. Such a precedent has been seen when, under pretext of blasphemy, access to Facebook and YouTube were also blocked in Pakistan.[69]

PECA 2016 exempts service providers from any civil and criminal offences for unlawful actions of their users.[70] On the contrary, in the past YouTube was blocked under the contention that it failed to regulate the offensive content.[71] However, in a famous YouTube case[72] the court consented to issue an interim order assuring YouTube of intermediary legal protection.[73]

In terms of net neutrality Pakistan lacks legislation and present market practices by service providers compromises its essence. Most of the service providers only allow limited access to services such as Free Basics and Facebook Zero.[74] Consequently a practice of discrimination remains apparent in terms of access to services to users from service pro*vide*rs.[75] Among service providers, it includes Mobilink[76], Zong[77] and Telenor,[78] with the exception of Ufone offering access to other web services under its data package.[79]

Pakistan's internet infrastructure stands in an inefficient state; however, addition of two new submarines recently will enable Pakistan to deal with such unforeseen problems. Pakistan's internet infrastructure's inefficiency was evident from the recent outbreaks of disruptions in the undersea cables on 5 and 6 July[80] and subsequently in the first week of August 2017. *Dawn* newspaper

64 Radio Free Europe/Radio Liberty. (2017, 19 January). Missing Pakistani activists hit by 'malicious' blasphemy charges, families say. *RFERL*. www.rferl.org/a/missing-pakistani-liberal-activists-hit-by-malicious-blasphemy-charges-families-say/28242577.html
65 The Nation. (2017, 4 June). Mashal Khan's murder was pre-planned: JIT report. The Nation. nation.com.pk/national/04-Jun-2017/mashal-khan-s-murder-was-pre-planned-jit-report
66 Ghyas, S. (2016, 19 September). Blasphemy law: Nabeel Masih, a Christian teenager, has been arrested for liking the Kaaba's picture on Facebook. The Nation. nation.com.pk/blogs/20-Sep-2016/blasphemy-law-nabeel-masih-a-christian-teenager-has-been-arrested-for-liking-the-kaaba-s-picture
67 Also read Pakistan Telecommunication Authority Act 1996, wherein the term "obscene" content is rather vaguely defined under the act which subsequently directs blocking of such content.
68 Wike, R., & Simmons, K. (2015, 18 November). Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech. *Pew Research Center*. www.pewglobal.org/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech
69 AFP. (2016, January 26). Govt orders 400,000 porn sites blocked. *Dawn.com*. www.dawn.com/news/1235554
70 Prevention of Electronic Crimes Act of 2016. National Assembly of Pakistan. www.na.gov.pk/uploads/documents/1470910659_707.pdf
71 Dawn. (2017, 21 June). Could it happen again? Remembering Pakistan's Facebook, YouTube ban. *Dawn.com*. www.dawn.com/news/1320650
72 Jajja, S. (2013, 15 May). YouTube ban: Google to appear before Lahore High Court. *Dawn.com*. www.dawn.com/news/1027189
73 Ibid.
74 Pakistan Internet Landscape Report, 2017.
75 Ibid.
76 expressm.jazz.com.pk/smart/free-sites.html
77 www.zong.com.pk/internet/mobile-internet/internet-promotions/facebook-freebasics
78 www.telenor.com.pk/freebasics-com
79 www.ufone.com/data/tariff/prepaid
80 Attaa, A. (2017, 7 July). After Cable Cut, Internet in Pakistan is Back to Normal: PTCL. propakistani.pk/2017/07/06/internet-slow-due-submarine-fault-ptcl

cited a report by Center for Technology Innovation[81] putting the economic losses due to internet disruption between 1 July 2015 and 30 June 2016 at USD 69.7 million.[82]

The practice of kill-switch specific to cellular phone services remains intact. On Pakistan Day, the government suspended cellphone services while a military parade was underway.[83] Similar practices are observed on Independence Day official celebrations and religious processions. This measure is taken under the legal blanket of Section 54 of Pakistan Telecommunications (Reorganisation) Act of 1996.[84]

Pakistan still faces an absence of legal regimes regarding data protection of individuals and businesses. The PECA 2016 legislation penalises violations regarding individual privacy or that involving compromise of business data, however, the dire need for such legal instrument was realised after government departments were hit by a ransomware attack in May 2017.[85] The same concern has been raised in *Digital Pakistan Policy*, a public policy document issued by the government.

For surveillance and lawful attempt laws such as Investigation of Fair Trial Act, 2013[86] and PECA 2016[87] grant authority – subject to approval from a court – to investigation agencies to undertake surveillance. The report also highlights legal compliance for service providers to retain traffic data of consumers for one year. Citing Privacy International's report from 2013, the study also highlights concern of anticipated development of mass-surveillance infrastructure by government and intelligence authorities.[88] The study further reports findings of Citizen Lab from 2013 which found attempts by Pakistan's government to procure off the shelf systems to expand its surveillance capabilities, such as from German company Finfisher.[89]

Media groups have started to incorporate digital journalism. This is evident from *Express Tribune's* launch of Tribune Labs[90] a digital journalism platform, and *Geo News*' attempts to use 360° degree technology for storytelling.[91] Moreover, *PakVoices* a digital news platform was launched in Pakistan to promote accountability and transparency at the grass root levels and to report news from remotest areas of Pakistan.[92]

Furthermore, over the past few years, Pakistan has experienced a steady surge in use of social media and internet for activism.[93] Political parties such as Pakistan Tehreek-e-Insaf used social media for political

81 Dawn. (2016, 7 October). $70 million – the loss to Pakistan's economy from internet shutdowns. *Dawn.com*. www.dawn.com/news/1288608/70-million-the-loss-to-pakistans-economy-from-internet-shutdowns

82 West, D. (2016, October). *Internet shutdowns cost countries $2.4 billion last year.* Center for Technology Innovation. Washington D.C.: Brookings. www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf

83 Dawn. (2017, 20 March). Blackout of mobile phone services irks Islamabad, Pindi residents. *Dawn.com*. www.dawn.com/news/1321565

84 Shehzad, R. (2017, 18 January). Connection interrupted: Cellular services can only be suspended in 'emergency'. *Express Tribune*. tribune.com.pk/story/1298744/connection-interrupted-cellular-services-can-suspended-emergency

85 Dawn. (2017, 29 May). Data protection. Dawn.com. www.dawn.com/news/1335971

86 National Assembly of Pakistan. (2013, 22 February). Investigation of Fair Trial Act of 2013. *The Gazette of Pakistan*. www.na.gov.pk/uploads/documents/1361943916_947.pdf

87 Prevention of Electronic Crimes Act of 2016. www.na.gov.pk/uploads/documents/1470910659_707.pdf

88 Rice, M. (2015). Tipping the scales: Security and surveillance in Pakistan. *Privacy International*. www.privacyinternational.org/node/624

89 Marquis-Boire, M. et al. (2013). For their eyes only: *the commercialisation of digital spying*. The Citizen Lab. citizenlab.ca/storage/finfisher/final/fortheireyesonly.pdf

90 labs1.tribune.com.pk/about-us

91 www.geo.tv/news360/360-The-sights-and-sounds-of-Karachi-Burnes-Road/list

92 www.pakvoices.pk/about-us-2/

93 Asia Despatch. (2013, 13 May). Pakistan elections 2013: The social media impact. *Asia Despatch*. www.asiadespatch.org/2013/05/13/pakistan-elections-2013-social-media-impact

activism and mobilisation prior to and after the 2013 general elections. The transgender community has used social media to raise awareness on violence and discrimination against the community. As a result, the community has successfully secured a rehabilitation plan by the provincial government of Khyber Pakhtunkhuwa, including issuance of national identity cards with gender "X" and the introduction of a comprehensive transgender policy. [94]

With respect to international cooperation and engagement by Pakistan's government, the present legislation PECA 2016, governs cooperation based on responsibility to troubleshoot cyber crimes.[95] The relevant section is also criticised by rights activists for the absence of any judicial oversight to the present mechanism. Human Rights Watch in a report released in May 2017 urged Pakistan to uphold the freedom of expression for all, to stop the "abusive monitoring of the internet activity and prosecute those committing violence on the basis of internet blasphemy allegations".[96]Despite aforementioned grave concerns, Pakistan underscores the importance of its commitment to global cooperation on internet rights, universal access and digital governance.[97]

94 Ali, U. (2017). Hashtag trans lives matter. Newsline, July. expressnewslinemagazine.com/magazine/ashtag-trans-lives-matter
95 www.na.gov.pk/uploads/documents/1470910659_707.pdf
96 Human Rights Watch. (2017, 16 May). Pakistan: Escalating Crackdown on Internet Dissent. www.hrw.org/news/2017/05/16/pakistan-escalating-crackdown-internet-dissent
97 Express Tribune. (2017, 18 January). IT minister committed to 'Digital Pakistan'. *Express Tribune*. https://tribune.com.pk/story/1298594/minister-committed-digital-pakistan/

COUNTRY REPORT INDIA

The Report has applied the APC-La Rue Framework in tandem with APC's framework to critically assess and examine India's internet landscape. It also encompasses a comprehensive reflection of the international normative and domestic legal framework, including the Human Rights Committee stance in 2012 on equality of offline and online rights. It further underscores significance of right to privacy and possible outfalls in backdrop of recent judgment by India's Supreme Court on the question of privacy. The report explores and addresses legal and executive instruments for arbitrary blocking of the content on the internet. The report critically and analytically examines judicial precedents having consequences for the Indian people's digital rights including freedom of expression, association and assembly online. It similarly examines the disturbing, yet growing, pattern of internet shutdowns to curtail political dissent across India. Similarly the role of domestic and international stakeholders is encapsulated in this report, including India's shifting stance on internet governance over the past few years.

The Indian Internet Landscape Report begins with a discussion on the constitutional framework and national policy. The discussion begins by citing international treaties including the International Covenant for Civil and Political Rights (ICCPR) and its Article 19(3). The section underscores circumstances impinging on the right to freedom of expression, and the right to liberty and privacy since Article 19 of the ICCPR enunciates right to freedom of expression, right to privacy, including right to religion. Therefore, the Human Rights Council in 2012 underscored protection of these rights in offline and online spaces alike.[98] The section highlights the role of international platforms such as the Internet Governance Forum (IGF), Internet Corporation for Assigned Names and Numbers (ICANN), World Summit on the Information Society (WSIS) and International Telecommunication Union (ITU). The report also cites parts of the national legal framework having implications on freedom of expression in online spaces, including freedom of assembly and privacy, such as Part III of the Indian Constitution, Indian Penal Code 1860 and Code of Criminal Procedure (CrPC) 1973, and Information Technology Act 2000 (as amended in 2008).

Under the area of intermediary liabilities, unlike the measure of content blocking, this measure involves having the intermediaries such as Google, Facebook, Twitter, YouTube, etc. remove the content from their respective websites. Section 79 and subsection (2) and (3) of the Information Technology Act of 2000 (as amended in 2008)[99] in tandem with Information Technology Rules 2011, particularly Rule 3(2)(b), guide the regulation practices of intermediaries. The legal provisions after the *Shreya Singhal v. Union of India* [100]removed the liability of intermediaries to remove content after legal requests from private entities and the order set the liability to respond on requests from government agencies or in light of a court order, and keeping intact immunity of the intermediaries in case of failure to comply with legal requests.

98 Human Rights Council. (2012, 29 June). The Promotion, Protection and Enjoyment of Human Rights on the Internet. 20th Session, A/HRC/20/L.13.
99 Information Technology Act of 2008. cc.tifrh.res.in/webdata/documents/events/facilities/IT_act_2008.pdf
100 *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

However failing to comply with legal requests sent by government agencies or in the case of a court order, intermediaries could be held liable. It has been observed that legal requests from government have greatly increased to Facebook[101] and Twitter,[102] particularly requests for user information since 2015. Also, requests to Google for user information, requests for user accounts and for take-down have drastically increased in 2016.[103]

On the state of the right to privacy and data protection in India, the report cites Article 21 in tandem with Article 14 of the Indian Constitution as the bedrock of the fundamental right to privacy of an individual citizen in India. Another interesting development is the recent historic judgment passed by the apex court of India on 24 August 2017 which can have implications across the online and offline continuum.[104] The verdict extended fundamental right to privacy as an absolute right protected under Article 21 of the constitution.[105] The verdict is likely to have implications on government's ongoing biometric data centralisation project called Aadhar (a Hindi word which means "foundation") and on the anticipated review of the 2013 apex court judgment which criminalised gay sex.[106] Similarly, the Internet Landscape Report 2017, while debating the restriction on an individual's liberty, cites the judgment from *Maneka Gandhi v. Union of India Case,* AIR 1978 SC 597.[107]

In the area of arbitrary blocking of content the report considers legal provisions sanctioning executive measures and the changes occurring between the period of 2014 and 2017. Lastly it pronounces recommendations on the challenges faced by relevant stakeholders. Legislative measures for this are sanctioned under Section 69A of the Information Technology Act. The report speaks at length about legal contours of the aforementioned section (including criminal penalisation) and the Blocking Rules, particularly the executive powers involving a layer of hierarchical structures and procedures for blocking and removal of the content over the internet in India.[108]

Under the part of criminalising legitimate expression the report looks at the implication of the existing legal regime on the online expression. India's apex court struck down Section 66A of the Information Technology Act (ITA) as being unconstitutional because of going beyond Article 19(2)[109] of the Indian Constitution. Despite being struck down, the section is scarcely being used by police to register complaints against citizens.[110] However, criminal defamation has been kept intact by the Supreme Court under Section 499 and 500 of the Indian Penal Code in its verdict in the *Subramanian Swamy v. Union of India*.[111] The court found the provisions to be consistent with the Article 19(2) of the Indian Constitution. However, hate speech

101 Government Requests Report: India (July-December 2016). govtrequests.facebook.com/country/India/2014-H2/
102 Twitter Transparency Report: Removal Requests. transparency.twitter.com/en/removal-requests.html#removal-requests-jan-jun-2016
103 Google Transparency Reports: Requests for user information (January-December 2016). transparencyreport.google.com/user-data/overview. Google produced and handed over data to the government at the rates of 55% and 57%, respectively.
104 The Wire. (2017, 24 August). Right to Privacy a Fundamental Right, Says Supreme Court in Unanimous Verdict. *The Wire*. https://thewire.in/170303/supreme-court-aadhaar-right-to-privacy
105 Ibid.
106 Biswas, S. (2017, 24 August). How significant is India's landmark privacy judgement?. *BBC News*. www.bbc.com/news/world-asia-india-41037992
107 *Maneka Gandhi v. Union of India,* AIR 1978 SC 597.
108 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. https://cis-india.org/internet-governance/resources/information-technology-procedure-and-safeguards-for-blocking-for-access-of-information-by-public-rules-2009
109 Hariharan, G. (2015, 26 March). What the 66A Judgment Means for Free Speech Online. *Huffington Post*. www.huffingtonpost.in/geetha-hariharan/what-66a-judgment-means-f_b_6938110.html
110 Shivadekar, S. (2015, 7 September). Nashik cops register case under Section 66A of IT Act despite SC scrapping it in March. *Mumbai Mirror*. https://mumbaimirror.indiatimes.com/mumbai/cover-story/Nashik-cops-register-case-under-Sec-66A-of-IT-Act-despite-SC-scrapping-it-in-March/articleshow/48851393.cms
111 Bhanu Mehta, P. (2016, 18 May). Supreme Court's judgment on criminal defamation is the latest illustration of a syndrome. *The Indian Express*. indianexpress.com/article/opinion/columns/supreme-court-criminal-defamation-law-subramanian-swamy-2805867

related crimes fall under Section 153A, and 295A of the Indian Penal Code. The disturbing element is that in a judgment Supreme Court added that it was not necessary for an offender to express intent under an expression of act or speech that falls under as hate speech under Section 153A.[112] However, in case of Section 295A, the Supreme Court restricted provision under Article 19(2) "in the interest of public order" to uphold the applicability of the Section 295A.[113] Section 124A is applied for pressing charges of sedition. Various cases from 2015 and 2016 are cited in the report where private citizens were charged for hate speech and sedition related crimes in the online spaces, including artists such as a comedian[114] and a cartoonist[115] for criticising corruption in the government.

While discussing internet shutdowns the report cites different events from different Indian states which experienced internet shutdowns. This part of the report begins with defining internet shutdowns, later it describes in detail Section 144 of the CrPC to enforce an internet shutdown. The report questions the constitutionality of forcing internet service providers (ISPs) to undertake a shutdown. Since 2015 there have been 73 internet shutdowns across India; most of these shutdowns have taken place in the state of Jammu and Kashmir, 48 to date, followed by Rajasthan, Gujrat and Haryana with 11, 10, and 9 shutdowns respectively.[116] A public interest litigation in Gujrat challenged the state government's shutdowns in the Gujrat High Court. The petition argued the applicability of the Section 144 of CrPC for shutting down of the mobile internet, while Section 69A gave powers to suspend intermediaries and apps (such as Facebook and WhatsApp). The State Government argued presence of sufficient valid grounds for use of force under Section 144.[117]

The section related to internet governance discusses prospects about governance of internet in India. It identifies relevant stakeholders from government such as the Ministry of External Affairs (MEA), Department of Telecommunications (DOT), Department of Electronics and Information Technology (DeITY), the last two departments being within the Ministry of Information and Communications Technology. The report mentions the swaying stance of Indian government on internet governance switching its position from supporting paragraph 35 of the Tunis Agenda for the Information Society,[118] a multilateral perspective (i.e. underscoring sovereign policy authority of states),[119] to a multi-stakeholder nature of the internet governance which is more consistent with the objects of the Internet Governance Forum.[120] Presently India has moved closer to a multistakeholder perspective of internet governance consistent with its stated stance at Internet Governance Forum, 2014.[121] While India has not held a national internet governance forum, it has held consultations with multiple stakeholders nationally including with civil society.

112 *Gopal Vinayak Godse* v. Union of India & Ors, AIR 1971 Bom 56.
113 *Ramji Lal Modi* v. State of Uttar Pradesh, AIR 1957 SC 620
114 Mangaldas, L. (2017, 17 July). How A Meme Of Indian PM Modi With Puppy Ears Provoked Police Complaints In India. *Forbes*. www.forbes.com/sites/leezamangaldas/2017/07/17/how-a-meme-of-indian-pm-modi-with-puppy-ears-provoked-police-complaints-in-india/#ff753dc6570d
115 The Hoot. (2015, 18 March). Mere criticism is not seditious: Bombay High Court on Aseem Trivedi's cartoons. *The Hoot*. www.thehoot.org/media-watch/law-and-policy/mere-criticism-is-not-seditious-bombay-high-court-on-aseem-trivedi-s-cartoons-8177
116 internetshutdowns.in/about
117 *Gauravbhai Sureshbhai Vyas* v. State of Gujarat, at indiankanoon.org/doc/29352399/
118 www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
119 Government of India's initial submission to the Global Multistakeholder Meeting on the Future of Internet Governance, Sao Paulo, Brazil, 23-24 April 2014. content.netmundial.br/contribution/government-of-india-s-initial-submission-to-global-multis-takeholder-meeting-on-the-future-of-internet-governance-sau-paulo-brazil-april-23-24-2014/138
120 India's Submission to the WCIT, 14 December 2012. pib.nic.in/newsite/erelease.aspx?relid=90748
121 Hariharan, G. (2014, 1 November). Good Intentions, Recalcitrant Text - II: What India's ITU Proposal May Mean for Internet Governance. *CIS India Blog*. cis-india.org/internet-governance/blog/good-intentions-recalcitrant-text-2013-ii-what-india2019s-itu-proposal-may-mean-for-internet-governance

COUNTRY REPORT MALAYSIA

The country report from Malaysia succinctly assesses the current dynamics of the country by applying the APC-La Rue Framework. It discusses policy and legal frameworks that can consequently jeopardise people's Freedom of Expression, Association and Assembly Online. Interestingly report has identified possible areas of inclusion in the framework by citing case-studies from national context. It highlighted cases of arbitrary blocking of content and website fundamental to FoE. Similarly, it offered a glimpse in the application of various laws for penalising and criminalising legitimate and free speech. The study also revealed existing discrepancies on protection of privacy under existing national legal regime, hurdles in exercising of right to information, and possible interventions to address lack of understanding regarding internet-related human rights at among the public and public-institutions.

The report on the internet landscape of Malaysia begins with a discussion of the general protection of FoE; under this chapter, the report discusses possible amendments to the existing Communication and Multimedia Act, 2015 by the Malaysian Government, which could require registration of the political bloggers and provision of greater powers for the Malaysian Communications and Multimedia Commission (MCMA).[122] The MCMA is also working on the proposal to initiate registration of portals with higher traffic allegedly to curb fake news or slander[123] which could have adverse outfall for the freedom of expression in the online sphere.

Interestingly the assessment report of the internet landscape in Malaysia contains a dedicated section titled Missing Components. It calls for inclusion of additional indicators in the APC-La Rue Framework, such as assessment of online harassment of women (sic gender motivated online harassment), threats posed by non-state actors specific to the indicated checklists and indicators under the framework.[124] Similarly, it draws attention to the contextual use of "free-speech" as a cover for expression of misogynist remarks against women in Malaysia.[125]

The third chapter deals with arbitrary blocking and filter of the content and webpages. The report highlights three relevant case studies from 2016 and 2017. The first case deals with blocking of the online publishing platform *Medium* for refusing to remove content from its website which it received from a whistleblower website, *Sarawak Report*, until

122 Joint Action Group for Gender Equality. (2016, 16 May). Press Statement: Consultation before Amendments: Keep the Internet Free. Net Merdeka. www.netmerdeka.org/2016/05/16/consultation-before-amendments-keep-the-internet-free/
123 Kaur, M. (2017, 14 September). Proposal to register high traffic online sites in final stages. *FMT News*. www.freemalaysiatoday.com/category/nation/2017/08/28/proposal-to-register-high-traffic-online-sites-in-final-stages/
124 Malaysia Internet Landscape Report, 2017.
125 Malaysiakini. (2015, 8 November). Bash Azalina, but don't be sexist, misogynist or other –ist. *Malaysiakini*. www.malaysiakini.com/news/318788

it received an order from a court of competent jurisdiction.[126] The second case study involves *The Malaysian Insider* which was blocked for violating Section 233 by several Malaysian ISPs after receiving orders from the Malaysian CMC.[127] The third case consists of temporary blocking of *Steam* for not complying with Malaysian authorities requests (citing religious grounds) to block certain download products for Malaysian users.[128]

The next section in the same chapter is titled Criminalising Legitimate Expression and it highlights the use of laws such as Section 4(1) of the Sedition Act, Section 233 of the CMA, including other legal provisions in the penal code to clamp down on legitimate expression.[129] The notable case cited under this section sheds light on case of a 46-year-old Kelantanese fisherman Nik Pa[130] and his son for posting insulting comments against the Johor crown prince.[131] Another case highlighted under this section mentions arrest of a former journalist Sidek Kamiso who was previously arrested under Section 298A of the Penal Code and Section 233 of the CMA for allegedly posting offensive remarks on the death of the spiritual leader of Islamic Party of Malaysia, Haron Din.[132] Kamiso was later re-arrested shortly after his release for allegedly posting insulting comments against Islam.[133] The section also cites a disturbing development, when Deputy Communications and Multimedia Minister Jailalani Johari Johari warned administrators of WhatsApp chat-groups that they could face prosecution if members of the chat groups posted "fake news".[134] Following his statement, MCMC issued advisory guidelines for administrators of WhatsApp chat groups on 3 May.[135]

The section discussing intermediary liabilities found few transparent details shared by the Malaysian authorities, particularly MCMC, regarding its cooperation and requests it made to either ISPs or intermediaries such as Google, Facebook, Twitter, etc. So far only the cases of *Medium* and *Steam* are publicly known. Interestingly, the two aforementioned companies were hosting their content from outside the country at the time the government is known to have requested their content removal.[136]

Under the section of cyber attacks, the report did not find any incident where government would have been involved in undertaking cyber attacks. However it pointed towards an interesting domestic and contextual dynamic where malicious acts by "cyber-troopers" targeted opposition and critics of the government. The section also reported an environment of impunity for the cyber attacks, particularly for the non-state actors.[137]

126 Berthelsen, J. (2016, 3 March). UN, US Call for Answers on Malaysian Press Blockages, *Asia Sentinel*. www.asiasentinel.com/politics/un-us-call-answers-malaysia-press-blockages/

127 Mollman, S. (2016, 14 March). A news website that reported on the Malaysian prime minister's alleged corruption is shutting down. *Quartz*. qz.com/638369/a-news-website-that-reported-on-the-malaysian-prime-ministers-alleged-corruption-is-shutting-down

128 Jones, A. (2017, 13 September). Fight of Gods is banned in Thailand too now. *PCGamesN*. www.pcgamesn.com/fight-of-gods/steam-blocked-malaysia-fight-of-gods

129 Malaysia Internet Landscape Report, 2017.

130 Malaymail. (2016, 31 May). Fisherman nabbed for allegedly insulting TMJ via Facebook. *Malaymail Online*. www.themalaymailonline.com/malaysia/article/fisherman-nabbed-for-allegedly-insulting-tmj-via-facebook

131 Ashraf, K. (2016, 16 June). Rakyat Johor lapor polis kerana sayangkan TMJ. *FMT News*. www.freemalaysiatoday.com/category/bahasa/2016/06/16/rakyat-johor-lapor-polis-kerana-sayangkan-tmj/

132 Malaysia Internet Landscape Report, 2017.

133 Malaymail. (2016, 29 September). Catch and release again for ex-journalist Sidek Kamiso. *Malaymail Online*. www.themalaymailonline.com/malaysia/article/catch-and-release-again-for-ex-journalist-sidek-kamiso

134 Zainal, S., et.al. (2017, 28 April). WhatsApp admins may face action. *The Star Online*. www.thestar.com.my/news/nation/2017/04/28/whatsapp-admins-may-face-action-they-can-be-punished-for-spreading-fake-news

135 Malaysian Communications and Multimedia Commission. (2016, 3 May). Peringatan Untuk Pentadbir Kumpulan. www.mcmc.gov.my/media/announcements/peringatan-untuk-pentadbir-kumpulan

136 Malaysia Internet Landscape Report, 2017.

137 Ibid.

On Right to Privacy and Data Protection, the report found that while the Personal Data Protection Act 2010 offers limited protection in the context of commercial transactions there are no safeguards or checks on state use of personal data.[138] Thus, lacunas are found under the current legal framework for provision of substantial and legitimate privacy related safeguards of citizens and businesses. The report also suggests inclusion of acts related to "dox"[139] to APC-La Rue Framework. The case also identified legal measures such as Section 116B of the Criminal Procedure Code which allows legal authorities to request passwords of devices and software for prosecution related purposes. It interestingly reports a case of a an independent candidate for the Bawang Assan constituency in Sarawak who was charged under Section 249 of the CMA for refusing to hand over his Facebook user name and password over a police investigation the previous year into a comment posted on his Facebook page.[140]

With respect to people's ability to access, the report found that despite widespread broadband and mobile internet access at 81.5% and 92% of mobile broadband subscriptions, respectively, there was disproportionate access across geography due to socio-economic factors and highlighted lack of equal access to computers to all Malaysians, particularly those from remote and least privileged areas.[141]

The report also found complications for citizens to have access to information under Right to Information, particularly due to different prices charged by different states for requesting public information. The report also identifies lack of online related disclosure by local and national government bodies to make it more convenient and economical for citizens to exercise their right to information.[142]

Lastly, the report concludes by highlighting a way forward for civil society organisations, legislators and government authorities in overcoming obstacles to people's internet related human rights. The report underscores policy measures for broader awareness and capacity building related measures for public and attitude change interventions for important stakeholders.

138 Ibid.
139 Dox, transitive verb, Merriam Webster: "To publicly identify or publish private information about (someone) especially as a form of punishment or revenge." www.merriam-webster.com/dictionary/dox
140 Borneo Post. (2016, 7 May). Independent candidate Yeu facing charge under Communication and Multimedia Act 1998. Borneo Post. www.theborneopost.com/2016/05/07/independent-candidate-yeu-facing-charge-under-communication-and-multimedia-act-1998
141 Malaysia Internet Landscape Report, 2017.
142 Ibid.

PATTERNS ACROSS PAKISTAN, INDIA AND MALAYSIA

There are interesting patterns noted across the country reports of India and Malaysia and Internet Landscape Report of Pakistan. The emergence of these characteristics demonstrates the efficacy of APC-La Rue Framework while they illustrate the converging yet Leviathan patterns in the exercise of power by the governments. Some of these prominent facets are being discussed under this section. While compiling this summary report, it became clear that there is a lack of transparency at requests sent to intermediaries or ISPs for removal of the content and the motivations behind them by the government authorities of India, Pakistan and Malaysia.[143] It was also noted, in these three countries, that the suppression of political dissent in online spaces is another common feature, particularly blocking of the content, and censoring internet access. In India's case this was overwhelmingly done in the Indian administered Kashmir valley.[144] while in Pakistan's case, this is common in the case of discussion surrounding Baluchistan, and draconian Frontier Crimes Regulations, laws which deal with territories of Federally Administered Tribal Areas.[145] In Malaysia's case it was usually the hard hand exercised by government to silence its critics.[146] With respect to the invocation of legal grounds, the text of Section 37 of PECA 2016 in Pakistan[147] and Section 69A of the Information Technology Act 2000 (as amended in 2008) in India hold some common ground justifying the need for blocking or removing online content.[148]

In terms of access it was found that India[149] and Pakistan[150] required considerable amounts of investment and interventions to facilitate equitable and equal access to quality internet services to the public whereas Malaysia ranked better. However with respect to the access to computers, it was observed that there remains a discrepancy to equal access to computers among the public.[151]

143 Malaysia Country Report, 2017.
144 Internet Shutdown Tracker. internetshutdowns.in
145 Baig, A., & Khan, S. (2015). Op. cit.
146 Malaysia Country Report, 2017.
147 www.na.gov.pk/uploads/documents/1470910659_707.pdf
148 India Country Report, 2017.
149 Ibid.
150 Pakistan Internet Landscape Report, 2017.
151 Malaysia Country Report, 2017.

It was also noted that in India[152] and Pakistan's case there was limited protection for intermediary liabilities. In the latter's case this development came after the enactment of the PECA 2016 which offered limited protection to intermediaries. [153]

The three distinct studies also revealed the presence of only limited legal provisions for privacy in India, Pakistan and Malaysia. However, more legislative and executive mechanisms and measures are required to address the issues. In Malaysia's case Personal Data Protection 2010[154] offers limited provision of privacy, while in Pakistan PECA 2016 also offers limited privacy protection.[155] It has also been learned that the law enforcement authorities enjoy considerable powers in Malaysia (under section 116 B of the Criminal Procedure Code)[156] and in Pakistan under PECA 2016[157] to solicit passwords from users for access to their hardware, software and other digital accounts to assist in prosecution of the alleged suspects or persons under investigation.

Moreover, it was noted that there exists an environment of impunity for the non-state actors in Pakistan, particularly non-state actors that are critical of bloggers or political commentators and threaten with either allegations of blasphemy or with threats to a person's life, property and family.[158] A common feature is observed in Malaysia where non-state actors enjoy impunity in attacking opposition and critics of the government.[159]

152 India Country Report, 2017.
153 Pakistan Internet Landscape Report, 2017.
154 Malaysia Country Report, 2017.
155 Pakistan Internet Landscape Report, 2017.
156 Malaysia Country Report, 2017.
157 www.na.gov.pk/uploads/documents/1470910659_707.pdf
158 Baig, A., & Khan, S. (2015). Op. cit. and Pakistan Internet Landscape Report, 2017.
159 Malaysia Country Report, 2017.

CHAPTER 2

COUNTRY REPORT: PAKISTAN

EXECUTIVE SUMMARY

With the introduction of 3G and 4G technology, access to the internet has become easier and Pakistan has seen a drastic increase in internet users over the past year. Pakistan currently stands 11th globally in terms of cellular subscribers. However, internet dispersion is still low when compared to the world and Asian average.

Civil society and digital rights groups are concerned about the passing of the Prevention of Electronic Crimes Act (PECA), which they fear will be misused by the authorities. While Pakistan continues to block pornographic websites, several other websites have become collateral damage during the process.

Online blasphemy still remains one of the biggest issues for freedom on the internet. Five bloggers abducted in January this year were accused of blasphemy online and four of them had to flee the country. The government is currently in negotiation with Facebook regarding "blasphemous content" present on the platform after an Islamabad High Court Judge threatened to ban social media if the issue was not resolved. It has become increasingly dangerous to criticise the military because of an organised crackdown by the Federal Investigation Agency against those critical of the military on the internet.

Service providers are now immune from violations committed by their users, but they are also now required by law to retain traffic data for at least one year and must cooperate with law-enforcement officials – from the Federal Investigation Agency (FIA) as well as Inter-Services Intelligence (ISI) – to carry out court-warranted access to data or surveillance. This raises concerns about censorship and silencinga of dissenting opinions with legal and social vigilantism. The fears are worsened by the country's first death sentence for online blasphemy, a propaganda campaign calling for the hanging of four liberal internet activists during their "disappearance", and an ad campaign asking citizens to report blasphemy on social media about the same time as the lynching of a university student over false blasphemy allegations. Media cells operated by rival political parties engage in highly charged online debates, but their criticism of the military led to a controversial crackdown by the FIA. Concerns related to the new internet laws led to a UN Human Rights Council probe on internet rights in Pakistan.

Prone to international espionage and malware attacks – such as the WannaCry ransomware cryptoworm attack that corrupted land record data in Punjab in May this year – the country still lacks a comprehensive data protection policy. Among the sources of attacks are hackers from India engaged in cyber warfare with hacker groups from Pakistan. Two new submarine cable connections in less than a year have diversified Pakistan's connectivity, but two major countrywide service disruptions this year show that the country's internet infrastructure is still vulnerable. Major disruptions in cellular services came from the government itself, which occasionally shuts off mobile networks in parts of the country as a safety precaution against terrorism.

Internet policy in Pakistan is overseen by the Ministry of Information Technology and Telecommunications, but FIA's new

mandate to fight cybercrimes translates into the involvement of the Ministry of Interior, which was at the forefront of a campaign this year against social media content deemed blasphemous. In an unprecedented case, a counterterrorism agent engaged a Shia man in a religious debate under cover, resulting in a death sentence for the latter on charges of online blasphemy. The FIA was also accused of suppressing political opposition after it clamped down on internet campaigners for ridiculing the military. PTA too carried out an SMS campaign asking people to report cases of blasphemy on the internet. In the absence of a transparent set of rules the authority is still allowed to arbitrarily censor internet content.

METHODOLOGY

9/11 and the wave of terrorist attacks since 2014 compelled a change in the extension of powers to different government institutions and authorities, which mandated the need for a research report which would deal with wider set of ongoing and emerging issues in the internet landscape. Pakistan published a research report titled "Expression Restricted: The Account of Online Expression in Pakistan" in 2015 under the IMPACT project.[160] The objective of the report was to monitor and assess the state of freedom of expression and the restrictions that were imposed by different sets of legislative and executive measures in Pakistan in online and offline spaces. However, the recently developed legislative framework has produced undesired consequences for the state of freedom of expression, association and assembly, and the right to information.

The research report found that there was an absence of legal measures and mechanisms for protection of Freedom of Expression, and pointed toward the need to address legal hurdles and restrictions such as stipulations in Article 19 and across various laws in the Pakistan Penal Code; many of these restrictions are against the spirit of ICCPR and Pakistan's international obligations.[161]

Additional issues that required further investigation with respect to restriction on free expression were discussions on Baluchistan and Frontier Crimes Regulations (FCR). The latter laws exclude the region of FATA from being included in the judicial and legislative system prevalent across Pakistan. It was also noted that issues associated with the fragile political structure and national security threats faced severe and considerable restrictions. The report further found that journalists and bloggers faced significant threats of harm particularly if their expressions were religious in nature. The threats often consisted of accusations of blasphemy and death threats.[162]

The report highlighted another concern, which was the emerging trend and incorporation of counter-terrorism within legislation of criminal and penal laws which could potentially jeopardise civil liberties in online spaces. It also cited obstacles which inhibit the development of an effective freedom of expression (FoE), right to information (RtI) and freedom of association and assembly (FoAA) narrative. The report also brought to the fore the increase in hate-speech related content against the Ahmadi community in Pakistan in social media and on the web. It pointed to the near vacuum of counter-narrative to such hate-speech and the need for protection of their civil liberties.[163]

---

160 Baig, A., & Khan, S. (2015). Expression Restricted: The Account of Online Expression in Pakistan. https://www.apc.org/sites/default/files/Expression-Restricted.-An-account-of-online-expression-in-Pakistan.pdf
161 Ibid
162 Ibid
163 Ibid

The report's recommendations were targeted primarily at policy makers and potential stakeholders within the government, regulators and political parties. However, for the government these recommendations underscored and called for the review of laws to address ambiguity surrounding terms such as "decency", "morality" and "reasonable" across different legislation which could affect FoE online. Furthermore, it called on the federal government to meet its international obligations on FoE, FoAA, including compliance with the FoE recommendations in the previous UPR. Similarly, it urged the government to report to the Human Rights Commission in obligations under the ICCPR. It also called on the government to address the rising trend of the misuse of blasphemy laws, particularly 295-A. On internet governance, it recommended the government to adopt a multi-stakeholder approach involving civil society, media and other stakeholders for protection of internet-related human rights.[164]

For regulators, the report recommended the need for mechanisms to make public the list of blocked websites and the reasons justifying such action. It additionally suggested to the regulators the need for transparency when blocking content on the web, the need for maintaining access to communication at all times, and the need for the protection of journalists and bloggers by ending impunity and putting in place safeguards, measures and mechanisms for the pursuit of cases in a court of law. The report recommended implementing more lenient measures for blocking online content and the need for introducing transparent public mechanisms for unblocking content which would have been previously blocked.[165]

Lastly, the report urged political parties to include internet-related human rights as part of their manifestos and mandates when elected to the respective parliaments.[166]

The current report "Internet Landscape of Pakistan 2017" serves as an extension and update of the 2015 report "Expression Restricted: The Account of Online Expression in Pakistan". This new report deals with a wider set of ongoing issues in Pakistan. As a result, by applying the APC-La Rue Framework, Pakistan's internet landscape report critically studies different developments under different indicators by analysing case studies of prominence in the media. Another reason to commission a study which deals with a wider set of issues is that the government enacted the Prevention of Electronic Crimes Act in 2016. Despite several beneficial clauses, this legislation has produced instances of unreasonable application of law in certain areas, such as religious-associated expression in online spaces, and indiscriminate blocking of internet content from Pakistan and outside in tandem with previous legal provisions. It was important to document these developments in a report.

Moreover, different executive measures were exercised which resulted in temporary yet crucial loss of access to the internet and mobile services. "Access" was one area which was not included in the 2015 "Expression Restricted" report and is a part of the current "Internet Landscape of Pakistan 2017" report.

The report is based on extensive study as well as interviews with different stakeholders of internet governance in Pakistan.

164 Ibid
165 Ibid
166 Ibid

SECTION 1

1. ACCESS TO INTERNET

In the 2015 report, internet penetration ranged from 10.8% to 17%. As of 2016, there were 34,342,400 internet users in Pakistan, which is 17.8% of the total population, marking an increase of 1.2% since 2015.[167] According to the CIA Factbook on Pakistan, the estimated internet penetration in Pakistan until July 2015 was 18%, as opposed to 10.8% in 2014.[168]

Pakistan is one of the least connected countries, as demonstrated by the global internet penetration figures, which stood at 46.1% in 2016.[169] The 17.8% penetration rate is too low, even when compared with the average penetration in Asia, which as of March 2017 is 45.2%.[170] A 2016 report by International Telecommunication Union (ITU) revealed that Pakistan, with 18% internet penetration, was among the least connected countries in the world, along with many African countries.[171]

The number of 3G and 4G subscribers in 2016 doubled in 2015 according to the PTA data, which shows 31.78 million subscribers, as opposed to 14.61 million in 2015.[172] The latest figure by the Pakistan Telecommunication Authority (PTA) shows that the number of 3G subscribers as of May 2017 is 41.7 million.[173]

According to the Pakistan Telecommunication Authority, the total number of cellular subscribers reported till May 2017 was 140,516,259.[7] According to the CIA World Factbook, Pakistan has the 11th largest number of cellular subscribers in the world.2 The number of broadband subscribers has also seen rapid increase from July 2016 (34.4 million) to May 2017 (44.3 million).[7] This a significant increase when compared with the 2.6 million broadband subscribers quoted in the Internet Landscape Report of 2013. As of 2014, there were 50 internet service providers (ISPs), with PTCL having the largest network of undersea cables.[174] Pakistan's Minister of State of Information Technology, Anusha Rehman, announced in April 2017 that Pakistan would be the first country in South Asia to test 5G services. However, no practical steps have yet been taken in this regard.[175]

The Freedom on the Net 2016 report by Freedom House ranked Pakistan's status as "Not Free" with an overall ranking of 69/100 on the scale of 0 (most free) to 100 (least free). Pakistan ranked 18/25 in terms of obstacles for citizens to access the internet, showing a little improvement from 2015 when the score was 20/25.[176]

167 www.internetlivestats.com/intern et-users/pakistan
168 www.cia.gov/library/publications/the-world-factbook/geos/pk.html
169 www.internetlivestats.com/internet-users
170 www.internetworldstats.com/stats.htm
171 Attaa, A. (2016, 25 July). Pakistan Among Countries With Lowest Internet Penetration: ITU. Propakistani. https://propakistani.pk/2016/07/25/pakistan-among-countries-with-lowest-internet-penetration-itu
172 Chaudhry, H. (2016, 24 August). 3G and 4G mobile internet users cross 30m milestone. Dawn.com. www.dawn.com/news/1279886
173 www.pta.gov.pk/index.php?Itemid=599
174 www.ispak.pk
175 Yasin, A. (2017, 12 April). Pakistan to be the first country in South Asia to test 5G services. Dawn.com. www.dawn.com/news/1326401
176 https://freedomhouse.org/report/freedom-net/2016/pakistan

According to Freedom House, the digital divide has persisted in Pakistan due to low literacy, difficult economic conditions and cultural resistance. Internet access for girls and women is increasing gradually, although online harassment serves as a deterrent for women to use the internet.[177]

As per the Pew Research Center, 20% of the internet users in Pakistan agreed that internet was a good influence in a Pew Global Attributes Survey published in 2015. Meanwhile, 31% of the respondents felt it was a bad influence and 43% had refused to answer the question. Pakistan was ranked to be the lowest among the 32 countries surveyed where internet was thought to have a good influence on politics, economics, education and personal relationships.[178]

1.2 BLOCKING AND FILTERING

The Pakistani government continues to censor content available online with a specific focus on blocking supposedly pornographic, blasphemous and anti-state content.[179]

The National Assembly of Pakistan passed the Prevention of Electronic Crimes Act (PECA) on 11 August 2016 after the Senate unanimously passed it on 29 July with 50 amendments. While members of opposition parties criticised the bill, suspecting the authorities would misuse it, the IT Minister Anusha Rehman rejected the criticism from NGOs as having "a certain agenda".[180]

PECA has been criticised by digital rights activists for being too vague and ambiguous. Section 34 of PECA empowers the Pakistan Telecommunication Authority (PTA) to "remove or block… information through any information system if it considers it necessary in the interest of the glory of Islam or the integrity, security or defence of Pakistan or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence under this Act". [181]

Before the enacting of PECA, telecommunications policy approved in 2015 uses similar language regarding the blocking of content. The 2016 Freedom on the Net report notes: "Section 9.8.3 states that the PTA will be enabled to 'monitor and manage content including any blasphemous and pornographic material in conflict with the principles of Islamic way of life as reflected in the Objectives Resolution and Article 31 of the Constitution' as well as material that is considered to be 'detrimental to national security, or any other category stipulated in any other law.'"[182]

The FotN (Freedom on the Net) report also discusses state and non-state actors exerting extra-legal pressure on content producers to take down content in online spaces. The report notes that a blanket ban on pornographic, allegedly blasphemous and anti-state content has resulted in blocking of several legitimate websites as well.

A localised version of YouTube with the domain Youtube.pk was launched last year in January after remaining blocked for years. According to PTA, the block was lifted after Google provided a process through which the offensive content could be reported directly to the company, which would be obliged to restrict it.[183] Digital rights activists expressed their concerns regarding the government's agreement with Google to restrict certain content. In a statement, Bytes For All said: "The enactment of this law criminalises a wide range of speech online, including legitimate

177 Ibid
178 Pew Research Center. (2015, 19 March). Internet Seen as Positive Influence on Education but Negative on Morality in Emerging and Developing Nations. www.pewglobal.org/2015/03/19/internet-seen-as-positive-influence-on-education-but-negative-influence-on-morality-in-emerging-and-developing-nations
179 Human Rights Watch. (2017, 26 May). Pakistan: Internet Crackdown Intensifies. www.hrw.org/news/2017/05/26/pakistan-internet-crackdown-intensifies
180 Khan, R. (2016, 11 August). Cyber crime bill passed by NA: 13 reasons why you should be worried. *Dawn.com.* www.dawn.com/news/1276662
181 www.na.gov.pk/uploads/documents/1470910659_707.pdf
182 https://freedomhouse.org/report/freedom-net/2016/pakistan
183 BBC. (2016, 18 January). Pakistan unblocks access to YouTube. *BBC.* www.bbc.com/news/world-asia-35345872

political and religious expression, with harsh prison sentences and fines. It also gives broad and sweeping powers to the government and law-enforcement agencies to surveil on citizens and censor their online expression, with little recourse for appeal."[184]

Facebook also complies with the government's requests to block online content. This compliance has shown a rapid increase. From June 2014 to December 2014, 42% of the requests out of the total 100 were censored. Comparatively, from July 2016 to December 2016, the government sent 1,002 requests for compliance, of which 67.56% were accepted by Facebook, showing an increasingly frequent cooperation between the government of Pakistan and Facebook.[185] A Facebook team visited Pakistan recently and held meetings with then Interior Minister Chaudhary Nisar Ali Khan over resolving the issue of blasphemy on Facebook. However, the team did not meet with any civil societies to address their concerns.[186]

Five social media activists and bloggers went missing in January this year. Among them were Salman Haider, Ahmad Waqas Goraya, Aasim Saeed, Ahmed Raza Naseer and Samar Abbas.[187] The Guardian reported that the missing activists had "outspoken, secular and anti-military views".[188] Right after the news of their abduction emerged, they were accused by certain websites and social media pages of having committed blasphemy and Twitter trends like #HangSalmanHaider called for their heads.[189] One of the bloggers – who was released after 21 days – accused the country's military of having planned and executed their abduction.[190]

The abduction of bloggers was the start of the state-sponsored crackdown on social media. A judge at Islamabad High Court threatened to ban all social media if the blasphemous content was not eliminated.[191]

In the past, Pakistan has blocked several websites citing similar reasons. In 2014, Twitter blocked "blasphemous content" upon the request of the Pakistani government. The decision, however was revoked a month after the mounting criticism by rights activists due to the "absence of additional clarifying information from Pakistani authorities."[192] Around the same time, Facebook also blocked Pakistani users from accessing several left-wing pages, and that of a rock band, Laal.[193]

In 2015, Pakistani authorities reportedly blocked WordPress, as the users were unable to access it through major ISPs, causing uproar among the public. Pakistan Telecommunication Authority did not confirm at the time if the website had been blocked officially.[194]

The government placed Pakistan Telecommunication Authority, along with several other regulators under the

184 Bytes for All. (2016, 8 November). Pakistan's new cyber-crime law set to raise havoc for political expression and religious expression. content.bytesforall.pk/node/196
185 https://govtrequests.facebook.com/country/Pakistan/2016-H2/
186 ARY News. (2017, 16 March). Facebook team to visit Pakistan to discuss blasphemous content issue. *ARY News*. https://arynews.tv/en/facebook-delegation-to-visit-pakistan-to-discuss-blasphemous-content-issue/
187 IFEX. (2017, 10 January). Four bloggers, social media activists go missing. *IFEX*. www.ifex.org/pakistan/2017/01/10/bloggers_activists_missing
188 Boone, J. (2017, 10 January). Disappearances spark fear of crackdown on leftwing dissent in Pakistan. *The Guardian*. www.theguardian.com/world/2017/jan/10/pakistan-military-critics-dissapearances-dissent-crackdown
189 Shams, S. (2017, 16 January). From 'abduction' to blasphemy allegations – What's in store for Pakistan's missing activists? Deutsche Welle. www.dw.com/en/from-abduction-to-blasphemy-allegation-whats-in-store-for-pakistans-missing-activists/a-37146225
190 BBC. (2017, 9 March). Pakistan activist Waqas Goraya: The state tortured me. *BBC*. www.bbc.com/news/world-asia-39219307
191 Shehzad, R. (2017, 7 March). Blasphemy: IHC directs authorities to block all social media if necessary. *Express Tribune*. https://tribune.com.pk/story/1348784/ihc-directs-authorities-block-social-media-necessary
192 AFP. (2014, 18 June). Twitter restores access to block content in Pakistan. (June 18, 2014). *Dawn.com* www.dawn.com/news/1113542
193 Walsh, D., & Masood, S. (2014, 6 June). Facebook under fire for temporarily blocking pages in Pakistan. *The New York Times.* www.nytimes.com/2014/06/07/world/asia/pakistan-facebook-blocked-users-from-political-pages-and-outspoken-rock-band-laal-against-taliban-.html
194 Dawn. (2015, 23 March). Blogging website WordPress blocked? *Dawn.com.* www.dawn.com/news/1171304

control of relevant ministries. However, the notification was later revoked by the Islamabad High Court.[195]

Pakistan Telecommunication Authority was given the power to block online content after the Islamabad High Court banned the controversial Inter-Ministerial Committee for Evaluation of Websites (IMCEW). For years, IMCEW, represented by several ministries and security agencies was responsible for determining the content that was to be blocked in Pakistan. Neither the names of its members, nor the details of its operations were ever made public.[196]

PTA was directed in 2015 to formulate a web content management mechanism. Its purpose was ensuring the basic rights of citizens and "the participation of relevant stakeholders in evaluation of complaints and decisions thereon will be ensured. A mechanism for redressal of grievances for affected users will also be provided. To ensure effectiveness of the content management system, PTA will also adequately strengthen its web monitoring cell".[197] However, little is known about the extent to which PTA follows these directives due to lack of transparency.

As the government increasingly attempts to censor content online, the Pakistani public is generally against unbridled access to the internet, especially when it comes to matters related to religion. A 2015 Pew Global Attitudes survey on freedom on the internet found out that only 25% of Pakistanis supported an uncensored internet, making the censor's task easy.[198]

1.2.1 Pornography

Pornographic content remains officially blocked in Pakistan under the Pakistan Telecommunications Act of 1996[199] which orders blocking of all sorts of content vaguely defined as "obscene".

After a Supreme Court order to block all websites having "obscenity and pornography that has an imminent role to corrupt and vitiate the youth of Pakistan", the PTA instructed ISPs in January 2016 block 400,000 "offensive" websites at the domain-level.[200]

A news report explaining this blanket ban said: "Like Tumblr, most of the list comprises sites blocked at the domain level i.e. all pages hosted on the domain would be blocked, rather than blocking specific content or pages hosted on a domain."[201]

Digital rights activists have expressed their concern on such a ban. Some believed the ban was based on keywords and it was entirely possible that many other websites appearing on these keywords could also be blocked.

In April 2017, the Federal Investigation Authority arrested a man in Sargodha for filming child pornography for a client based in Norway. The action was taken after the Norwegian Embassy informed the FIA through a written letter.[202]

Due to the websites being blocked at domain level and through keywords, several websites not remotely connected to porn have also been blocked by PTA and due to the lack of transparency, very little is publicly known about the process.[203]

195 Asad, M. (2017, 28 March). IHC orders regulators out of ministries' control. Dawn.com. www.dawn.com/news/1323299
196 Haque, J. (2016). Pakistan's Internet Landscape 2016. Bytes for All. www.gp-digital.org/wp-content/uploads/2016/09/Pakistan_Internet_Landscape_2016.pdf
197 Haider, M. (2015, 21 March). PTA given powers for content management on internet. The News. www.thenews.com.pk/print/30534-pta-given-powers-for-content-management-on-internet
198 Wike, R., & Simmons, K. (2015, 18 November). Global Support for Principle of Free Expression, but Opposition to Some Forms of Speech. Pew Research Center. www.pewglobal.org/2015/11/18/global-support-for-principle-of-free-expression-but-opposition-to-some-forms-of-speech
199 www.na.gov.pk/uploads/documents/1329727963_180.pdf
200 AFP. (2016, January 26). Govt orders 400,000 porn sites blocked. Dawn.com. www.dawn.com/news/1235554
201 Haque, J. (2016, 25 May). Pakistan's impossible attempt to block 400,000 porn websites continues. Dawn.com. www.dawn.com/news/1260452
202 Tahir, Z. (2017, 13 April). Sargodha man planned to take children to Norway to film pornographic videos: FIA. Dawn.com. www.dawn.com/news/1326731
203 Ibid

1.2.2 Blasphemy

The crackdown on allegedly blasphemous content online has continued in the last year and has now expanded to offline spaces as well. The trend which started in 2003 has seen a large number of websites blocked. Among them were social media giants like Twitter, BlogSpot, YouTube and Facebook.

Five bloggers who were abducted in January 2017 were accused of operating an allegedly blasphemous page titled "Bhensa". An online campaign directed towards them asked for their hanging.[204] Four of the individuals, after their release, immediately left the country due to fear for their lives.[205] During their abduction, some reports suggested that the bloggers would be charged for blasphemy, but the Interior Minister Chaudhary denied these reports and denounced the blasphemy allegations against them.[206]

In March 2017, FIA arrested three individuals in a case related to online blasphemy.[207] After their arrest, Twitter hashtag #HangAyazNizami started trending in Pakistan.[208]

Mashal Khan, a journalism student at Abdul Wali Khan University was lynched to death by his fellow university students over an accusation of committing blasphemy on his social media profile.[209] It was subsequently revealed that his murder was planned by some university insiders who were not happy with Mashal Khan's criticism of the university administration.[210]

In the 2016 Freedom on the Net report Freedom House noted that social media users exercised extra caution and self-censorship while opining on the matters related to religion and blasphemy. The blasphemy cases, which can be reported by any citizen against another, are often used to settle personal scores; digital media has become the most popular platform for that.[211]

In September 2016, a 16-year-old boy was arrested from Sheikhupura over allegedly sharing a derogatory picture of a Muslim holy place. He remains in jail (September 2017).[212] Similarly, a First Information Report was registered against Shaan Taseer – a human rights activist and son of the slain governor Punjab Salmaan Taseer for alleged "hate speech" after he sent out Christmas greetings in a video message. Sunni Tehreek, a Barelvi group associated with Mumtaz Qadri requested Shaan Taseer be booked under Section 295-A of the Pakistan Penal Code (PPC).[213]

Rights activists believe the state's hunt against alleged blasphemers online has resulted in increased mob violence. Millions of Pakistanis were sent text messages by the PTA, warning them against sharing "blasphemous content" online and encouraging the public to report such content immediately to PTA.[214] A spokesperson of PTA revealed that the messages were sent out on court orders. Judge Shaukat Aziz Siddiqui of Islamabad High Court had earlier threatened to ban social media if the issue of blasphemy was not resolved. He requested the establishment a "Muslim-only" Joint Investigation Committee

204 Radio Free Europe/Radio Liberty. (2017, 19 January). Missing Pakistani activists hit by 'malicious' blasphemy charges, families say. www.rferl.org/a/missing-pakistani-liberal-activists-hit-by-malicious-blasphemy-charges-families-say/28242577.html
205 Zahra-Malik, M. (2017, 29 January). Second missing Pakistani blogger found, leaves country fearing for life: family. *Reuters.* www.reuters.com/article/us-pakistan-activists-idUSKBN15D0DB
206 APP. (2017, 20 January). Propaganda against missing bloggers angers Nisar. *Dawn.com.* www.dawn.com/news/1309527
207 Jami, A. (2017, 24 March). FIA arrests three in social media blasphemy case. *Dawn.com.* www.dawn.com/news/1322531
208 https://twitter.com/hashtag/hangayaznizami?lang=en
209 Rasmussen, S. E., & Baloch, K. (2017, 26 April). Student's lynching sparks rare uproar in Pakistan over blasphemy killings. *The Guardian.* www.theguardian.com/world/2017/apr/26/lynching-of-a-student-sparks-uproar-in-pakistan-against-blasphemy-laws
210 The Nation. (2017, 4 June). Mashal Khan's murder was pre-planned: JIT report. *The Nation.* nation.com.pk/national/04-Jun-2017/mashal-khan-s-murder-was-pre-planned-jit-report
211 https://freedomhouse.org/report/freedom-net/2016/pakistan
212 Ghyas, S. (2016, 19 September). Blasphemy law: Nabeel Masih, a Christian teenager, has been arrested for liking the Kaaba's picture on Facebook. The Nation. expressnation.com.pk/blogs/20-Sep-2016/blasphemy-law-nabeel-masih-a-christian-teenager-has-been-arrested-for-liking-the-kaaba-s-picture
213 Tanveer, R. (2017, 31 December). Shaan Taseer booked for hate speech following Christmas message. *Express Tribune.* https://tribune.com.pk/story/1280484/shaan-taseer-booked-hate-speech-following-christmas-message/
214 AFP. (2017, 10 May). Millions of Pakistanis receive blasphemy warning texts. *Times of India.* timesofindia.indiatimes.com/world/pakistan/millions-of-pakistanis-receive-blasphemy-warning-texts/articleshow/58614233.cms

to probe into the issue of blasphemy.[215]

With these statements by a senior judge, followed by the action taken against alleged blasphemers, the risk of emboldening the extremists to take the law in their own hands can increase.

1.3 INTERMEDIARY LIABILITY

Service providers in Pakistan are no longer liable for civil or criminal violations committed by their users, unless there is evidence that they made a wilful attempt to participate in those offences.[216] The burden of proof, if such an allegation is made, is on the accuser, according to the new Prevention of Electronic Crimes Act of 2016.[217] If a service provide is made aware of an investigation against a client, it can notify the user after a gag period of 14 days (that a court can extend), and has the legal right to disclose any user data for such a probe.

Importantly, intermediaries are under no obligation to proactively monitor the content they host or transmit for their users to ensure no law is being broken, as long as they provide their service "in good faith".

In the past, Pakistani authorities have banned popular international online platforms entirely because of their inability to regulate offensive content.[218] A court hearing a petition against the 2012 ban on YouTube was told that its parent organisation Google would not incorporate in Pakistan because there were no laws to protect online platforms from being held liable for any offences committed by their users. The court offered to issue a temporary order assuring the company of limitation of liability until laws were made,[219] but YouTube launched a localised version months before the new law was passed, bypassing the concern of intermediary liability with a mechanism to allow PTA to send censorship requests directly to Google.[220]

1.4 NET NEUTRALITY

Pakistan's internet laws do not protect net neutrality. It is not clear if the country's competition laws or consumer rights protections can safeguard against discriminatory practices by internet service providers.

Some of Pakistan's cellular phone service providers offer controversial Facebook-led services like Free Basics and Facebook Zero, which have raised net neutrality concerns elsewhere in the world.[221]

Mobilink's Jazz service offers Facebook Zero,[222] which allows free access to a text-only version of the social media giant's website. Free Basics – a service that allows free access to a selection of websites, not including those of Facebook's rivals – is offered by Telenor[223] and Zong.[224] Ufone, the only remaining mobile phone service provider, offers free access to specific web services as part of its data packages.[225]

Unlike in the neighbouring India, where Facebook had to pull the Free Basics service

215 AFP. (2017, 9 March). IHC judge threatens to block social media over 'blasphemy'. Newsweek Pakistan. expressnewsweek-pakistan.com/ihc-judge-threatens-to-block-social-media-over-blasphemy/
216 www.na.gov.pk/uploads/documents/1470910659_707.pdf
217 Ibid
218 Dawn. (2017, 21 June). Could it happen again? Remembering Pakistan's Facebook, YouTube ban. Dawn.com. www.dawn.com/news/1320650
219 Jajja, S. (2013, 15 May). YouTube ban: Google to appear before Lahore High Court. Dawn.com. www.dawn.com/news/1027189
220 Junaidi, I. (2016, 19 January). YouTube returns to Pakistan. Dawn.com. www.dawn.com/news/1233960
221 Vincent, J. (2016, 8 February). Facebook's Free Basics service has been banned in India. The Verge. www.theverge.com/2016/2/8/10913398/free-basics-india-regulator-ruling
222 expressm.jazz.com.pk/smart/free-sites.html
223 www.telenor.com.pk/freebasics-com
224 www.zong.com.pk/internet/mobile-internet/internet-promotions/facebook-freebasics
225 www.ufone.com/data/tariff/prepaid

amid controversy, there has been little debate on net neutrality in Pakistan.[226]

1.5 NETWORK DISCONNECTION

By 2016, Pakistan was connected to four submarine cables through two operators with landing rights. PTCL was linked to Sea-Me-We-3 (with a design capacity of 480gbps), Sea-me-we-4 (1.28tbps) and I-Me-We (3.86tbps), while Transworld Associates (TWA) was connected to the 1.28tbps submarine cable TW1.[227]

TWA enhanced its capacity significantly with the completion of Sea-Me-We-5 in December 2016. It was part of a 16-company consortium that built the cable with a capacity of 24tbps.[228]

5 July 5 2017, after several days of trouble at TWA, the resulting shift in its traffic to PTCL caused a brief disruption. A day later, on 6 July, a cable fault in Sea-Me-We-4 resulted in a countrywide slowdown. (A breakdown in Sea-Me-We-4 had caused a similar countrywide congestion in June 2015).[229] PTCL claimed it was able to solve the problem in a day.[230]

This was possible because around the same time, the operator had connected to the new 40tbps submarine cable AAE-1, seen as part of the one-belt-one-road initiative.[231] Work on a project to bring a fibre-optic cable via a land route from China, part of the larger Pakistan-China-Economic-Corridor program, began in 2016.[232]

5 August 2017 damage to the I-Me-We cable near Jeddah slowed down internet services across the country for hours.[233]

Disruptions were also reported because of inland fibre-optic cable breakdowns. A network outage at PTCL, because of a cable fault within Pakistan, resulted in a drop in internet speeds and some service outages for customers of PTCL and Ufone in December 2016.[234] In June 2017 internet, telephone and ATM users in Chiniot and nearby towns were left without services for hours after PTCL cables were damaged.[235]

It has now become a standard practice for government authorities to temporarily shut down mobile phone services in various parts of Pakistan as a security precaution, especially on occasions of religious or national gatherings prone to terrorist attacks.

In most parts of FATA, where the military is still campaigning against the Taliban and other militant groups, mobile phone services were shut down for security reasons on 15 March 2017 and had not been reopened by July,[236]

226 Doval, P. (2016, 11 February). Facebook withdraws the controversial 'Free Basics' platform from India. GadgetsNow.com. www.gadgetsnow.com/tech-news/Facebook-withdraws-the-controversial-Free-Basics-platform-from-India/articleshow/50947427.cms

227 Baloch, F. (2015, 8 March). Broadband connectivity: New cable to provide faster access for consumers, businesses. *Express Tribune.* expresstribune.com.pk/story/849956/broadband-connectivity-new-cable-to-provide-faster-access-for-consumers-businesses/

228 TR Pakistan. (2016, 19 December). Pakistani internet bandwidth to increase by 24Tbps. *Dawn.com.* www.dawn.com/news/1303258

229 GEO. (2015, 25 June). Fault in submarine cable impacts internet services in Pakistan. *The News.* www.thenews.com.pk/latest/5711-fault-in-submarine-cable-impacts-internet-services-in-pakistan

230 Attaa, A. (2017, 7 July). After Cable Cut, Internet in Pakistan is Back to Normal: PTCL. *ProPakistani.* https://propakistani.pk/2017/07/06/internet-slow-due-submarine-fault-ptcl

231 APP. (2017, 2 July). AAE-1 submarine internet cable linking Asia, Africa and Europe starts operations. *Dawn.com.* www.dawn.com/news/1342780

232 cpec.gov.pk/progress-update

233 Shahid, J. (2017, 6 August). Undersea cable fault strangles internet services. *Dawn.com.* www.dawn.com/news/1349860

234 Rehman, D. (2016, 26 December). Technical fault in PTCL fibre optics causes massive Internet outage across Pakistan. *Daily Pakistan.* en.dailypakistan.com.pk/headline/underwater-cable-damage-causes-massive-internet-outage-across-pakistan

235 The Nation. (2017, 19 June). Damage to fibre cable disrupts telecom services. *The Nation.* expressnation.com.pk/national/19-Jun-2017/damage-to-fibre-cable-disrupts-telecom-services

236 MENAFN. (2017, 18 June). Pakistan - Suspension of mobile phone services creates problems for tribesmen. *MENAFN.* www.menafn.com/1095566087/Pakistan--Suspension-of-mobile-phone-services-creates-problems-for-tribesmen

when the federal government announced it would restore connectivity in phases.[237]

In Islamabad and Rawalpindi, cellular phones were suspended on Independence Day,[238] and were shut down without prior warning several times ahead of Pakistan Day (23 March) military parade, since the rehearsals of the event are also a likely terrorist target.[239]

The practice is now a typical part of security plans in various parts of the country on days of religious commemorations, such as the 9th and 10th of the month of Muharram,[240] [241] Youm-e-Ali,[242] and Chehlum,[243] when Shia gatherings are especially vulnerable to terrorist attacks.

The government argues that it has a legal right to suspend cell phone services for reasons of security of citizens, in line with section 54 of the Pakistan Telecommunications (Reorganization) Act of 1996, which allows it to "exercise preference and priority" in order to ensure "defence and security of Pakistan". An Islamabad High Court judge hearing a plea against the practice remarked in January 2017 that the provision is specific to when a state of emergency has been declared.[244]

In the past, authorities in Islamabad have used the measure to stop controversial cleric Abdul Aziz from addressing worshippers on Fridays[245] and to disperse a crowd of protesters from religious groups who sat in for days in the capital's highly secure Red Zone.[246]

1.6 DATA PROTECTION

As Pakistan waits for a robust data protection law promised by the government, violations of individual privacy and stealing of business data are addressed by the 2016 law against cybercrimes. After government departments were hit by a ransomware attack in May this year, concerns were raised about a broader initiative to better protect government and citizen data.[247]

Land record services were suspended in Punjab after a global ransomware cryptoworm attack in May corrupted a government department's information system.[248] This was seen as a matter of concern in a country where the government keeps large-scale biometric data of all its citizens. According to Digital Pakistan Policy, an agenda document released this year, concerns about privacy and security of sensitive government data could both be addressed with a comprehensive data protection law.[249] The minister for information technology promises the proposed law will balance individual privacy concerns with business interests.[250]

237 MENAFN. (2017, July 9). Pakistan - Govt decides to restore cellular, internet services in Fata. *MENAFN*. www.menafn.com/1095611510/Pakistan--Govt-decides-to-restore-cellular-internet-services-in-Fata
238 The News. (2016, 12 August). Mobile phone services to be suspended in Islamabad on August 14. *The News*. https://www.thenews.com.pk/latest/141997-Mobile-phone-services-to-be-suspended-in-Islamabad-on-August-14
239 Dawn. (2017, 20 March). Blackout of mobile phone services irks Islamabad, Pindi residents. *Dawn.com*. www.dawn.com/news/1321565
240 The News. (2016, 10 October). Mobile phone services to be suspended in KP on 9-10 Muharram. *The News*. www.thenews.com.pk/latest/156188-Mobile-phone-services-to-be-suspended-in-KP-on-9-10-Muharram
241 Mansoor, H. (2016, 30 September). Govt decides to suspend cellphone, internet services on Ashura. *Dawn.com*. www.dawn.com/news/1287002
242 Geo News. (2017, 16 June). Sindh bans pillion riding, mobile services on Youm-e-Ali. *Geo TV*. www.geo.tv/latest/145976-sindh-govt-bans-pillion-riding-heli-cams-on-youm-e-ali
243 Geo News. (2016, 21 November). Chehlum security: Mobile phone services restored in Karachi. *Geo TV*. www.geo.tv/latest/121103-Chehlum-Security-Ban-on-pillion-riding-in-Karachi-for-two-days-mobile-signals-suspended-in-cities
244 Shehzad, R. (2017, 18 January). Connection interrupted: Cellular services can only be suspended in 'emergency'. *Express Tribune*. https://tribune.com.pk/story/1298744/connection-interrupted-cellular-services-can-suspended-emergency
245 Dawn. (2015, 19 December). Mobile signals suspended for third Friday now. *Dawn.com*. www.dawn.com/news/1227313
246 Ali, I., Haider, I., & Bhatti, H. (2016, 28 March). Nearly 2,000 pro-Qadri protesters continue sit-in outside Parliament. *Dawn.com*. www.dawn.com/news/1248261
247 Dawn. (2017, 29 May). Data protection. Dawn.com. www.dawn.com/news/1335971
248 Butt, W. A. (2017, 22 May). Virus attack: Land record services suspended in Punjab. *Dawn.com*. www.dawn.com/news/1334613
249 moit.gov.pk/policies/DPP-2017v5.pdf
250 Ahmadi, A. (2017, 5 April). IT ministry to introduce DPA within three months. *Pakistan Today*. www.pakistantoday.com.pk/2017/04/05/it-ministry-to-introduce-dpa-within-three-months

Meanwhile, the Prevention of Electronic Crimes Act of 2016 criminalises unauthorised access to and copying of data and unauthorised interception of electronic communication.[251] Jail terms and fines are harsher if the hacker targets "critical infrastructures".

1.7 SURVEILLANCE AND LAWFUL INTERCEPTION

Although privacy is a fundamental right under Pakistan's constitution, and the country's law now requires a court to warrant any surveillance required for investigation of crimes, there are deep concerns about surveillance by government agencies.

Real-time collection of data to investigate an offence requires permission by a court, according to Section 36 of the Prevention of Electronic Crimes Act of 2016.[252] The specific offence and the type of data required need to be identified upfront, and there needs to be an assurance that privacy of other users will not be violated. The surveillance can be carried out for a maximum of seven days, unless a new permission is sought from the court. Unauthorised disclosure of someone's personal information may result in a prison sentence and fine unless the service provider or officer who obtained the information prove they were acting in good faith. Section 39 of the law allows the government to share information, electronic communications, or evidence with foreign governments, agencies and organisations, apparently without judicial oversight.

Service providers are required to retain traffic data for at least one year (or more, if the Pakistan Telecommunications Authority asks), under the new law. But investigation agencies require a court warrant to access such data.

The government had initially put the civilian Federal Investigation Agency in charge of investigation of cybercrimes, but in October, it allowed the military spy agency Inter-Services Intelligence the same powers.[253] In the middle of a drawn out war against terrorism with tech-savvy opponents, the government argues that it needs to carry out electronic surveillance to ensure security. But there are concerns that the vague words of the law will give them the right to suppress dissent.[254]

A 2013 report by Privacy International had said the ISI wanted to build a robust mass surveillance system, spanning across platforms, matching those of the US and the UK, with direct access to submarine cables.[255] Pakistan had procured surveillance tools from seven international companies for the purpose, including the German surveillance technology vendor Trovicor and its parent company Nokia Siemens Network.

Outed emails hosted on Wikileaks show Pakistan had discussed buying surveillance equipment from an Italian company that calls itself The Hacking Team.[256] But it was their rival German company FinFisher whose surveillance software was found to be operating in the country by a forensic probe by The Citizen Lab in April 2013.[257] Another report by the same organisation said Pakistan's PTCL was using Canadian packet-filtering software Netsweeper to filter websites with a technology that can also be used for surveillance.[258] The secrecy of these efforts has caused concern among civil rights activists.

251 www.na.gov.pk/uploads/documents/1470910659_707.pdf
252 Ibid
253 Gishkori, Z. (2016, 20 October). National security issues: Govt accepts ISI's role in checking cyber crimes. *The News.* www.thenews.com.pk/print/158580-Govt-accepts-ISIs-role-in-checking-cyber-crimes
254 Shah, B. (2016, 24 November). The vagaries of Pakistan's cybercrime law. *Al Jazeera.* expresswww.aljazeera.com/indepth/opinion/2016/11/vagaries-pakistan-cybercrime-law-161124082838234.html
255 Rice, M. (2015). Tipping the scales: Security and surveillance in Pakistan. *Privacy International.* www.privacyinternational.org/node/624
256 Haque, J., & Rehman, A. (2017, 22 June). Hacking Team hacked: The Pakistan connection, and India's expansion plan. *Dawn.com.* www.dawn.com/news/1196767
257 Marquis-Boire, M. et al. (2013). For their eyes only: The commercialization of digital spying. *The Citizen Lab.* https://citizen-lab.ca/storage/finfisher/final/fortheireyesonly.pdf
258 Dalek, J. et al. (2013). O Pakistan, we stand on guard for thee: An analysis of Canada-based Netsweeper's role in Pakistan's censorship regime. The Citizen Lab. https://citizenlab.ca/2013/06/o-pakistan/

1.8 SOCIAL SURVEILLANCE AND VIGILANTISM

In March 2017, a countrywide newspaper ad campaign by the FIA appealed to citizens to submit evidence of blasphemy carried out on social media.[259] Weeks later, a mob consisting largely of university students in Mardan beat up and shot a journalism pupil on campus over false allegations of online blasphemy.[260] The next month, millions of Pakistanis received text messages[261] and saw newspaper ads[262] from Pakistan Telecommunication Authority asking them to report incidents of blasphemy on social media. The campaign had been ordered by the Islamabad High Court, and caused concerns about "state-sponsored vigilantism". [263]

In July, a court sentenced a man to death for committing blasphemy on Facebook in the first such case in the country's history, after an undercover counterterrorism agent engaged him in a debate.[264] Months earlier, four liberal bloggers who were believed to be abducted by state security agencies in January, were the target of a largescale social media campaign in their absence, making unverified blasphemy allegations and asking for their death.[265]

A report by the Digital Rights Foundation released this year found that female journalists faced gendered surveillance from the state and society.[266] The social surveillance was frequent, and led to abuse including sexualised threats as well as attacks based on appearance and character.[267]

Amid fears of a rise in vigilantism in Pakistan in general,[268] there are concerns that mob behaviour on the internet can be especially serious, because unverified allegations travel fast on social media, and access to and spreading of personal information is easy.[269]

1.9 CYBER ARMIES

What is referred to as cyber warfare between hacker groups from India and Pakistan continues,[270] with a Pakistani group claiming to have hacked more than 7,000 Indian websites in October 2016.[271] In April 2017, after Pakistan sentenced to death an alleged Indian spy, an Indian group claimed they had taken over 30 websites belonging to the Pakistani government.[272] A Pakistani group of hackers claimed to have defaced 10 Indian websites[273] Indian hackers claimed to have

259 The Nation. (2017, 11 March). FIA releases ads against 'social media blasphemers'. *The Nation*. expressnation.com.pk/national/11-Mar-2017/fia-releases-advertisement-against-social-media-blasphemers
260 RT. (2017, 15 April). 'Skull caved in': Pakistani journalism student beaten to death for 'blasphemy'. RT. www.rt.com/news/384653-pakistan-student-beaten-to-death-journalism
261 RT. (2017, 11 May). Millions of Pakistanis sent govt blasphemy warning by text. RT. www.rt.com/news/387910-pakistan-text-messages-blasphemy
262www.pta.gov.pk/index.php?option=com_content&task=view&id=2303&Itemid=740
263 Ahmed, A. (2017, 17 July). Blasphemy: The Unpardonable Offense. *LobeLog Foreign Policy.* https://lobelog.com/blasphemy-the-unpardonable-offense
264 Rasmussen, S. E., & Wong, J. C. (2017, 22 July). Facebook was where Pakistan could debate religion. Now it's a tool to punish 'blasphemers'. *The Guardian.* www.theguardian.com/technology/2017/jul/19/facebook-pakistan-blasphemy-laws-censorship
265 Shams, S. (2017, 16 January). Op. cit.
266 Digital Rights Foundation. (2017). Surveillance of female journalists in Pakistan. https://digitalrightsfoundation.pk/surveillance-of-female-journalists-in-pakistan
267 Ibid
268 Kamal, D. (2017, 21 May). The rise of vigilantism in Pakistan. *The Citizen.* www.thecitizen.in/index.php/NewsDetail/index/1/10727/The-Rise-of-VigilantismIn-Pakistan
269 Dad, N. (2014, 26 November). Mob rule, vigilante behaviour and blasphemy in Pakistan's digital age. *TechPresident.* expresstechpresident.com/news/25359/blasphemy-digital-age
270 Shukla, P. (2017, 14 August). India-Pakistan Gear Up For Cyber Wars This I-Day. *Business World.* expressbusinessworld.in/article/India-Pakistan-Gear-Up-For-Cyber-Wars-This-I-Day/14-08-2017-124037/
271 Kumar, C. (2016, 5 October). 7,000 Indian sites hacked, claim Pak rookies. *Times of India*. expresstimesofindia.indiatimes.com/india/7000-Indian-sites-hacked-claim-Pak-rookies/articleshow/54686941.cms
272 Mail Today. (2017, 25 April). Indian hackers take down 30 Pakistan govt sites to avenge Kulbhushan Jadhav. *Business Today.* www.businesstoday.in/current/economy-politics/indian-hackers-take-down-30-pakistan-govt-sites-to-avenge-kulbhushan-jadhav/story/250705.html
273 Arora, K., & Ibrar, M. (2017, 27 April). It's just a trailer, says Pakistani hacker group that defaced 10 Indian websites. *The Economic Times.* expresseconomictimes.indiatimes.com/news/politics-and-nation/its-just-a-trailer-says-pakistani-hacker-group-that-defaced-10-indian-websites/articleshow/58391885.cms

hacked 500 Pakistani websites in response and said they would continue the assault.[274] The claims cannot be verified. On Pakistan's 70th Independence Day – 14 August 2017 – Indian hackers defaced websites belonging to several government ministries, and placed pictures of the Indian military and the Indian flag on them.[275]

"Suspected Pakistani and Chinese hackers" targeted midlevel Indian military officers in a malware attack in May 2017, using a phishing email that offered them a course in Sri Lanka.[276] The Indian home ministry warned android smartphone users in the country to delete four applications that they claimed Pakistani agencies were using to spy on Indians.[277] They included a gaming app named Top Gun, an entertainment app titled Talking Frog, and music and video apps Mpjunkie and Bdjunkie.

Political parties in Pakistan organise their own internet corps or cells, which engage in political attacks, push certain positions and narratives in social media, or participate in hashtag wars.[278] Little is known about how they operate, but a news report in September 2017 claimed that the PML-N's Strategic Media Communications Cell – set up in 2014 to counter similar tactics by their rival PTI – has 38 employees and volunteers and more than 250 official members.[279]

In May 2017, when a disagreement between the military and the government ended in reconciliation, supporters of PTI began a social media campaign very critical of the army, leading to a controversial FIA crackdown against tens of social media users[280] including members of PTI's social media force.[281] Two members of the PML-N media cell were also questioned by the authorities.[282]

At least 41 banned political, religious and terrorist organisations in the country also run hundreds of social media pages and accounts.[283] In January 2017, a large-scale robust social media propaganda campaign made dubious blasphemy allegations against four liberal internet activists who were believed to have been abducted by Pakistan's security agencies.[284]

1.10 CYBER ATTACKS

Pakistan's new electronic crimes law criminalises hacking, but with its vulnerable cybersecurity, the country is prone to international cyber-espionage and is one of the top targets of malware in the world.[285]

Unauthorised access to information systems or data, and unauthorised copying of data, are crimes under the new Prevention of Electronic Crimes Act of 2016.[286] Unauthorised interference with an information system or data, which covers denial of service attacks, is also punishable by jail time and fines. The sentences are harsher for attacks on "critical

274 NewsX. (2017, 26 April). Indian hackers cripple more than 500 Pakistan government websites; avenge Jadhav's penalty. *NewsX*. www.newsx.com/national/62284-indian-hackers-cripple-500-pakistan-government-websites-avenge-jadhavs-penalty
275 Ahmed, Z. (2017, 15 August). Indian hackers deface numerous Pakistani ministries websites. PakWired. https://pakwired.com/indian-hackers-deface-numerous-pakistani-ministries-websites
276 Dubey, A. (2017, 14 May). Suspected Pakistani, Chinese hackers target Indian Army officers' computers. *India Today*. expressindiatoday.intoday.in/story/pakistani-chinese-hackers-target-indian-army-officers/1/953352.html
277 ABP. (2016, 15 December). Home ministry asks users to delete 4 apps from smartphones. *ABP Live*. www.abplive.in/india-news/home-ministry-asks-users-to-delete-4-apps-from-smartphones-463200
278 Shah, B., & Shah, Z. (2017, 9 September). The PML-N's digital soldiers. *Geo TV*. www.geo.tv/latest/157329-the-pml-ns-digital-soldiers
279 Ibid
280 Wasim, A., & Tahir, Z. (2017, 22 May). FIA launches crackdown on 'anti-army campaigners'. *Dawn.com*. www.dawn.com/news/1334626/fia-launches-crackdown-on-anti-army-campaigners
281 Express Tribune. (2017, 17 May). Cyber crime: PTI social media activist in FIA custody. *Express Tribune*. https://tribune.com.pk/story/1412372/cyber-crime-pti-social-media-activist-fia-custody/
282 Ibid
283 Haque, J., & Bashir, O. (2017, 13 June). Banned outfits operate openly on Facebook. *Dawn.com*. www.dawn.com/news/1335561
284 Shams, S. (2017, January 16). Op. cit.
285 Chaudhry, H. (2016, 6 May). Pakistan top target of malware attacks worldwide, says Microsoft. *Dawn.com*. www.dawn.com/news/1256601
286 www.na.gov.pk/uploads/documents/1470910659_707.pdf

infrastructure". Writing, distributing and using malicious code is a separate offence in the law. But most of Pakistan's ISPs may not be capable of dealing with distributed denial-of-service-attacks in a sophisticated way, and its law enforcement is seemingly incapable of tracing hackers who use proxies.[287]

Amid growing reports of hacking, impersonation, harassment and blackmail on social media, especially targeting women,[288] the new law addresses not just electronic fraud and identity theft, but specifically criminalises what it calls offences against the dignity and modesty of people. These include intimidation using sexually explicit imagery, posting superimposed or actual sexually explicit imagery of someone, or cultivating someone to engage in a sexual act.[289] The sentences are harsher if the victim is a minor. In July 2017, a man from Peshawar was jailed for an unprecedented 12 years for blackmailing a woman on Facebook after creating a fake Facebook profile in her name.[290]

Internationally, a number of recent revelations raise concerns about the vulnerability Pakistan's information-technology infrastructure. The US National Security Agency spied on Pakistani civilian and military leadership according to reports last year that site leaked classified documents from 2013.[291] The NSA used malware to gain access to targets in the "VIP division" of the National Telecommunications Corporation, which provides internet services to government departments. They were able to access data on their Green Line communications network, used by military and civilian leaders. (A malicious code named seconddate was used to redirect target browsers to the NSA's Foxacid malware web servers).[292]

A data leak by hackers group ShadowBrokers in April revealed that the NSA had hacked and obtained information such as call logs of users of at least one cellular network in Pakistan.[293]

In 2016, at least one million android devices in Pakistan were affected by the sophisticated CopyCat malware which took control of smartphones and tablets to inject a malicious code that showed fraudulent ads and installed unauthorised applications.[294]

In May 2017,[295] public and private[296] organisations in Pakistan were hit by the global WannaCry ransomware cryptoworm attack.

Hackers belonging to India and Pakistan are responsible for recurrent tit-for-tat attacks on websites belonging to each other's country, defacing[297] or carrying out denial-of-service attacks[298] against websites run especially by public organisations.[299]

287 Express Tribune. (2015, 1 February). Cybercrimes: Pakistan lacks facilities to trace hackers. *Express Tribune*. https://tribune.com.pk/story/831178/cybercrimes-pakistan-lacks-facilities-to-trace-hackers
288 Verma, S. (2017, 30 May). Study in Pakistan Finds 40% Women Harassed Online. *The Wire*. https://thewire.in/141298/pakistan-online-womenharassment
289 www.na.gov.pk/uploads/documents/1470910659_707.pdf
290 Ullah, I. (2017, 11 July). Peshawar man gets 12-year jail term for blackmailing woman on Facebook. *Express Tribune*. https://tribune.com.pk/story/1455517/man-peshawar-gets-12-years-creating-womans-fake-facebook-profile-blackmailing
291 Biddle, S. (2016, 19 August). The NSA lead is real, Snowden documents confirm. *The Intercept*. https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm
292 Ibid
293 Haider, S. (2017, 10 April). US spy agency hacked Pakistani cellular networks, shows leaked data. *Geo TV*. www.geo.tv/latest/137536-Leaked-hacking-tools-show-NSA-infiltrated-Pakistani-cellular-network
294 Check Point. (2017, 6 July). How the CopyCat malware infected Android devices around the world. *Check Point*. https://blog.checkpoint.com/2017/07/06/how-the-copycat-malware-infected-android-devices-around-the-world
295 Butt, W. A. (2017, 22 May). Virus attack: Land record services suspended in Punjab. *Dawn.com*. www.dawn.com/news/1334613
296 ARY News. (2017, 19 May). Global 'ransomware' virus hits Pakistan. *ARY News*. https://arynews.tv/en/ransomware-infiltrates-computers-pakistans-govt-owned-insurance-company
297 Ahmed, Z. (2017, 15 August). Indian hackers deface numerous Pakistani ministries websites. *PakWired*. https://pakwired.com/indian-hackers-deface-numerous-pakistani-ministries-websites
298 Cuthbertson, A. (2016, 1 November). Hackers take down Pakistan government websites on live radio. *Newsweek*. www.newsweek.com/hackers-take-down-pakistan-government-websites-live-radio-413888
299 Shukla, P. (2017, 14 August). India-Pakistan Gear Up For Cyber Wars This I-Day. *Business World*. expressbusinessworld.in/article/India-Pakistan-Gear-Up-For-Cyber-Wars-This-I-Day/14-08-2017-124037/

In December 2016, apparent Pakistani hackers defaced the Google Bangladesh domain in what seemed like a case of DNS hijacking.[300] Days before that, a Pakistani hacker group that called itself the Pashtun Cyber Army defaced the website of the Khyber Pakhtunkhwa government leaving a political message.[301]

1.11 AN INTERNATIONAL LEVEL

In line with its prior commitments to global cooperation on electronic crimes Pakistan has developed a legal framework to share electronic evidence or data relating to electronic crimes with foreign governments and entities in its new law.[302]

Section 39 of the Prevention of Electronic Crimes Act of 2016 says mutual assistance requests would be sent and entertained with the expectation of a commitment to keep the data confidential, and as long as the request is not political or discriminatory, does not violate any rights or prejudice an ongoing trial in Pakistan, or is against the country's laws or sovereignty.[303] The vaguely worded conditions do not require judicial oversight, but the investigation agencies in Pakistan are required to keep a register of such requests.

Global concerns focus more on internet rights in Pakistan, and what is seen as violation of Islamabad's commitments to freedom of expression and protection of privacy, such as those expressed in Article 19 of the Universal Declaration of Human Rights. The 2016 law allows the government to block content "in the interest of the glory of Islam, or the integrity, security or defense of Pakistan, or any part thereof, public order, decency or morality". The vaguely worded legal protection gives the government overwhelming powers to clamp down on free speech.[304] Human Rights Watch asked Pakistan to stop "abusive state monitoring of internet activity, prosecute those committing violence on the basis of internet blasphemy allegations, and commit to upholding free expression for all" in a report released in May.[305]

In July, the UN Human Rights Committee asked Pakistan to review its freedom of expression laws, including "its legislation on data collection and surveillance, in particular, the Prevention of Electronic Crimes Act 2016," and "licensing requirements which impose obligations on network service providers to engage in communication surveillance, particularly in relation to indiscriminate data retention", to make sure they do not violate Article 19 of the International Covenant on Civil and Political Rights.[306] It also asked Islamabad to "adopt a comprehensive data protection law in line with international standards". Pakistan has been given until 2020 to address these problems, and has been asked to report progress in a year.

Despite these concerns, Pakistan continues to participate in global debates about the internet and its future. Speaking at the World Economic Forum in January, Information Technology Minister Anusha Rehman said Islamabad was committed to global cooperation on internet rights, universal access, and digital governance.[307]

300 Express Tribune. (2016, 20 December). 'Pakistani hackers' take down Google's Bangladesh domain. *Express Tribune.* https://tribune.com.pk/story/1268986/pakistani-hackers-take-googles-bangladesh-domain
301 Dawn. (2016, 15 December). KP govt website defaced by hackers. *Dawn.com.* www.dawn.com/news/1302501
302 APP. (2015, 17 December). Need stressed for cooperation to end malicious use of cyberspace. *Dawn.com.* www.dawn.com/news/1226903
303 www.na.gov.pk/uploads/documents/1470910659_707.pdf
304 Shah, B. (2016, 24 November). Op. cit.
305 Human Rights Watch. (2017, 16 May). *Pakistan: Escalating Crackdown on Internet Dissent.* www.hrw.org/news/2017/05/16/pakistan-escalating-crackdown-internet-dissent
306 IFEX. (2017, 1 August). UN Committee urges Pakistan to protect freedom of expression and fight impunity. www.ifex.org/pakistan/2017/07/31/un-committee/
307 Express Tribune. (2017, 18 January). IT minister committed to 'Digital Pakistan'. *Express Tribune.* https://tribune.com.pk/story/1298594/minister-committed-digital-pakistan/

SECTION 2
KEY PLAYERS

2.1 FEDERAL INVESTIGATION AGENCY

The Federal Investigation Agency (FIA) has been the key law-enforcement arm in charge of investigation of cybercrimes, and continues to play the role after the 2016 electronic crimes law. It must be noted that in October 2017, the government granted the military spy agency Inter-Services Intelligence similar powers.[308]

Through its National Response Centre for Cyber Crimes, the agency addresses complaints of electronic crimes, helps other law-enforcement departments with its expertise, and carries out capacity-building and awareness activities.[309]

Although the FIA has been prosecuting harassment and blackmail cases aggressively,[310] there is concern that women are deterred by the fact that the authority does not allow a complaint to be launched anonymously.[311]

The FIA has been criticised for a crackdown against dozens of social media users who the agency alleged were "running an organized campaign on social media against the Pakistan Army". Opposition parties accused the government of misusing the electronic crimes law to target its political opponents.[312]

The agency has sought action against 64,000 Facebook and Twitter accounts so far, acting on more than 7,500 complaints from government organisations as well as citizens, primarily over charges of "blasphemy, anti-state activities and terrorism".[313]

2.2 MINISTRY OF INFORMATION TECHNOLOGY

The Ministry of Information Technology and Telecommunications is the premier government department dealing with IT and telecom policy, infrastructure and projects.[314] It oversees key organisations in the telecommunication sector, such as Pakistan Telecommunication

308 Gishkori, Z. (2016, 20 October). National security issues: Govt accepts ISI's role in checking cyber crimes. The News. https://www.thenews.com.pk/print/158580-Govt-accepts-ISIs-role-in-checking-cyber-crimes
309 www.fia.gov.pk/en/NR3C.php
310 Sindhu, H. A. (2017, 2017 August). Facebook blackmailer fined, sentenced to 14 months in prison. Daily Pakistan. https://en.dailypakistan.com.pk/pakistan/facebook-harasser-sentenced-to-14-months-in-prison-besides-hefty-fine
311 Toppa, S. (2017, 9 August). Abuse in Pakistan: 'I'm more scared of harassment online than offline'. The Guardian. www.theguardian.com/global-development-professionals-network/2017/aug/09/abuse-in-pakistan-im-more-scared-of-harassment-online-than-offline
312 Wasim, A., & Tahir, Z. (2017, 22 May). Op. cit.
313 Haq, R. (2017, 20 August). Cybercrime: 64,000 social media users reported to FIA. Express Tribune. https://tribune.com.pk/story/1486291/cybercrime-64000-social-media-users-reported-fia
314 www.moitt.gov.pk/frmDetails.aspx?opt=basic&id=1

Authority, the National IT Board, Pakistan Software Export Board, and the National ICT Research and Development Fund, recently renamed *Ignite*.[315]

It has faced serious public criticism because of its key role in internet censorship in the past, such as the 2012 call for proposals for an internet censorship project in Pakistan.[316] As the primary drafter of the controversial Prevention of Electronic Crimes Act of 2016, the ministry has been accused of ignoring serious rights concerns by civil society organisations.[317] It is now working a data protection law, but a draft has not been made publicly available by August 2017.[318]

The ministry supervised the 3G and 4G license auctions, and claims that Pakistan will become the first country in south Asia to test-run 5G technology. [319]

The IT and telecom ministry has recently funded a project to set up a large-scale automatic surveillance system to monitor video feeds from closed-circuit television cameras all over the country, "to combat terrorism".[320]

2.3 MINISTRY OF INTERIOR

With federal law and order in its domain, the Ministry of Interior's influence includes matters of security and crimes related to IT and telecom. It supervises the Federal Investigation Agency (FIA) which is one of the law-enforcement agencies dealing with electronic crimes.

The ministry has been at the forefront of a campaign against content on social media deemed blasphemous, after a court order in March 2017.[321] Former minister Chaudhry Nisar Ali Khan has pressured Facebook and Twitter in public statements to comply with the government's demands for data in such cases.[322] The FIA claims it acts in such cases on complaints by the Ministry of Interior and intelligence agencies.[323] In May, Chaudhry Nisar also told the FIA to crack down on social media users "ridiculing Pakistan Army".[324]

Concerns about the ministry's role were highlighted especially after a Shia man became the first Pakistani to be sentenced to death over social media posts.[325] He was charged with blasphemy after a debate with an under-cover counterterrorism agent.[326]

The ministry also directs cellular phone companies to suspend their services during religious and political events as a security precaution, via PTA (see Section 1).

2.4 PAKISTAN TELECOMMUNICATION AUTHORITY

Pakistan Telecommunication Authority is the primary regulator of the telecommunication

315 Ibid
316 AP. (2012, 8 March). Wanted: Censor for Pakistan's Internet. *Dawn.com.* www.dawn.com/news/701079
317 Dad, N., & Khan, S. (2017, 7 January). Naila Rind killed herself because Pakistan's cybercrime laws failed her. *Dawn.com.* www.dawn.com/news/1306976
318 Ahmadi, A. (2017, 5 April). IT ministry to introduce DPA within three months. *Pakistan Today.* www.pakistantoday.com.pk/2017/04/05/it-ministry-to-introduce-dpa-within-three-months
319 Yasin, A. (2017, 12 April). 'Pakistan to be the first country in South Asia to test 5G services'. *Dawn.com.* www.dawn.com/news/1326401
320 Pakistan Today. (2017, 3 August). IT ministry developing surveillance system to combat terrorism. *Pakistan Today.* www.pakistantoday.com.pk/2017/08/03/it-ministry-developing-surveillance-system-to-combat-terrorism
321 Human Rights Watch. (2017, 16 May). *Pakistan: Escalating Crackdown on Internet Dissent.* www.hrw.org/news/2017/05/16/pakistan-escalating-crackdown-internet-dissent
322 Hern, A. (2017, 17 March). Pakistan asks Facebook and Twitter to help identify blasphemers. *The Guardian.* www.theguardian.com/world/2017/mar/17/pakistan-asks-facebook-twitter-help-identify-blasphemers
323 Zahra-Malik, M. (2017, 27 July). Crackdown on online criticism chills Pakistani social media. *The New York Times.* www.nytimes.com/2017/07/27/world/asia/pakistan-social-media-online-criticism.html
324 Dawn. (2017, 14 May). Interior minister orders action against those maligning Pakistan Army on social media. *Dawn.com.* www.dawn.com/news/1333100
325 Rasmussen, S. E., & Wong, J. C. (2017, 22 July). Op. cit.
326 Ibid

sector in Pakistan, granting business licenses, setting infrastructure standards, and addressing complaints.[327] Its newest function, assigned in last year's electronic crimes law, is to regulate internet content.

The authority has been allowed to block information "in the interest of the glory of Islam, or the integrity, security or defence of Pakistan, or any part thereof, public order, decency or morality, or in relation to contempt of court or commission of or incitement to an offence," according to Section 34 of the new law.[328] While it has been asked to set up rules to ensure transparency and safeguards in the process, there is no time limit to developing such a framework, and the body retains its censorship powers in the absence of any guidelines. Appeals for review can be filed with the authority itself, and then at a high court. As a content regulator, the PTA will also deal with individual complaints of violation of privacy and certain forms of harassment.

PTA is the primary authority that negotiates with Facebook for the removal of content it deems illegal. In May 2017, PTA sent out text messages to millions of Pakistani cell phone users warning them against blasphemy on social media and telling them how to report it. The move was in line with a court order, but rights activists are concerned such messages encourage vigilantism.[329] In July, Facebook was told to link accounts to biometrically-verified mobile phone numbers, to make anonymity impossible.[330] In 2015, it had blocked 27.5 million cell phone sim cards after a long process of fingerprint verification linking phone numbers to citizens.[331] Facebook denied the request. [332]

The same year, the authority had ordered a ban on Blackberry services in Pakistan "for security reasons" because its end-to-end encryption makes interception nearly impossible.[333] The shutdown was cancelled later after the demand for access to private communications was withdrawn.[334] The 2016 law allows PTA to set the time for which service providers must retain their data, which can be accessed with a court warrant.

The frequent suspension of mobile phone services because of security concerns at political and religious events is also implemented by the PTA, which complies with the interior ministry's directions (see Section 1).

PTA also addresses consumer complaints in the telecommunication sector. From April to June 2017, it heard 10,237 complaints of which it claims to have redressed 96.04%.[335] After a controversial[336] text message and newspaper ad campaign asking citizens to report blasphemy on social media, carried out in line with a court order, the authority received 3,000 complaints of offensive content, and had blocked 12,968 such websites on its own by April 2017.[337]

2.5 POLITICIANS

Only a small number of politicians take interest in legislation regarding the internet. PMLN government's Minister for Information Technology and Telecommunication Anusha Rehman is the leading figure steering the policies directed towards internet. Rehman pushed for the passing of the Prevention of

327 www.pta.gov.pk/index.php?option=com_content&view=article&id=359&Itemid=325
328 www.na.gov.pk/uploads/documents/1470910659_707.pdf
329 RT. (2017, 11 May). Op. cit.
330 APP. (2017, 13 July). Pakistan asks Facebook to link accounts to mobile numbers. *Dawn.com*. www.dawn.com/news/1344893
331 APP. (2015, 16 May). PTA blocks 27.5m SIM cards as biometric verification process ends. *Express Tribune*. https://tribune.com.pk/story/887510/pta-blocks-27-5m-sim-cards-as-biometric-verification-process-ends/
332 Rasmussen, S. E., & Wong, J. C. (2017, 22 July). Op. cit.
333 Bhatti, S.I. (2014, 12 August). Mobile phone services being suspended in parts of Islamabad: PTA. *Dawn.com*. www.dawn.com/news/1124907
334 BBC. (2015, December 31). Blackberry to keep operating in Pakistan. *BBC*. www.bbc.com/news/technology-35204922
335 www.pta.gov.pk/index.php?Itemid=599
336 RT. (2017, 11 May). Op. cit.
337 Haq, R. (2017, 10 May). PTA blocked 12,968 websites till April. *Express Tribune*. https://tribune.com.pk/story/1405744/pta-blocked-12968-websites-till-april

Electronic Crimes Act and has been criticised for her statements on civil society and Non-Governmental Organisations. She accused the NGOs of having "vested interests" while lobbying for amendments in the original draft of PECA and said, "Cyber Crime Law has been weakened and not remains even 40 percent of the original draft, after some NGOs [who had vested interest] raised the issue while quoting attack on freedom of expression".[338]

Earlier, the 20-member National Assembly Standing Committee on Information Technology approved PECA while only one opposition politician Ali Raza Abidi opposed some parts of the bill. Five other members from the opposition were absent.[339]

On the party level, little resistance was shown to the Prevention of Electronic Crimes Act but few individuals took part actively in the meetings. PPPP Senator Farhatullah Babar, in one of the meetings discussing the PECA said: "The bill is an attempt to curb citizens' freedom of speech rather than protect them. Banned militant outfits continue to operate freely on social media but restrictions are being placed on citizens raising relevant questions on online portals".[340]

The government was criticised when PECA was passed by the National Assembly through a simple majority but with the presence of only 30 out of a total of 342 members. Pakistan People's Party's Shazia Marri, Pakistan's Tehreek-i-Insaf's Shireen Mazari and Muttahida Qaumi Movement's Ali Raza Abidi objected to many clauses of the bill. [341]

Amid the rumours of an apparent crackdown on social media, then Interior Minister Chaudhry Nisar Ali Khan denied any such move but added that unbridled freedom was not allowed either. He further claimed that "our cultural and religious values are under attack from a section of social media".[342]

2.6 INTERNET SERVICE PROVIDERS (ISPS)

There are about 50 internet service providers in Pakistan, of which 10 provide DSL services and at least four own domestic fibre backbones.[343] The number of cellular phone service providers, who also offer high-speed mobile internet, is five.[344] To deal with what they call "a state-owned monopoly" apprehensive towards the private sector, ISPs in the country decided to form the Internet Service Providers Association of Pakistan in 1997.[345] Despite having gained significant grounds, private service providers in Pakistan still depend largely on PTCL.[346]

PTCL was the only bandwidth provider in the country until 2009.[347] Although the rate of a 2-megabit bandwidth dropped from 80,000 dollars a month in the late 1990s[348] to 400 dollars a month by 2014,[349] PTCL still controls most of the bandwidth in the country, with three undersea cable connections – the 480gbps Sea-Me-We-3, the 1.28tbps Sea-Me-We-4, and the 3.86tbps I-Me-We. Transworld Associates (TWA), the only private bandwidth owner in Pakistan, is connected

338 Yusufzai, A. (2017, 5 April). NGOs weakened cyber crime law for vested interests: Anusha. *Propakistani*. https://propakistani.pk/2017/04/05/ngos-weakened-cyber-crime-law-vested-interests-anusha/
339 Shahid, J. (2015, 17 April). 'Flawed' cyber crime bill approved. *Dawn.com*. www.dawn.com/news/1176440
340 Guramani, N. (2016, 19 July). Senators term Prevention of Electronic Crimes Act, 2016 a 'black law'. *Dawn.com*. www.dawn.com/news/1346310
341 Abbasi, W. (2016, 14 April). Cyber crime bill passed in the absence of 90pc of MNAs. *The News*. www.thenews.com.pk/print/112570-Cyber-Crime-Bill-passed-in-absence-of-90pc-MNAs
342 (2017, May 23). No restrictions either: No unbridled freedom on social media, says Nisar. *Express Tribune*. https://tribune.com.pk/story/1417195/anti-army-content-social-media-will-not-tolerated-chaudhry-nisar/
343 www.ispak.pk/index.php
344 www.pta.gov.pk/index.php?option=com_content&task=view&id=269&Itemid=658
345 www.ispak.pk/aboutus.php
346 Ibid
347 https://opennet.net/research/profiles/pakistan
348 www.ispak.pk/aboutus.php
349 www.ispak.pk/index.php

to the 1.28tbps submarine cable TW1,[350] and joined 24tbps 16-party Sea-Me-We-5 cable in December 2016.[351]

All ISPs are legally required to retain traffic data for a period specified by the PTA, and cooperate in surveillance warranted by courts.[352] The new internet law passed in 2016 however criminalises unauthorised disclosure of private data.[353] PTCL also owns the Pakistan Internet Exchange through which most of the country's internet traffic is routed,[354] and all ISPs are in any case required to enforce censorship carried out by the PTA.[355] There are concerns the law can potentially be used to silence dissenting opinion.[356]

2.7 MILITARY

Pakistan's military has historically been very influential in policy matters and has exerted significant pressure on civilian governments and politicians to drive the narrative in their favour.[357]

The military, which poses as the protector of Pakistan's geographical as well as ideological frontiers attempts to censor the content it deems "anti-state". In the past, several Baloch websites have been blocked (see ILR 2016).

The public relations unit of the military, the ISPR, effectively uses cyberspace to reach out to the masses. In April this year, the Director General of ISPR took on Twitter to "reject" a notification from the Prime Minister on "Dawn leaks", a news story about a rift between civilian and military leadership over a crackdown against certain terror groups published in Dawn.[358] However, the tweet was withdrawn two weeks later after the issues were settled between the military and government. [359]

The military has also been accused of suppressing dissenting voices online. One of the abducted bloggers Ahmad Waqas Goraya told the BBC days after his release that he was abducted and tortured by an agency linked with the military,[360] while Salman Haider also took to Twitter and claimed that he was abducted by a military agency for running a page critical of its role in politics.[361] Former Interior Minister Chaudhary Nisar Ali Khan also threatened to take action against those critical of the military using online spaces. He was quoted as saying: "As far as the freedom of speech is concerned, the Constitution makes it clear that national security and defence institutions would not be criticised and that citizens would not engage themselves in any activity that causes damage to the prestige, reputation and goodwill of Pak Army".[362]

350 Baloch, F. (2015, 8 March). Broadband connectivity: New cable to provide faster access for consumers, businesses. *Express Tribune*. expresstribune.com.pk/story/849956/broadband-connectivity-new-cable-to-provide-faster-access-for-consumers-businesses
351 TR Pakistan. (2016, 19 December). Pakistani internet bandwidth to increase by 24Tbps. *Dawn.com*. www.dawn.com/news/1303258
352 www.na.gov.pk/uploads/documents/1470910659_707.pdf
353
354 Attaa, A. (2016, 14 November). Pakistan ranked among worst 10 countries for internet freedom: report. *Dawn.com*. www.dawn.com/news/1296904
355 www.na.gov.pk/uploads/documents/1470910659_707.pdf
356 Shah, B. (2016, 24 November). Op. cit.
357 Javid, H. (2014, 23 November). The army and democracy: military politics in Pakistan. *Dawn.com*. www.dawn.com/news/1146181
358 Sikander, S. (2014, 29 April). Army rejects PM Office statement on Dawn leaks report. *Express Tribune*. https://tribune.com.pk/story/1396876/pakistan-army-rejects-govt-notification-dawn-leaks
359 Geo News. (2017, 10 May). Dawn leaks: Army withdraws tweet rejecting PM's orders, says issues settled. *Geo TV*. www.geo.tv/latest/141230-Army-ISPR-withdraws-tweet-says-Dawn-leaks-issue-settled
360 BBC. (2017, 9 March). Op. cit.
361 https://twitter.com/salmanhydr/status/899490810357587968
362 Dawn. (2017, 14 May). Interior minister orders action against those maligning Pakistan army on social media. *Dawn.com*. www.dawn.com/news/1333100

The military-run Special Communications Organisation (SCO) has been bidding to enhance their operations across the country on a commercial basis. Run by a military officer, the SCO currently operates throughout the northern areas and Kashmir. However, the government recently made it clear to the Senate that it had no intentions to grant permission to the SCO to operate commercially.[363]

2.8 MILITANT RELIGIOUS GROUPS

Many militant religious groups, although banned officially by the government, continue to operate freely in cyberspace.

An investigation by Pakistan's leading newspaper Dawn found that 41 of the total 64 banned outfits continue to use social media, especially Facebook, to further their agenda.[364] The groups included sectarian outfits like Ahle Sunnat Wal Jamaat (ASWJ), Sipah-e-Sahaba (SSP), Lashkar-e-Jhangvi (LeJ) and terrorist outfits like Tehreek-i-Taliban Pakistan (TTP) and Jamat-ul-Ahrar.[365]

Chief of Army Staff General Qamar Javed Bajwa, while speaking to a group of students warned them about the presence of terror outfits on social media and their potential recruiting methods.[366]

The terror outfits seem to increase their recruiting efforts online, which were indicated by a student of Liaquat University of Medical Sciences Noreen Leghari who was arrested in a raid by the Counter Terrorism Department of Punjab Police. She confessed to planning to conduct a suicide attack.[367]

Tehreek-i-Taliban Pakistan also launched a women's magazine for would-be female Jihadists which urged women to gather others for secret meetings and learn to use weapons.[368]

Little or no action has been taken against the individuals and groups using social media to spread extremist views. However, in some of the rare incidents, the Counter Terrorism Department in Abbottabad arrested a man last year for uploading material supporting terrorism.[369]

363 Shahid, J. (2017, 18 August). Military-run SCO denied permission to operate across country. *Dawn.com*. www.dawn.com/news/1352296
364 Haque, J., & Bashir, O. (2017, 13 June). Op. cit.
365 Ibid
366 Samaa. (2017, 17 August). COAS warns youth against militant outfits active on social media. *Samaa TV*. www.samaa.tv/pakistan/2017/08/coas-warns-youth-against-militant-outfits-active-on-social-media/
367 Tanveer, R. (2017, 16 April). Female militant arrested in Lahore found to be IS-affiliate who went missing. *Express Tribune*. https://tribune.com.pk/story/1385163/female-militant-arrested-lahore-found-affiliate-went-missing
368 Janjua, H. (2017, 8 August). Pakistani Taliban starts magazine for would-be female Jihadists. *The Guardian*. www.theguardian.com/world/2017/aug/08/pakistani-taliban-starts-magazine-for-would-be-female-jihadists
369 Pakistan Today. (2016, 27 April). Man arrested for supporting banned outfits on social media. *Pakistan Today*. www.pakistantoday.com.pk/2016/04/27/man-arrested-for-supporting-banned-outfits-on-social-media/

SECTION 3

3.1 DIGITAL JOURNALISM

With the introduction of third and fourth generation technology in Pakistan, internet accessibility has become cheaper and more people are joining social media platforms. The media landscape has also changed rapidly as media outlets invest heavily in digital platforms.

Many of the recent journalism training programs focused on Pakistan have included digital journalism as a key theme.[370] In recent years, media groups like Express Tribune have launched digital journalism platforms like "Tribune Labs", which is self-described as "a platform for cutting-edge, digital storytelling; a place new age media meets old-school journalistic standards".[371] The digital presence of Geo TV has also focused on 360° graphics for storytelling.[372]

Many digital news platforms have also emerged over the past few years, focusing on an entirely different reporting strategy as compared to the mainstream media. A recently launched platform PakVoices focuses on bringing stories from the remotest areas of Pakistan to "bring greater transparency and accountability to governance."[373]

The popularity of online news portals is demonstrated by the fact that 8 out of a total 50 websites ranking on top in Pakistan are news websites.[374]

3.2 ACTIVISM ON DIGITAL MEDIA

There are more than 44 million social media accounts being operated from Pakistan, out of which 31 million are on Facebook and 3.1 million on Twitter.[375] In the 2013 elections, Pakistan saw a surge in the social media use as Pakistan Tehreek-i-Insaf effectively used these platforms to rally the younger generation in its support.[376]

Since then, social media has become a major tool for political and social activism in Pakistan and many major incidents were first reported on social media, instead of the mainstream media. The most recent example is the murder of Mashal Khan. After the videos of his lynching were shared online and sparked widespread outrage, it was picked up by the mainstream media outlets.[377]

The transgender community in Pakistan has used social media effectively to raise their voices against the violence and discrimination they face in their daily lives. Their efforts have led to the KP government drafting a comprehensive transgender policy, including announcing a trans-specific rehabilitation plan, and allowing for ID cards with gender X. [378]

However, with positive activism, digital media is also used for negative campaigning and propaganda. An investigation earlier this year revealed that an organised campaign against Afghan refugees was launched online after the attack on Army Public School Peshawar asking to drive them out of the country.[379]

370 International Center for Journalists. (2015, 10 August). Pakistan alumni summit builds digital journalism skills. www.icfj.org/blogs/pakistan-alumni-summit-builds-digital-journalism-skills
371 expresslabs1.tribune.com.pk/about-us
372 www.geo.tv/news360/360-The-sights-and-sounds-of-Karachi-Burnes-Road/list
373 www.pakvoices.pk/about-us-2
374 www.alexa.com/topsites/countries/PK
375 Jahangir, R. (2017, 13 May). Society: The politics of hashtag activism. Dawn.com. www.dawn.com/news/1332869
376 Asia Despatch. (2013, 13 May). *Pakistan elections 2013: The social media impact. Asia Despatch.* www.asiadespatch.org/2013/05/13/pakistan-elections-2013-social-media-impact
377 Jahangir, R. (2017, 13 May). Op. cit.
378 Ali, U. (2017). Hashtag trans lives matter. Newsline, July. expressnewslinemagazine.com/magazine/ashtag-trans-lives-matter
379 Ali, U. (2017, 4 July). Tweeting hatred: *The hounding of Afghan refugees in Pakistan. News Deeply.* www.newsdeeply.com/refugees/articles/2017/07/04/tweeting-hatred-the-hounding-of-afghan-refugees-in-pakistan

CHAPTER 3

COUNTRY REPORT: INDIA

INTRODUCTION METHODOLOGY

The International Covenant on Civil and Political Rights (ICCPR) guarantees to all individuals certain inalienable rights. Our human rights are the foundation of our free existence in our countries. Of these rights, one of the most important rights is the right to freedom of speech and expression (Article 19, ICCPR). Without Article 19, many of our other rights would become toothless. It is our freedom of speech and expression that provides us with access to information, the right to seek information from governmental authorities, and the right to opinion, exchange and sharing of information, and the right to speak and express freely. For decades, this right has been instrumental in ensuring the free flow of information in offline media.

In India, the right to freedom of speech and expression is guaranteed by Article 19(1)(a) of the Constitution. However, as in the International Covenant on Civil and Political Rights, freedom of expression in India is not absolute. Article 19(2) sets out certain criteria for the reasonable restriction of freedom of expression; these being "in the … interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence." These criteria have been applied for offline media for decades, shaping India's jurisprudence on freedom of speech and expression.

The internet is no different. Rights on the internet have been affirmed by the La Rue Report (2011), and again by the Human Rights Council and the United Nations General Assembly. As the General Comment No. 34 of the UN Human Rights Committee makes clear:

> **[Article 19]**… protects all forms of expression and the means of their dissemination. Such forms include spoken, written and sign language and such non-verbal expression as images and objects of art. Means of expression include books, newspapers, pamphlets, posters, banners, dress and legal submissions. *They include all forms of audio-visual as well as electronic and internet-based modes of expression.* (Emphasis added.)

The freedom of expression that we enjoy offline applies equally online, states General Comment no. 34. Taking cue from the Frank La Rue Framework for freedom

of expression online, the Association for Progressive Communications developed the APC-La Rue Framework (see Appendix 1). The APC-La Rue Framework sets for certain indicators to test the extent of online freedoms across countries.

In our previous report, *Limited Access Restricting Expression*, the Digital Empowerment Foundation produced a comprehensive study of India's internet freedoms, with an emphasis on freedom of speech and expression. This report held valid until the year 2014, when it was produced. This report is an update. In this report, wherever possible, we follow the APC-La Rue Framework. The report is structured thus: Each chapter studies a specific issue, such as arbitrary blocking on the internet, intermediary liability, criminalisation of legitimate expression, internet governance etc. Within each chapter, the sections study and summarise the situation until and after 2014, while providing the legal framework.

The report concludes with general recommendations to assist the better exercise of the right to freedom of speech and expression in India. One of the major recommendations is to ensure greater transparency in governmental procedure for website-blocking, surveillance and other measures to ensure that citizens have access to both information and legal remedies. Further, we recommend that the government implement projects to expand internet access to rural areas, to effectively bridge the urban-rural divide, through partnerships with other stakeholders.

SECTION 1
CONSTITUTIONAL AND POLICY FRAMEWORKS FOR INTERNET RIGHTS: GLOBAL AND NATIONAL

without an understanding of the country's constitutional, legal and policy framework. It is equally important to place this understanding against the international context. In this section, the author explores the international framework for internet rights, taking note of the platforms where discussions on internet rights occur, and then briefly explains India's constitutional and policy framework.

1.1 UNDERSTANDING THE INTERNATIONAL CONTEXT

Two aspects must be studied to gather an understanding of the international protections for human rights online: first, the history of internet rights, and secondly, the platforms where discussions on internet rights occur today. Together, these give us a sense of how internet rights function internationally, which in turn affords a better understanding of the Indian context.

1.1.1 The history of internet rights

To trace the international history of internet rights, one must go back to the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). As a binding treaty, the ICCPR holds more weight in international law. The rights enshrined in these have been largely extended online, making the ICCPR the fundamental document for internet rights.

The ICCPR was opened for accession in 1966,[380] and entered into force on 23 March 1976. Recognising that the rights derive from the "inherent dignity of the human person", the ICCPR accords to all human beings certain inalienable rights. These include, but are not limited to, the right to freedom of speech and expression,[381] the right to privacy,[382] the right to religion,[383] and the right against advocacy of national, religious or racial hatred (it has been understood as the right against hate speech).[384]

It is important to remember that these rights are not absolute. The author will take the example of the right to freedom of speech and expression to explore the nature of restrictions. The ICCPR provides that the right to freedom of speech and expression (as well as the rights to privacy and religion) may be restricted, by law and if necessary:[385]

- For respect of the rights or reputations of others;
- For the protection of national security or of public order (*ordre public*), or of public health or morals.

380 UNGA Res. 2200A (XXI). (1966, 16 December).
381 ICCPR, Article 19: (1) Everyone shall have the right to hold opinions without interference; (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice…
382 ICCPR, Article 17: (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) Everyone has the right to the protection of the law against such interference or attacks.
383 ICCPR, Article 18: (1) Everyone shall have the right to freedom of thought, conscience and religion. This right shall include freedom to have or to adopt a religion or belief of his choice, and freedom, either individually or in community with others and in public or private, to manifest his religion or belief in worship, observance, practice and teaching; (2) No one shall be subject to coercion which would impair his freedom to have or to adopt a religion or belief of his choice…
384 ICCPR, Article 20: …(2) Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.
385 ICCPR, Article 19(3).

This is crucial. While restrictions may legitimately be placed by national governments on the rights accorded by the ICCPR – indeed, they may even be suspended under certain circumstances[386] – the restrictions must meet the tests of legality, legitimacy and necessity in order to withstand contestation. The test of legality requires that any restriction of the freedom of speech and expression must be by law – that is, it must have the backing of a statute, order, by-law or other legal document. In the event, say, that a government arrests an individual for a statement made online, without the backing of a penal provision, such an arrest must be deemed invalid in the eyes of Article 19(3), ICCPR.

The test of legitimacy requires that the governments restrict the freedom of speech and expression on the basis of a *legitimate reason.* What are these reasons? Article 19(3) provides the answer when it refers to the "protection of national security or of public order (*ordre public*), or of public health or morals", and "respect of the rights or reputations of others." These are the only legitimate reasons the ICCPR recognises. Any government restricting speech and expression for other reasons – say, for contempt of court, is liable to find itself contested.

Finally, the test of necessity requires that there be a pressing social need, making the restriction on speech and expression necessary in a democratic society.[387] While the state is afforded a certain "margin of appreciation" to judge the necessity of restriction,[388] it is also required to exhibit pluralism and broadmindedness.[389] Moreover, the restriction must be *proportional* – i.e., the benefits of the restraint must outweigh the loss of the right.[390] The restriction must be the *least restrictive*.[391] Where a narrowly tailored restraint suffices, the presence of a broad restriction is unacceptable. For instance, the imposition of an internet shutdown, where a narrower restriction such as *post facto* examination suffices, is a violation of Article 19, ICCPR.

1.1.2 The ICCPR and the internet

The ICCPR is not merely an offline rights document. Importantly, in 2011, the Human Rights Committee noted that Article 19 was equally applicable online, as it is offline.[392] Further, in his report, the Special Rapporteur for Freedom of Expression, Frank La Rue, underscored the "unique and transformative nature of the internet not only to enable individuals to exercise their right to freedom of opinion and expression, but also a range of other human rights."[393] The Special Rapporteur stated that the internet, as an interactive *Medium*, was far more valuable in the creation and sharing of information, as individuals become "active publishers."[394] As such, the internet affords individuals a chance to access objective information, and to share critical views in ways previously unimaginable. Not only this, but the ICCPR and the UDHR originally considered technological advancements when guaranteeing the right to freedom of speech and expression to individuals. The ICCPR states:

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, *or through any other media of his choice.* (Emphasis added.)

386 Except for non-derogable rights, which may not be curtailed even in times of national emergency. ICCPR, Article 4(2).
387 Jacobs, F.C., & White, R.C.A. (1996). The European Convention on Human Rights. Oxford: Clarendon Press, 306.
388 O'Donnell, T. A. (1982). The Margin of Appreciation Doctrine: Standards in the Jurisprudence of the European Court of Human Rights. Human Rights Law Quarterly 14(4), 474-475.
389 Handyside v. United Kingdom. (1976, 7 December). Series A no. 24 (ECHR); *The Sunday Times v. United Kingdom* (no. 1). (1979, 26 April). Series A no. 30 (ECHR).
390 Indian Express v. Union of India. (1985) SCR (2) 287 (Indian Sup. Ct.).
391 Human Rights Committee. (2011, 12 September). General Comment no. 34, *Article 19: Freedoms of Opinion and Expression, 102nd Session.*
392 Ibid., Article 12: They include all forms of audio-visual as well as electronic and internet-based modes of expression.
393 Human Rights Council. (2011, 16 May). 17th Session, A/HRC/17/27.
394 Ibid., 19.

Moreover, the Human Rights Council affirmed that offline human rights must be equally protected and guaranteed online. In its 20th session (29 June 2012), the Human Rights Council unanimously voted as follows:[395]

> Affirms that the *same rights that people have offline must also be protected online, in particular freedom of expression,* which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. (Emphasis added.)

It may seem that the internet is primarily concerned with the right to freedom of speech and expression. While this right is crucial to the way individuals utilise the internet, it is also an enabler for other rights.[396] Without the freedom to speak, hold opinions and express oneself, other rights such as the rights to assembly, association and religion would be meaningless. Equally, economic and social rights, such as the right to education, the right to work etc., would become toothless. The internet, as such, enables economic development and the enjoyment of a range of human rights.[397]

Moreover, where the internet is concerned, access to its content is crucial. Without such access, the rights available for exercise on the internet would be inaccessible. A digital divide would be (and is) created amongst those elites in urban areas who have easy access to the infrastructure and content of the internet and the rural poor who have neither.[398] The divide between marginalised groups and the elite would be perpetuated, without steady and effective access to the internet, leading to perpetual inequality between and within nation-states. This affects not only economic development, but also education, technological advancement, access to information etc.

1.1.3 Platforms for discussion

In the present day, a discussion of global internet rights is incomplete without a mention of platforms where such conversations take place. Global Internet Governance (GIG) platforms have created a space for the discussion of internet rights internationally. These platforms are briefly noted below (the list is non-exhaustive).

The United Nations creates multiple channels for the discussion of internet rights. Notwithstanding the ongoing discussions in the Human Rights Council (and occasionally, through resolutions in the General Assembly), the International Telecommunications Union (ITU) addresses concerns regarding access to infrastructure (such as spectrum allocations), child online protection, spam and other content-related issues, etc. The World Summit on Information Society (WSIS), a crucial moment in the development of Global Internet Governance, is run jointly by the ITU, UNESCO and other UN agencies. UNESCO and other agencies also run parallel projects on issues such as child online protection, online harassment of women and LGBTQI groups etc.

The Internet Corporation for Assigned Names and Numbers (ICANN) is another crucial organ where discussion on human rights on the internet is ongoing. ICANN is the body that manages internet protocols, domain names and IP addresses. Within ICANN, a working group on human rights questions the rights implications of ICANN policies and processes, such as the WHOIS.

The global Internet Governance Forum (IGF), as well as regional and national IGFs, is another platform where internet rights are discussed and protection methods strategised. The IGF is a talking forum, where stakeholders such as the private sector, civil society, academia, governments etc. come together to discuss concerns and possible solutions to rights violations, as well as access questions.

395 Human Rights Council. (2012, 29 June). 20th Session. The Promotion, Protection and Enjoyment of Human Rights on the Internet. A/HRC/20/L.13.
396 Ibid., 22.
397 Ibid., 62.
398 Ibid., 60-61.

1.2 INDIA'S FRAMEWORK FOR INTERNET RIGHTS: CONSTITUTIONAL, LEGAL AND POLICY

Given the pervasiveness and connectedness of the internet, global discussions necessarily inform national developments on internet rights. However, it is also equally important to understand national frameworks. In this section, the author discusses India's constitutional, legal and policy frameworks for internet rights. While these are obviously interrelated, a distinction may be drawn amongst them for the purposes of study.

1.2.1 Fundamental rights in the Indian Constitution

Part III of the Indian Constitution guarantees fundamental rights to its citizens (and in certain cases to all persons, such as the right to life under Article 21). Article 14 guarantees the right to equality, while Article 15 prohibits discrimination on the basis of religion, race, caste, sex or place of birth. Importantly, the Constitution guarantees fundamental freedoms by way of Article 19. Article 19 accords to all citizens, non-exhaustively, the right to freedom of speech and expression (since extended to the press, and to online spaces), the rights to free assembly and association and the right to trade. Article 21 guarantees the right to life and personal liberty (within which the right to privacy has hitherto been included).[399] Article 25 guarantees the right to freedom of religion while Article 26 grants to every religious denomination or section the freedom to manage its religious affairs.

These are fundamental rights which may not be derogated except under circumstances of national emergency. Even in such a situation, the right to life and personal liberty cannot be suspended. The right to freedom of expression (Article 19(1)(a)), for instance, may only be curtailed by way of reasonable restrictions in the "interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence."[400] Similarly, the rights to freedom of assembly and association may be restricted only on grounds laid down in the Constitution. These are the legitimate aims that Article 19 of the ICCPR requires of national governments.

While these rights were originally intended to be offline rights, they have since been extended to other media including the online space through judicial pronouncements. For instance, in *PUCL v. Union of India,*[401] the Supreme Court extended the right to privacy to telephonic communications, in a case that concerned wiretapping and interception of communications. Similarly, in *Shreya Singhal* v. Union of India,[402] the Supreme Court recognised that freedom of speech and expression are integral to the internet, where access to and publication of information require this fundamental right.

1.2.2 Legal frameworks

Article 13(3) of the Indian Constitution lays down the meaning of the word law, for the purposes of Part III of the Constitution. What this means is that fundamental rights may be restricted only by those instruments that may be considered law under Article 13(3) of the Constitution. Article 13(3) states:

- "law" includes any Ordinance, order, bye-law, rule, regulation, notification, custom or usage having in the territory of India the force of law;

- "laws in force" includes laws passed or made by a Legislature or other competent authority in the territory of India before the commencement of this Constitution and not previously repealed...

399 A case presently ongoing in the Supreme Court of India may alter this situation. A bench of nine judges has been constituted to decide on whether there exists a fundamental right to privacy in the Indian constitution. As of the date of writing, the Supreme Court has completed its hearings and the case is pending judgment.
400 The Constitution of India. (1950). Article 19(2).
401 AIR 1997 SC 568.
402 Shreya Singhal v. Union of India, AIR 2015 SC 1523.

In India, three main types of laws regulate the internet space: first, offline laws that have since been applied online; secondly, laws specific to cyberspace; thirdly, sector-specific laws, such as those applicable to telecommunications, which have an impact on the internet.

The Indian Penal Code, 1860 (IPC) and its ancillary procedural laws (the Criminal Procedure Code 1973 and the Evidence Act 1872) are the major offline laws that have since been made applicable to online spaces. The Indian Penal Code lists out a variety of offences that have been found applicable to the online space. These include offences related to obscenity and pornography (Section 292, IPC), hate speech (Sections 153A and 295A, IPC), sedition (Section 124A, IPC) etc. These criminalise expression online and offline, and give rise to debates concerning legitimate and illegitimate restrictions on expression.

The Information Technology Act 2000 (as amended in 2008) regulates online activity. It gives the state the authority to engage in website blocking, to criminalise activity online, including those considered obscene, child pornography, fraud and phishing, cyber terrorist activities etc., as well as creating an intermediary liability regime.

Sector-specific laws, such as the Telegraph Act 1885, regulate the telecommunications sector. There exist licenses for telecommunications operators which create conditions (such as turning over identifying or other information upon governmental request) for the continuance of such services on the part of the operators.[403]

1.2.3 Policy spaces for discussion and development of internet rights

Several policy spaces exist in India for the discussion of internet rights. In this section, the author provides a non-exhaustive list. The Ministry for Communications and Information Technology is the governmental body tasked with coming up with law and policy surrounding the internet. The Ministry holds consultations from time to time, on issues such as access, net neutrality, internet governance etc.[404]

In addition to the Ministry and its working groups, the National Internet Exchange of India (NIXI) holds consultations on internet governance and related rights; the TRAI holds consultations and frames policy on issues such as access, net neutrality, telecom licensing, infrastructure policy etc. The Law Commission of India also considers questions such as hate speech etc.

403 Ghosh, S. (n.d.). Licensing Framework for Telecom: A Historical Overview. CIS India Blog. cis-india.org/telecom/resources/licensing-framework-for-telecom; Telecom Regulatory Authority of India. (n.d.). Licensing. trai.gov.in/telecom/licensing

404 The Ministry has, in recent years, adopted the practice of holding multi-stakeholder consultations, though closed-door meetings also continue.

SECTION 2
ACCESS

In this section, the report first looks at the existing framework for internet access in India, focusing on the situation in 2014. Secondly, the report considers the major changes that have taken place between 2014 and 2017.

2.1 THE SITUATION UNTIL 2014

In our previous report, we stated, "Access to the internet is a precondition for the exercise of freedom of speech and expression online, as well as related rights, such as freedom of association and freedom of assembly."[405] This is a matter of utmost importance. Access to the internet is necessary for human development, and also a basic human right. When more people have and can exercise the right of access to information, it can improve lives. As an open and democratic *Medium* for the sharing and exchange of information, it "becomes a source to organise and share information in an efficient, transparent, accountable manner."[406]

India has 700 million phone subscribers, out of which 97 million people access the internet through their mobile phones. However, the rural digital penetration is only 7%. Efforts are being made to bridge the digital divide between urban and rural populations, through convergence of digital infrastructure through the Digital India plan.[407] The aim is to provide e-access across the central and state governments, as well as the Gram Panchayats. The Digital India plan has three areas of focus. These are (1) digital infrastructure, including mobile internet, Common Service Centres, and a safe and secure cyberspace; (2) e-governance services; and (3) digital empowerment, including digital literacy.

In addition to this, the Indian government has put in place a plan to ensure connectivity of rural areas to the internet. Named the National Optical Fibre Network (NOFN), the plan aims to connect 250,000 Gram Panchayats by laying 70,000 km of optical fibre. Last mile connectivity is envisioned through optical fibre leading to high-speed broadband connectivity across villages. The government also envisions private-public partnerships to provide connectivity. For instance, in Delhi the government is tying up with Reliance Jio Infocomm to provide Wi-Fi connectivity across central Delhi.

The government has also put in place plans for e-governance and conversion of paper into digital archives where government services and documents are concerned. Mobile Seva, a mobile application platform for the delivery of government services, is being utilised by over 1500 government departments and agencies across the country to deliver services such as Aadhar, passport, voter registration etc. Health monitoring and education services are also offered. For instance, the Election Commission of India mapped over 900,000 polling booths in India, converting it into a web-map to make it "easier for citizens to locate polling booths."

405 Digital Empowerment Foundation. (2015). *India: Limited Access Restricting Expression*, 57. www.apc.org/sites/default/files/Annex%2013_%20DEF%20Country%20Report%20Year%201_0.pdf
406 Ibid
407 Digital India Plan. www.cmai.asia/digitalindia

2.2 ACCESS: 2014 TO 2017

At the end of 2016, the global internet penetration was around 3.5 billion,[408] out of a total population of about seven billion. India alone has one billion yet to be connected to the internet, out of a total population of 1.25 billion.[409] A large number of the unconnected reside in rural areas.

Though the government has set aside a budget to connect the unconnected, there remain large problems that are yet to be accounted for. For instance, in many cases, individuals give their biometric information in exchange for an Aadhar card (Unique Identification). However, when they are manual labourers (among the poorest of the poor in the country), it is found that their fingerprints do not match those on record and hence, their identification is often rejected.[410] Moreover, the NOFN project has so far had Rs 70,000 crore (USD 10.7 billion) added to its budget, but despite this, the project, begun in 2011, has not reached the point of conclusion.[411] Despite the many plans floated by the government, access to the internet remains a dream for most people in rural areas. The digital divide is far from being bridged.

408 Manzar, O. (2017, 3 March). Connecting the other half. *Livemint.* www.livemint.com/Opinion/h4obchfeTfClWKXo52SXtM/Connecting-the-other-half.html
409 The World Bank. (2016). World Development Report 2016: *Digital Dividends.* www.worldbank.org/en/publication/wdr2016
410 Manzar, O. (2016, 26 October). The cost of digital exclusion. *Livemint.* www.livemint.com/Opinion/W8ikKtNvw3qrSzEv-9V42lK/The-cost-of-digital-exclusion.html
411 Manzar, O. (2016, 16 October). Rs70,000 crore budget, and not even 70,000 connected? *Livemint.* www.livemint.com/Opinion/FcGsXzS4Vho8OIpKf3V9aN/Rs70000-crore-budget-and-not-even-70000-connected.html

SECTION 3
INTERMEDIARY LIABILITY

In this section, the report first looks at the existing framework for intermediary liability in India, focusing on the situation in 2014. Secondly, the report considers the major changes that have taken place between 2014 and 2017.

3.1 EXISTING FRAMEWORK FOR INTERMEDIARY LIABILITY

Intermediary liability refers to the safe harbour given to intermediaries from liability for the publication of third party information. When intermediaries are intimated (when it comes to their knowledge), they are required to take down the content from their pages. This is similar to, but not the same as blocking of content. In content blocking, the information is not removed at the source; it is merely blocked so that a certain population has no access to it. That is why VPNs allow for blocked content to be accessed. In the case of take downs, the information is removed at source and becomes completely unavailable.

The intermediary liability regime in India is set out in the Information Technology Act 2000 (as amended in 2008) (IT Act). The IT Act pro*vide*s an inclusive definition of an intermediary as "any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service provides, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online market-places and cybercafés."[412]

Section 79 of the Act, which establishes the intermediary liability regime, reads:

> (1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of subsections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

Under certain circumstances, laid down in subsections (2) and (3) of Section 79, an intermediary shall not incur liability for third party information. These circumstances are: first, if the function of the intermediary is limited to providing access to a communication system over which third party information is transmitted, stored or hosted; secondly, if the intermediary has no editorial control over the information – i.e., the intermediary does not initiate the transmission, select its receiver, and modify the information contained therein; thirdly, if the intermediary exercises due diligence in discharging its duties under the IT Act.

412 Information Technology Act. (2000). Section 2(w). (As amended in 2008).

What due diligence must an intermediary exercise? These are laid down in the Information Technology (Intermediaries Guidelines) Rules, 2011 (Intermediaries Guidelines).[413] The Intermediaries Guidelines require that an intermediary "publish the rules and regulations, privacy policy and user agreement for access or usage of the intermediary's computer resource by any person." The Terms of Agreement, Privacy Policy and other policies published by search engines, video websites, email sites and other intermediaries fall within this ambit.

The crucial aspect of the Intermediaries Guidelines lies within Rule 3(2). Rule 3(2) requires intermediaries to inform its users that certain content is impermissible on its platform.[414] Importantly, in Rule 3(2) (b), information that is "grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging" is prohibited. This creates a content-restriction, constituting a privately instituted prior restraint.

Moreover, when the intermediary obtains knowledge of the violative content (either by itself, or when "brought to actual knowledge by an affected person in writing or through email"), it must act immediately to remove or take down such content – i.e., within 36 hours of knowledge.[415] Similarly, the intermediary must comply with government or judicial takedown orders. Not only this, but in order to avoid liability intermediaries are also required to capitulate to government orders requesting identifying and other information, for the purposes of "verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force."[416] It may be argued that this undermines the anonymity that the internet affords to individuals (who may or may not be legitimate dissidents) and also citizens' right to privacy.

Since 2009, governmental requests to intermediaries to take down content have increased.[417] Intermediaries also argue that the Intermediaries Guidelines force them to screen and self-censor online content.[418] On the other hand, the government routinely sends takedown requests to intermediaries such as Google, Facebook and Twitter on a number of grounds.

In 2014 alone, Facebook restricted a total of 10,792 pieces of information, on the basis of requests received from "government agencies, including law enforcement agencies and the India Computer Emergency Response Team within the Ministry of Communications and

413 These were published in the Gazette of India (Extraordinary) and came into force on 11 April 2011.
414 Ministry of Communications and Information Technology in New Delhi. (2011, 11 April). Information Technology (Intermediaries Guidelines) Rules. Rule 3(2): …terms and conditions or user agreement shall inform the users of computer resource not to host, display, upload, modify, publish, transmit, update or share any information that —
(a) belongs to another person and to which the user does not have any right to;
(b) is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;
(c) harm minors in any way;
(d) infringes any patent, trademark, copyright or other proprietary rights;
(e) violates any law for the time being in force;
(f) deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;
(g) impersonate another person;
(h) contains software viruses or any other files programmes designed to interrupt, destroy or limit the functionality of any computer resource;
(i) threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation.
415 Ibid., Rule 3(4).
416 Ibid., Rule 3(7).
417 Digital Empowerment Foundation. (2015). Op. cit., 40.
418 Mouthshut.com v. Union of India, W.P.(C).No. 217 of 2013.

Information Technology," as well as non-governmental entities.[419] Google, in 2014, received over 500 takedown requests from the government for various reasons, including defamation, obscenity/nudity and adult content, religious offences, impersonation etc., complying with 61% of them.[420] Twitter, on the other hand, received 20 takedown requests in 2014, complying with 7% of the requests.[421]

Unfortunately, the Indian government does not details of content removal requests sent to intermediaries. There is no transparency requirement with respect to this under the IT Act, or under the Intermediaries Guidelines. As such, the government publishes no document that clarifies how many takedown requests are sent to intermediaries, and for what reasons. Occasionally, a document might surface that contains information regarding block-requests,[422] but takedown requests have so far been unavailable, except through transparency reports of intermediaries.

3.2 INTERMEDIARY LIABILITY REGIME: 2014 TO 2017

Between 2014 and 2017, two major differences have been observed: first, the state no longer requires intermediaries to self-police and self-censor content; secondly, the number of takedown requests to intermediaries have increased since 2014, though reasons for such takedowns are not always available.

3.2.1 Sub-indicator 1: State does not delegate censorship to private entities

Prior to 2014, intermediaries were required to screen and censor content on the basis of Rule 3(2) of the Intermediaries Guidelines.

Moreover, as *per se*ction 79, IT Act, and Rule 3(4) of the Intermediaries Guidelines, the intermediaries were required to take down information when intimated by governmental and judicial authorities, as well as non-governmental entities like individuals, groups or organisations. Such takedowns were many, as the intermediaries take down content as a precautionary measure to avoid liability. A study by the Centre for Internet and Society (India) showed clearly how intermediaries act to privately censor and take down content on receiving such requests, leading to a chilling effect on free speech and expression.[423]

However, with the Supreme Court's decision in *Shreya Singhal v. Union of India,*[424] the scenario shifted entirely *Shreya Singhal* challenged the constitutionality of, inter alia, Section 79 of the IT Act. The petitioners argued that the aforementioned Rules 3(2) and 3(4) of the Intermediaries Guidelines are unconstitutional, as "the intermediary is called upon to exercise its own judgment under sub-rule (4) and then disable information that is in contravention of sub-rule (2)."[425] That is, the intermediaries are called upon to judge the nature of the content complained about, and then take down such content. This is the very nature of private censorship.

While holding Section 79 and the Intermediaries Guidelines constitutional, the Supreme Court in any event read down the provision. In *Shreya Singhal*, the Supreme Court wisely put an end to private adjudication of lawfulness. Section 79(3)(b) and Rule 3(4) have been read down to mean that the intermediary must have actual knowledge of a court order or government notification. The intermediary will incur liability only if it ignores a government notification or a court order requiring takedown of content.

419 Government Requests Report: India (2014, July-December). govtrequests.facebook.com/country/India/2014-H2
420 Google Transparency Reports: India (2014, July-December). transparencyreport.google.com/government-removals/by-country/IN; Digital Empowerment Foundation. (n.d.). Op. cit., 40.
421 Twitter Transparency Report: Removal Requests. transparency.twitter.com/en/removal-requests.html#removal-requests-jan-jun-2016; Digital Empowerment Foundation. (n.d.). Op. cit., 40.
422 Digital Empowerment Foundation. (2015). Op. cit., 30: On 31 December 2014, 32 websites like vimeo.com, dailymotion.com, pastebin.com and github.com, were blocked by the Government of India Anti-Terrorism Squad (ATS), under the Blocking Rules of the IT Act 2011 for "Objectionable Con- tent" on grounds of national security.
423 Dara, R. (2012, 27 April). Intermediary Liability in India: Chilling Effects on Free Expression on the Internet. CIS India Blog. cis-india.org/internet-governance/chilling-effects-on-free-expression-on-internet
424 AIR 2015 SC 1523.
425 Ibid., 114.

Even if an intermediary chooses not to act in response to a private takedown notice – i.e., a complaint sent by an individual or other non-governmental entity – it will retain its immunity under Section 79.

Facebook, for instance, states: "In 2016, informed by the decision of the Supreme Court of India last year amending the proper interpretation of the Information Technology Act of 2000, we ceased acting upon legal requests to remove access to content unless received by way of a binding court order and/or a notification by an authorised agency which conforms to the constitutional safeguards as directed by the Supreme Court."[426] In this way, the Supreme Court has contributed to reducing the number of private censorship requests, and restricted it to the hands of the government or courts.

3.2.2 Sub-indicator 2: State requests to internet intermediaries to prevent access to content, or to disclose private information

Are:

- strictly limited to purposes such as the administration of criminal justice; and
- by order of a court or independent body.

It has been discussed earlier how the *Shreya Singhal* judgment alters the legal landscape in India for intermediary liability. Today, intermediaries lose their immunity from legal action only if they refuse to take down content on the basis of government notifications or judicial orders.

However, the Indian government routinely sends requests to intermediaries such as Google, Facebook and Twitter to take down content, as well as to disclose private information of users. While such requests have been sent prior to 2014, their number has increased drastically since then. In 2015, for instance, Google received over 1,500 requests for content removal from the Indian government,[427] 6,352 requests for user information, and 10,094 requests for user accounts from the Indian government.[428] This increased drastically in 2016, when Google received over 4,500 takedown requests,[429] 6,901 requests for user information, and 12,600 requests for user accounts.[430]

It is not only in the case of Google that the government has increased its number of requests to. Both Facebook and Twitter have received an increased number of requests since 2014. In 2015, Facebook restricted over 30,000 pieces of content, while receiving 13,286 requests for user information (Facebook's response rate was 45.3%).[431] In 2016, the number of content removals fell drastically to 2,753, while the number of user information requests rose to 18,222. [432]In the case of Twitter also, the number of content removal requests rose to 73 in 2015, while in 2016, the number rose to 140 requests.[433]

While the government does not make the reasons for its requests public, the intermediaries offer some insight into these reasons. Google, for instance, offers the following reasons for content-removal requests received by it:

426 Government Requests Report: India (2015, July-December). govtrequests.facebook.com/country/India/2014-H2
427 Google Transparency Reports: India (2015, December). transparencyreport.google.com/government-removals/by-country/IN
428 Google Transparency Reports: Requests for user information (2015, January-December). transparencyreport.google.com/user-data/overview. Google produced and handed over data to the government at the rates of 44% and 49%, respectively.
429 Google Transparency Reports: India (2016, December). transparencyreport.google.com/government-removals/by-country/IN
430 Google Transparency Reports: Requests for user information (2016, January-December). transparencyreport.google.com/user-data/overview. Google produced and handed over data to the government at the rates of 55% and 57%, respectively.
431 Government Requests Report: India (2015, July-December). govtrequests.facebook.com/country/India/2014-H2
432 Government Requests Report: India (2016, July-December). govtrequests.facebook.com/country/India/2014-H2
433 Twitter Transparency Report: Removal Requests. transparency.twitter.com/en/removal-requests.html#removal-requests-jan-jun-2016

SERVICE PROVIDER	YEAR	REASON	NUMBER OF REQUESTS
GOOGLE	2015	Religious offences	23
		Privacy and security	24
		Obscenity/nudity	29
		Defamation	49
		All others	76
		Unspecified	58
	2016	Bullying/harassment	27
		Copyright	29
		Privacy and security	52
		Defamation	72
		All others	102
		Unspecified	40

While Facebook and Twitter do not offer such a breakdown of requests and reasons as Google does, Facebook states that the "majority of content restricted was alleged to violate local laws against anti-religious speech, hate speech, and disrespect of national symbols." [434]

As such, it may be noted that the Indian government's requests to intermediaries to remove content are not solely limited to the administration of criminal justice. They include other reasons, such as defamation, privacy and copyright. However, following the decision in *Shreya Singhal*, intermediaries operating in the Indian jurisdiction are not required to remove content when sought by private entities. They will only lose their immunity if they refuse to remove content if the government or a court orders such removal. In this section, the report first looks at the existing framework for intermediary liability in India, focusing on the situation in 2014. Secondly, the report considers the major changes that have taken place between 2014 and 2017.

434 Government Requests Report: India (2016, July-December). govtrequests.facebook.com/country/India/2014-H2

SECTION 4
RIGHT TO PRIVACY AND DATA PROTECTION

In this section, the report first looks at the existing framework for privacy and data protection in India, focusing on the situation in 2014. Secondly, the report considers the major changes that have taken place between 2014 and 2017.

4.1 EXISTING FRAMEWORK FOR PRIVACY AND DATA PROTECTION

Although not expressly enumerated under Article 21, the right to privacy has been judicially included in Article 21 of the Indian Constitution, beginning with the decision in *Kharak Singh v. State of Uttar Pradesh.*[435] *Kharak Singh* involved the case of a convicted offender, who was required to report regularly to the police. The police could also make home-visits to check on the offender. The question in the case was whether such reporting and home-visits violated a right to privacy. The dissenting opinion of Subba Rao, J. held that such a violation did indeed occur, reading in the right to privacy under the fundamental right of life and personal liberty (Article 21).

Relying on a broad, residual interpretation (as opposed to the enumeration of liberties in Article 19(1)) of the term "personal liberty" in Article 21 in *Kharak Singh*,[436] the Supreme Court in *Gobind v. State of Madhya Pradesh* held privacy to be a fundamental right implicit in the concept of ordered liberty in Article 21, and included in its ambit, albeit non-exhaustively, personal intimacies of the home, family, marriage, motherhood, procreation and child-rearing. [437]A catena of cases following *Gobind* upheld the inclusion of the right of privacy within Article 21. [438]

The scope of the right to privacy was extended to include telephonic conversations in *PUCL v. Union of India*,[439] as these can often be "of an intimate and confidential character."[440] Internationally as well, it has been accepted that all forms of electronic and internet communications fall within the protection of the privacy right: Article 8 of the European Court of Human Rights has been interpreted to include this into the definition of private life.[441] In the United States, the boundaries of the sphere of privacy was set by Katz v. United States,[442] which held (Harlan, J., concurring) that privacy protection extends to all those activities or places where "a person [has] exhibited an actual (subjective) expectation of privacy" and such expectation "be one that society is prepared to recognize as 'reasonable'."

In addition to this, the procedural fairness requirement, under Article 14 generally and Article 21 specifically, for the legitimate restriction of personal liberty was expressed in *Maneka Gandhi*'s case.[443] A law purporting to restrict personal liberty reasonably must satisfy the triple test: "…(i) it must prescribe a procedure; (ii) the procedure must withstand the test of one or more of

435 AIR 1963 SC 1295.
436 Ibid., 19.
437 AIR 1975 SC 1378, 24.
438 *R. Rajagopal v. State of Tamil Nadu, AIR 1995 SC 264; Mr 'X' v. Hospital 'Z'*, AIR 1999 SC 495; *State of Maharashtra v. Bharat Shanti Lal Shah, (2008) 12 SCALE 167; Selvi v. State of Karnataka*, 2010 (4) SCALE 690.
439 AIR 1997 SC 568, 18.
440 Ibid., 19.
441 *Weber & Saravia v. Germany*, no. 54934/00 (2006); *K.U. v. Finland*, no. 2782/02 (2008); *Liberty v. the United Kingdom*, no. 58243/00 (2008).
442 389 US 347 (1967).
443 *Maneka Gandhi v. Union of India*, AIR 1978 SC 597.

the fundamental rights conferred under Article 19 which may be applicable in a given situation; and (iii) it must also be liable to be tested with reference to Article 14."[444] Further, discretionary power placed in the executive hands must be sufficiently curtailed and regulated by legislative direction, guidelines and safeguards.[445]

4.1.1 Privacy legislation

India does not, so far, have privacy legislation. Efforts have been made since 2010 to introduce a privacy law. Three drafts of the Privacy Bill have circulated, while none have yet been legislated. While the text of the draft legislations were not made public, they were leaked and civil society organisations received access.[446] In the previous report, we noted: [447]

> The 2011 version of the bill extended the Right to Privacy to all Indian citizens, and the 2014 version extends privacy rights to all Indian residents. The 2014 Bill furthermore recognises the right to privacy as a part of Article 21 of the Indian Constitution and extends to whole India including Jammu and Kashmir. Furthermore, the 2014 version of the bill exempts insurance companies and government intelligence agencies from obtaining information, collecting and processing data *in the interests of national sovereignty, integrity and security or strategic, scientific, or economic interests of India.*

4.1.2 Surveillance and monitoring

The IT Act enables the governmental to intercept and monitor internet communications *vide* Section 69. Where the central or state government or its officer think necessary or expedient "in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign states, or public order or for preventing incitement to the commission of any cognizable offence relating to the above or for investigation of any offence," they may direct any agency of the government to "intercept, monitor or decrypt… any information generated, transmitted, received or stored in any communication device."

Section 69 is accompanied by the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (the Interception Rules). The Interception Rules lay down the procedure for interception, monitoring and decryption of communication, under general circumstances as well as under emergency situations. The Interception Rules state that "No person shall carry out the interception or monitoring or decryption of any information generated, transmitted, received or stored in any computer resource … except by an order issued by the competent authority."[448] The secretary in the Ministry of Home Affairs in the central government, or the secretary in charge of Home Affairs in the state governments or Union Territories of India may issue interception orders. Such orders must be for any of the aims set out in Section 69(1), IT Act. That is, for any of the following seven reasons:

1. in the interest of sovereignty or integrity of India,
2. defence of India,
3. security of the State,
4. friendly relations with foreign states, or

444 *District Registrar and Collector, Hyderabad v. Canara Bank,* AIR 2005 SC 186, 57.
445 *PUCL v. Union of India,* AIR 1997 SC 568, 30.
446 Hikok, E. (2014, 31 March). Leaked Privacy Bill: 2014 v. 2011. *CIS India Blog.* cis-india.org/internet-governance/blog/leaked-privacy-bill-2014-v-2011
447 Digital Empowerment Foundation. (2015). Op. cit., 52.
448 The Interception Rules, Rule 3.

5. public order or
6. for preventing incitement to the commission of any cognizable offence relating to the above or
7. for investigation of any offence.

While all of the reasons may be interpreted by the government with some amount of subjectivity, it is the final reason that raises the most concern. "Investigation of any offence" may refer to any offence in the Indian penal Code, 1860, as well as any offence under tax statutes, other special legislations etc. The ambit of Section 69, IT Act, is therefore, very wide. Particularly, the central and state governments may authorise any agency of the government (including, for instance, the Central Board of Direct Taxes) to issue an order for interception, monitoring or decryption.[449] Moreover, while the Interception Rules state that the government authority or agency must consider alternative means to acquire information,[450] there is no way to check whether such means have been pursued or not. There is no requirement that the exhaustion of other means be shown under the Interception Rules.

There are four other concerns associated with the Interception Rules. First, the government authority or agency that issues the interception order is permitted to share information across other agencies for the purposes of investigation of any offence, including sharing with security agencies, as well as before a court in judicial proceedings.[451] Secondly, while information acquired through interception, monitoring or decryption is required to be destroyed by the government agency within 6 months of discontinuance of the interception[452] (and within 2 months by the intermediary who provides such information to the government[453]), the government agency can retain this information if it thinks that this information is likely to be needed for "functional requirements." Thirdly, the intermediary is given a lot of responsibility in handling interception, monitoring and decryption requests. It is required to set up a designated officer for handling these requests, and also to ensure that its employees do not use the information in any unauthorised manner[454] (if this happens, then the intermediary is liable.)[455] Such responsibility is large to place on the intermediary, as it only comes as a direction to ensure effective internal checks within its organisation. Finally, while the interception order can stay in place for a period of two months (60 days), the order can be renewed and extended for a maximum of 6 months (180 days). This is a long period for an interception order to stay in place.

There is a review process under the Interception Rules, however. An interception order, with written reasons, has to be sent to the Review Committee within seven working days.[456] The Review Committee – set up under the Indian Telegraph Rules, 1951 and comprising the cabinet secretary, secretary to the Government of India (Legal Affairs) and secretary (Department of Telecom) – meets once every two months to review interception orders.[457] If it finds that the interception order is not in accordance with the reasons given under Section 69(1) (enumerated above), then it can stop the interception and also order that all the information generated from the interception be destroyed. While this is a good provision on paper, in reality, two months may be too late.

India has had another concern with regard to surveillance of individuals and their information, the Central Monitoring System (CMS). The CMS was set up in 2011 and

449 Ibid., Rule 4.
450 Ibid., Rule 8.
451 Ibid., Rule 25(2).
452 Ibid., Rule 23(1).
453 Ibid., Rule 23(2).
454 Ibid., Rule 20.
455 Ibid., Rule 21.
456 Ibid., Rule 7.
457 Ibid., Rule 22.

became operational in 2013[458] and has the power to "access to everything that happens over India's telecommunications network – online activities, phone calls, text messages and even social media conversations."[459] Telecommunications operators are now required to hand over call data records (metadata about calls).[460] While in India, interception and monitoring can happen for the reasons enumerated in Section 69(1), IT Act, and also Section 5(2) of the Indian Telegraph Act 1881,[461] there seems to be no other law that regulates such a massive surveillance programme such as the CMS.[462]

Even if such a large surveillance and interception system has been set up, does India have the capability and technology to carry out such mass surveillance? Maria Xynou argues that India does. There are companies that provide "communication monitoring solutions to law enforcement agencies around the world" as well as "social network analysis solutions."[463] Moreover, there are surveillance technology companies that provide their products to law enforcement agencies globally. As such, the CMS is a legitimate threat to the privacy of individuals in India.

4.2 PRIVACY REGIME: 2014 TO 2017

Three major changes have cropped up in the last three years: first, existence of a 2014 draft of the Privacy Bill, which was leaked to civil society in India; secondly, the Indian Supreme Court was presented with a reference to decide whether there does exist a fundamental right to privacy under the Indian Constitution.

4.2.1 The draft Privacy Bill

While the Privacy Bill is not yet law, it is interesting to note the changes that have occurred between 2011 and 2014. In the 2014 Bill, "sensitive personal data" has been redefined to include personal data relating to:

1. physical and mental health including medical history,
2. biometric, bodily or genetic information,
3. criminal convictions
4. password,
5. banking credit and financial data
6. narcoanalysis or polygraph test data,
7. Sexual orientation.

However, if the information is already available in the public domain, then it will not be considered sensitive personal data.

"Covert surveillance" was also redefined. This includes direct surveillance, which is carried out through a device and captures information about an individual, intrusive surveillance, which is carried out by an individual or a device, and penetrates the individual's residence or private vehicle, and covert human intelligence service, which is information "obtained by a person who establishes or maintains a personal or other relationship with an individual for the covert purpose of using such a relationship to obtain or to provide access to any personal information about that individual."[464]

458 Prakash, P. (2013, 7 July). How Surveillance Works in India. India Ink, *New York Times*. india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india

459 Nandakumar, I. (2013, 7 May). Government can now snoop on your SMSs, online chats. *Gadgets Now*. www.gadgetsnow.com/tech-news/internet/Government-can-now-snoop-on-your-SMSs-online-chats/articleshow/19932484.cms

460 Xynou, M. (2014, 30 January). India's Central Monitoring System (CMS): Something to Worry About? *CIS India Blog*. cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about

461 Indian Telegraph Act. (1881). Section 5(2): …in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states, public order, for preventing incitement to the commission of an offense…

462 Xynou, M. (2014). Op. cit.

463 Xynou, M. (2013, 8 April). India's 'Big Brother': The Central Monitoring System (CMS). *CIS India Blog*. cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system

464 Hikok, E. (2014, 31 March). Op. cit.

In the 2011 Bill, there are several exceptions to privacy noted. These are:

1. Sovereignty, integrity and security of India, strategic, scientific or economic interest of the state
2. Preventing incitement to the commission of any offence
3. Prevention of public disorder or the detection of crime
4. Protection of rights and freedoms of others
5. In the interest of friendly relations with foreign state
6. Any other purpose specifically mentioned in the Act.

The 2014 Bill alters this only very slightly, removing "detection of crime" from the list. Also, under the 2011 Bill, under several circumstances, information can be gathered about an individual without it being considered a deprivation of privacy. These are:

1. For journalistic purposes unless it is proven that there is a reasonable expectation of privacy,
2. Processing data for personal or household purposes,
3. Installation of surveillance equipment for the security of private premises,
4. Disclosure of information via the Right to Information Act 2005,
5. And any other activity exempted under the Act.

Under the 2014 Bill, this is limited to only three reasons:

1. The processing of data purely for personal or household purposes,
2. Disclosure of information under the Right to Information Act 2005,
3. And any other action specifically exempted under the Act.

Disclosure and sharing of sensitive personal data is also permitted. Under the 2014 Bill, this is limited to:

1. legitimate purpose,
2. for achieving any of the objectives of Section 5,
3. the authority has by order authorized such disclosure,
4. the disclosure is required under any law for the time being in force,
5. the disclosure is made to the government intelligence agencies in the interest of the sovereignty, integrity, security or the strategic, scientific or economic interest of India.

For these purposes, sensitive personal data can be disclosed without the individual's consent. As can be seen, the 2014 Bill creates circumstances where an individual is granted the right to privacy, but also circumstances where this right can be undermined for various reasons. However, the Bill has not yet been written into law.

4.2.2 India and the fundamental right to privacy

In 2012, *Justice K.S. Puttaswamy* filed a petition in the Supreme Court, citing the lack of procedural safeguards in Aadhar, as well as the coercion to enroll in Aadhar. He also referred to the blocking of access to various schemes on account of access being permitted only through Aadhar. The main opposition to Aadhar was that, as a massive collection of biometric information, it violates the individuals' right to privacy. The government's main stand on Aadhar in the Supreme Court was that the Indian Constitution does not guarantee a right to privacy. Seeing the importance of the matter in question, through a series of petitions, the Supreme Court set up a nine-judge bench to consider the question of whether the Indian Constitution does, in fact, guarantee a right to privacy.

On 24 August 2017, the nine-judge bench of the Supreme Court, in *Justice K.S. Puttaswamy*

v. Union of India,[465] unanimously upheld the right to privacy as a fundamental right under the Indian Constitution. A historic judgment, *Justice K.S. Puttaswamy* will have far-reaching impacts. As Gautam Bhatia writes:[466]

> [The privacy judgment] will impact the interplay between privacy and transparency and between privacy and free speech; it will impact State surveillance, data collection, and data protection, LGBT rights, the legality of food bans, the legal framework for regulating artificial intelligence, as well as many other issues that we cannot now foresee or anticipate.

Justice K.S. Puttaswamy overruled the decisions of *M.P. Sharma* and *Kharak Singh*, which held that there was no right to privacy guaranteed under the Constitution. The government argued that there exists no right to privacy under the Constitution as previous judgments of the Court have held so. In *M.P. Sharma,*[467] the Supreme Court examined the extent of the Fourth Amendment of the U.S. Constitution, and concluded that the Indian Constitution does not guarantee a "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." However, as *Puttaswamy* notes (four out of nine judges comprehensively considered this argument of the government), the Fourth Amendment is not "exhaustive of the concept of privacy."[468] Insofar as *Kharak Singh* was concerned, the Supreme Court found that in order to be consistent, the Supreme Court could not have held the matter under question (visits to the house of a recidivist) to be unconstitutional without invoking the right to privacy.

The petitioners argued that privacy was implicit in human dignity, autonomy and liberty, and that without privacy, freedoms of speech, expression, religion and association were meaningless. The Supreme Court found that privacy was indeed intrinsic to liberty, guaranteed under Article 19 and Article 21. It stated that privacy was an "enabler of guaranteed freedoms," which may at times, be required to be exercised in a secluded manner. As Nariman, J. held:

> "The dignity of the individual encompasses the right of the individual to develop to the full extent of his potential. And this development can only be if an individual has autonomy over fundamental personal choices and control over dissemination of personal information which may be infringed through an unauthorized use of such information."

465 supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
466 Bhatia, G. (2017, 27 August). The Supreme Court's Right to Privacy Judgment I: Foundations. *Indian Constitutional Law and Philosophy.* indconlawphil.wordpress.com/2017/08/27/the-supreme-courts-right-to-privacy-judgment-i-foundations
467 *M.P.Sharma v. Satish Chandra*, AIR 1954 SC 300.
468 Bhatia, G. (2017, 27 August). Op. cit.

SECTION 5
ARBITRARY BLOCKING OF CONTENT

In this section, the report first looks at the existing framework for content-blocking in India, focusing on the situation in 2014. Secondly, the report considers the major changes that have taken place between 2014 and 2017.

5.1 EXISTING FRAMEWORK FOR CONTENT BLOCKING

In India, the IT Act provides for content blocking *vide* Section 69A and its corresponding rules, the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (Blocking Rules).[469] Section 69A and the Blocking Rules provide for blocking on the basis of certain enumerated reasons and process. Section 69A is as follows:

> **69A.** Power to issue directions for blocking for public access of any information through any computer resource.
> (1) Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.
> (2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.

As stated above, the central government may, if satisfied that it is necessary or expedient to do so, order the blocking of any information that is "generated, transmitted, received, stored or hosted" in any computer resources. This extends to any webpage available or hosted in India.

469 Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009. *CIS India Blog*. cis-india.org/internet-governance/resources/information-technology-procedure-and-safeguards-for-blocking-for-access-of-information-by-public-rules-2009

The procedure for website blocking is set out in the Blocking Rules, which were notified on 27 October 2009. The government must, in theory, follow the procedure set out in the Blocking Rules in order to block websites or web content. The blocking procedure is set out below.

The blocking procedure:

The blocking procedure consists of four steps.[470] First, officers with relevant designations or committees have been set up or designated; secondly, the Blocking Rules set out the procedure for blocking of content, under normal and special circumstances; thirdly, a review process to study the blocking orders is set out.

The Blocking Rules designate that certain officials shall be responsible for the content-blocking procedure.

First, the central government notifies an officer, not below the rank of Joint secretary, as the designated officer. The designated officer is the official who issues the blocking direction to the relevant intermediary or agency.[471] The group coordinator, Cyberlaw Division, Department of Information Technology (DIT) from the Ministry of Communications and Information Technology is the designated officer for India.[472]

Secondly, a nodal officer is designated by every organisation. The nodal officer receives blocking requests from any individual or group, and passes on such requests to the designated officer.[473] The Blocking Rules define organisation as "Ministries or Departments of the Government of India, State governments and Union Territories, and any Agency of the Central government notified in the Official Gazette."[474]

Thirdly, every intermediary must designated one of its offices as an Intermediary Contact. They must also designate one person to receive and handle blocking directions from the designated officer.[475]

The Blocking Rules require that the entire blocking procedure be carried out within seven days from the date on which the designated officer receives the blocking request from the nodal officer.[476] This includes the whole process, from examining a blocking request received from a nodal officer, to issuing a blocking direction to an intermediary.

How does the blocking process work? First, a request is sent to a nodal Officer of any organisation, requesting the blocking of any website or content. The nodal officer himself may also raise a blocking request. Each organisation then examines the blocking requests and, satisfied that it meets the requirements of Section 69(1), IT Act, forwards it to the designated officer with the approval of the chief secretary of the State or Union Territory. [477]

Secondly, when the designated officer receives a blocking request, he/she places it before the Committee for Examination of Requests (CER). The CER is a five-member committee comprising the designated officer (who is the Chairman of the CER), and officers from the Ministries of Law and Justice, Home Affairs, Information & Broadcasting and CERT-In (not below the rank of a joint secretary).[478] The designated officer is required to identify the person or intermediary, who hosts the content sought to be blocked. Once identified, the designated officer issues a notice to the person or intermediary, seeking their representation before the CER within 48 hours of receiving the designated officer's notice. Foreign entities hosting the information are also informed over

470 Hariharan, G. (2014, 11 December). Is India's website-blocking law constitutional? – I. Law & procedure. CIS India Blog. cis-india.org/internet-governance/blog/is-india2019s-website-blocking-law-constitutional-2013-i-law-procedure
471 The Blocking Rules, Rule 3.
472 *Vide Notification* (2010, 20 January). deity.gov.in/sites/upload_files/dit/files/Gazette1_20082010(1).pdf
473 The Blocking Rules, Rule 4.
474 Ibid., Rule 2(g).
475 Ibid., Rule 13.
476 Ibid., Rule 11.
477 Ibid., Rule 6, for the procedure set out herein.
478 Ibid., Rule 7, for the composition of the Committee for Examination of Requests.

fax/email. Following this, the CER considers "whether the request is covered within the scope of Section 69A(1)." [479]

Finally, once the CER determines that it is justifiable to block the offending content, the designated officer places the CER's recommendation before the secretary, the Department of Electronics and Information Technology (DeitY) for his/her approval. If and once approval is granted, the designated officer directs the relevant agency or intermediary to block the offending website/page.

Under emergency situations, "when no delay is acceptable", the above process may be bypassed. On the basis of written recommendations, the designated officer places the blocking request before the secretary, DeitY for his/her approval. The secretary, DeitY then issues, as an interim measure, a blocking order. This order must be placed before the CER within 48 hours of issuance. A similar procedure is followed if a court orders blocking of content. Importantly, all requests and complaints received under the Blocking Rules are to be kept confidential.[480]

A review procedure has also been set out in the Blocking Rules. The Review Committee is a body set up under Rule 419A, Indian Telegraph Rules 1951.[481] The central Review Committee comprises the cabinet secretary, secretary to the Government of India (Legal Affairs) and secretary (Department of Telecom).[482] Per the Blocking Rules, the Review Committee is to meet once every two months to evaluate the blocking directions issued by the secretary, DeitY. [483]

In the previous report, *Limited Access Restricting Expression*, it was noted that since 2006 the government has made many efforts to block web content. In 2006, for instance, the CERT-In ordered the blocking of rightwing websites (including Hindu extremist and American rightwing websites), while in 2013, 108 URLs were blocked following communal violence in the Muzaffarnagar district of Uttar Pradesh. Moreover, in 2013, the Ministry of Communications and Information Technology received over 130 court orders to block websites on various grounds.

5.2 CONTENT-BLOCKING REGIME: 2014 TO 2017

Three major aspects are relevant for the purposes of this report: first, with the Supreme Court's ruling in *Shreya Singhal*, generic bans on certain types of content have been removed; secondly, the state's blocking of websites based on lawful criteria laid down in Section 69A has been held constitutional, and finally, the number of website blocks has remained largely the same, with anecdotal evidence providing a view of the website blocking scenario in India.

5.2.1 Sub-indicator 1: There are no generic bans on content

Section V of this report covered the issue of intermediary liability. Section 79, the provision that establishes the intermediary liability regime in India, is an exemption provision. That is, an intermediary following the requirements of Section 79 is exempt from liability and immune to prosecution. As such, Section 79 is intrinsically connected to other provisions, including the website-blocking provision, Section 69A.

Prior to the Supreme Court's decision in *Shreya Singhal*,[484] there existed certain generic bans on content. As we saw in Section V of this report, Rule 3(2) of the Intermediaries Guidelines required that the intermediary put out a Terms

479 Ibid., Rule 8(4).
480 Ibid., Rule 16.
481 Ibid., Rule 2(i).
482 The Telegraph Rules (1954). Rule 419A(16). www.dot.gov.in/sites/default/files/358GI-2014 dated 8.2.2014_6.pdf
483 The Blocking Rules, Rule 14.
484 *Shreya Singhal v. Union of India,* AIR 2015 SC 1523.

of Service agreement and a Privacy Policy. In these agreements, the intermediary was to warn the users that certain types of content were unacceptable to the website. These types of content include:[485]

a. "belongs to another person and to which the user does not have any right to;

b. is grossly harmful, harassing, blasphemous defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever;

c. harm minors in any way;

d. infringes any patent, trademark, copyright or other proprietary rights;

e. violates any law for the time being in force;

f. deceives or misleads the addressee about the origin of such messages or communicates any information which is grossly offensive or menacing in nature;

g. impersonate another person;

h. contains software viruses or any other files programmes designed to interrupt, destroy or limit the functionality of any computer resource;

i. threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation."

Prior to *Shreya Singhal*,[486] the intermediary was required to proactively censor content on the basis of the criteria laid down in Rule 3(2), Intermediaries Guidelines.[487] Rule 3(4), Intermediaries Guidelines placed this responsibility on the intermediary. If the intermediary came to know – either by itself, or when brought to its knowledge by anyone (government or individual) – that such content was present on its website, it was required to acknowledge this within 36 hours, and to remove the content at the earliest. If it failed to do so, it would lose its exemption under Section 79 and be liable to prosecution. Rule 3(2)(b) is particularly problematic as it is open to highly subjective interpretation and could lead to the blocking of large swathes of content.

However, after *Shreya Singhal*, the situation has altered. The Supreme Court read down Rule 3(4) to mean that the intermediary was only required to block or take down content if ordered to do so by a court or by a competent government authority.[488] That is, the intermediary is no longer required to act as a judge, and to remove content based on its own judgment of whether certain content is unlawful or not.[489] While Rule 3(2), which sets out the above criteria for unlawfulness of content, remains, the intermediary is no longer required to proactively censor and make unavailable such content. To this extent, the presence of a generic ban on content has been reduced.

Furthermore, Section 69A, IT Act, also requires intermediaries to block content only when required to do so by a government or judicial authority. Section 69A, the blocking provision, also does not place any generic bans on content. While there exist lawful criteria on the grounds of which content may be blocked,[490] the intermediaries are not require to ban or block such content proactively.

An exception to this is the Pre-Conception and Pre-Natal Diagnostic Techniques Act 1994 (PCPNDTA). Section 22 of the PCPNDTA places a generic ban on advertisements –

485 Intermediaries Guidelines, Rule 3(2).
486 *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.
487 For a list of the criteria, see Section VII.B.i of this Report.
488 For a detailed explanation of this change in the law, see Section V.B.i of this Report.
489 *Shreya Singhal v. Union of India*, AIR 2015 SC 1523, 117-118.
490 IT Act, Section 69A(1).

print, audio or electronic, including internet advertisements – regarding "prenatal determination or sex or sex selection before conception."[491] In 2017, the Supreme Court ordered the search engines Google India Pvt. Ltd., Yahoo! India and Microsoft Corporation (I) Pvt. Ltd. to ensure deletion of materials that go counter to the PCPNDTA.[492] The Supreme Court ordered the search engines to "appoint in-house expert body which shall take steps if any words or key words that are shown on Internet and which has the potential to go counter to section 22 of the Pre-Conception and Pre-Natal Diagnostic Techniques Act 1994, shall be deleted forthwith."[493]

5.2.2 Sub-indicator 2: State blocks or filters websites based on lawful criteria

Section 69A(1) sets out certain criteria on the basis of which websites can be blocked. These are:

1. Sovereignty and integrity of India,
2. Defence of India,
3. Security of the state,
4. Friendly relations with foreign states,
5. Public order,
6. Preventing incitement to the commission of any cognizable offence relating to above.

These criteria are the only lawful criteria for website-blocking in India. In *Shreya Singhal*, the Supreme Court considered the question of whether the website-blocking provisions (Section 69A, IT Act and the Blocking Rules) are constitutional on grounds of arbitrariness and violation of freedom of expression. The petitioners, who sought to have the provision declared unconstitutional, argued that there was no opportunity for the originator of the information to be heard, as also the absence of procedural safeguards against misuse. Further, the provision requiring confidentiality of blocking orders was questioned by the petitioners. [494]

The Court held Section 69A to be constitutional, stating that it was a narrow provision. It noted that "blocking can only be resorted to where the Central Government is satisfied that it is necessary so to do." Importantly, it noted that the lawful criteria for blocking of websites or web content must be "relatable to Article 19(2)". Article 19(2) of the Indian Constitution lays down certain conditions under which freedom of expression can be curtailed in India. Along with a reasonableness criterion, Article 19(2) lays down seven reasons on the basis of which freedom of speech and expression can be curtailed. These are:

1. sovereignty and integrity of India,
2. the security of the state,
3. friendly relations with foreign states,
4. public order, decency or morality, or
5. in relation to contempt of court,
6. defamation or
7. incitement to an offence

A comparison of the criteria laid down in Section 69A and the constitutional criteria show that there is a strong similarity. The

491 Pre-Conception and Pre-Natal Diagnostic Techniques Act (1994). Section 22(1) and Section 22(2).
492 Hariharan, G. (2015, 29 January). Search Engine and Prenatal Sex Determination: Walking the Tight Rope of the Law. *CIS India Blog*. cis-india.org/internet-governance/blog/search-engine-and-prenatal-sex-determination
493 The New Indian Express. (2017, 17 February). SC Pulls Up Internet Giants Over Sex Determination Ads. The New Indian Express. www.pressreader.com/india/the-new-indian-express/20170217/282003262183283; Rajagopal, K. (2017, 11 April). Banning online pre-natal sex determination content dangerous: SC. The Hindu. www.thehindu.com/news/national/general-ban-on-online-pre-natal-sex-determination-content-may-smother-citizens-right-to-know-supreme-court/article17926261.ece
494 The Blocking Rules, Rule 16, requires that all blocking requests and complaints remain confidential.

Supreme Court referred to this relatability when holding Section 69A to be constitutional. Further, the Supreme Court was clear that Section 69A and the Blocking Rules allow for procedural safeguards. They allow for a hearing for both the originator and/or intermediary of the information sought to be blocked. However, the government is not required under the law to make the blocking direction public, nor to publicly provide a list of blocked websites. Most often, lists that become available are leaked.

5.2.3 Website blocking in India

The Indian government routinely blocks websites for a variety of reasons. For instance, in 2014, the government ordered the blocking of 32 websites, including Github, Vimeo, Weebly and Dailymotion, on the grounds that "Anti National group are using social media for mentoring Indian youths to join the Jihadi activities (sic)."[495] After considerable pressure, these websites mentioned above were unblocked. Interestingly, in 2015, in the case of the blocking of websites prior to the India-Australia Cricket Series 2014-2015, the government has also taken a stance that blocking entire websites would be an infringement of the right of access to information.[496] The government also opposed the blocking of websites after the event was over.

Also in 2015, the government on June 29 ordered the blocking of at least 40 websites that hosted "inflammatory content relating to a minority community, including posts on social media and popular video-sharing platform."[497] Further, on July 8, the government ordered the blocking of social media posts and accounts, as also videos posted on popular video-sharing platforms, "containing content aimed at inciting a particular minority community" in Myanmar. [498]

The controversial 2015 documentary I*ndia's Daughter* concerned Nirbhaya, a woman who was brutally raped in December 2014 and later succumbed to her injuries. The documentary showed both the justifications mentioned by the alleged rapists and their lawyers, as well as footage covering interviews with the victim's family. The film was hugely controversial. Citing potential unrest, the documentary was banned in India, and the government (as well as the courts) ordered that it be blocked on all video-sharing websites.[499] While netizens uploaded the video multiple times onto difference video sharing websites, they were blocked promptly, leaving the user with the message: "This content is not available on this country domain due to a court order."[500] In 2015, the government also blocked over 857 websites citing the reason of pornography under Section 79(2)(b), IT Act.[501]

Interestingly, in 2015, Google proactively blocked torrent websites such as Kickass Torrents. Google Chrome provides a warning message: "The site ahead contains harmful programmes. Attackers on (the file sharing site the user has attempted to access) might attempt to trick you into installing

495 BBC. (2015, 2 January). India 'jihadi' web blocking causes anger. *BBC News*. www.bbc.com/news/technology-30656298
496 Apoorva. (2015, 5 February). Blocking entire website infringes public's right of access to information: govt to HC. Livemint. www.livemint.com/Politics/LsKF2inpUbX4o9MJUdH5hP/Blocking-entire-website-infringes-publics-right-of-access-t.html
497 PTI. (2015, 26 July). Government orders ISPs to block websites with inflammatory content. *Gadgets Now*. www.gadgetsnow.com/tech-news/Government-orders-ISPs-to-block-websites-with-inflammatory-content/articleshow/48223714.cms
498Ibid
499 Arora, K. (2015, 6 March). Uploaded and blocked, a daylong battle rages on the web over BBC documentary. *The Times of India*. timesofindia.indiatimes.com/india/Uploaded-and-blocked-a-daylong-battle-rages-on-the-web-over-BBC-documentary/articleshow/46472422.cms
500Ibid
501 Deccan Chronicle. (2015, 4 August). Banned: Complete list of 857 porn websites blocked in India. *Deccan Chronicle*. www.deccanchronicle.com/150803/nation-current-affairs/article/porn-ban-complete-list-857-porn-websites-blocked-india

programmes that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit)." [502]Google also ranked down popular torrent websites in its search results.

In 2016, the Maharashtra Anti-Terrorism Squad blocked over 94 websites with information relating to the IS, citing the spread of IS' influence as the reason. [503]Also in 2016, the Madras High Court ordered the blocking of 830 websites, including many torrent websites, in India.[504] The John Doe order sought the blocking of all websites that provides pirate access to a film *A Flying Jatt*. Interestingly, the order directed internet service pro*vide*rs (ISPs) to "block websites that might not be in the list of 830 sites submitted to court but may indulge in piracy of *A Flying Jatt*."[505] When visiting a blocked website, the following message is seen most often by the user: "Your requested URL has been blocked as per the directions received from Department of Telecommunications, Government of India."

Most recently, in 2017, the government has ordered the blocking of websites that host or make available the Blue Whale challenge, citing the number of suicides and the adverse impacts the game has on children.[506] The Ministry of Electronics and Information Technology directed Google, Facebook, WhatsApp, Instagram, Microsoft and Yahoo to "immediately remove the links of the deadly Blue Whale Challenge, which has led several children in India and other countries to commit suicide."[507]

As can be seen, website-blocking is widespread in India. While there are lawful criteria that allow for website-blocks, it is a question of concern that the government uses the provision very often.

502 Khan, S. (2015, 14 July). Kickass Torrents, Other Sites Get Blocked by Google: Chrome Warns Users of Malware Attacks. International Business Times. www.ibtimes.co.in/kickass-torrents-other-sites-get-blocked-by-google-chrome-warns-users-malware-attacks-639202

503 The Indian Express. (2016, 25 January). Terror trail: ATS blocks 94 websites, says IS spreading influence. *The Indian Express.* indianexpress.com/article/india/india-news-india/maharashtra-cops-block-94-sites-used-to-radicalise-youth-about-isis

504 Anwer, J. (2016, 25 August). 830 more websites blocked in India, many torrent links in list. *India Today.* indiatoday.intoday.in/technology/story/830-more-websites-blocked-in-india-many-torrent-links-in-list/1/748565.html

505 Ibid

506 Financial Express. (2017, 16 August). Ban Blue Whale game: Government asks Google, Facebook, WhatsApp to remove online suicide dare. *Financial Express.* www.financialexpress.com/industry/technology/blue-whale-suicide-game-govt-orders-google-facebook-whatsapp-to-remove-dangerous-online-challenge/809026

507 PTI. (2017, 17 August). Blue Whale Challenge: Delhi HC expresses concern over internet game causing children's suicide. *Firstpost.* www.firstpost.com/india/blue-whale-challenge-delhi-hc-expresses-concern-over-app-causing-childrens-suicide-3940177.html

SECTION 6
CRIMINALISING LEGITIMATE EXPRESSION

In this section, the report first looks at the existing framework of law that criminalises online freedom of expression, focusing on the situation in 2014. Secondly, the report considers the major changes that have taken place between 2014 and 2017.

6.1 LEGAL FRAMEWORK FOR CRIMINALISATION OF ONLINE FREEDOM OF EXPRESSION

In India, the Indian Penal Code, 1860 (IPC) is the foremost law when it comes to criminalisation of online expression. The IT Act also has several sections wherein online freedom of expression is curtailed and criminalised.

6.1.1 The Indian Penal Code

In this section, we look at three instances of criminalisation of online expression: the provisions regarding sedition, hate speech and defamation.

Section 124A of the IPC deals with sedition. The section reads:

> Whoever by words, either spoken or written, or by signs, or by visible representation, or otherwise, brings or attempts to bring into hatred or contempt, or excites or attempts to excite disaffection towards, the Government established by law in India, shall be punished with imprisonment for life, to which fine may be added, or with imprisonment which may extend to three years, to which fine may be added, or with fine.

As the section makes clear, if anyone tries to bring hatred or contempt against India, or tries to excite disaffection against the government – that is, if the speech is considered disloyal or threatening to the state – he/she commits sedition. If he/she is found guilty of committing sedition, he/she may be imprisoned for life, or for three years, and a fine may be added as well.

Section 124A was upheld as constitutionally valid in the case of *Kedarnath Singh v. State of Bihar.*[508] However, the scope of the provision was narrowed down to include only those speech and actions that involve an intention or tendency to create a disturbance of law and order, or to incite violence. That is, if the speech was only a constructive criticism against the government, then it was permitted. However, even though constructive dissent is allowed, the government has used Section 124A in many instances to curb dissent. In *Aseem Trivedi,* the government arrested a cartoonist for drawing cartoons concerning corruption.[509]

Two safeguards exist for Section 124A. First, Section 196, CrPC states that the central government must give sanction or permission before a court can take cognisance of an offence under Section 124A. Secondly, a legal opinion must be given in writing by the district law officer, following which a legal opinion has to be given by the state's public prosecutor within two weeks. However, given the number of arrests under this provision, especially after 2013, gives rise to doubt about the efficacy of these safeguards.

There are two sections under the IPC for hate speech, Section 153A and 295A. While the IPC does not use the term hate speech, Sections 153A and 295A criminalise speech that deals with "the incitement of violence" and "the hurt sentiments of religious and other communities." Section 153A states that if anyone does any act – by words, speech, signs or any other visible representation – that creates "disharmony or feelings of enmity, hatred or ill-will between different religious, racial, language or regional groups or castes or communities" or "commits any act which is prejudicial to the maintenance of harmony…", or organises any exercise wherein the participants are trained to use violence against "against any religious, racial, language or regional group or caste or *community*", then he/she is guilty of an offence under Section 153A. Section 295A, on the other hand, reads as follows:

> Deliberate and malicious acts intended to outrage religious feelings of any class by insulting its religion or religious beliefs: Whoever, with deliberate and malicious intention of outraging the religious feelings of any class of citizens of India, by words, either spoken or written, or by signs or by visible representations or otherwise insults or attempts to insult the religion or the religious beliefs of that class, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

As can be seen, under Section 295A, a person must *intend* that his/her words, speech, signs or other visible representation will insult a religious group. One may wonder: if "promoting enmity between different groups" and "deliberate and malicious acts intended to outrage religious feelings" are not given as an exception to freedom of expression under Article 19(2) of the Constitution, then how are Section 153A and 295A constitutionally valid?

The answer to this lies in the case of *Ramji Lal Modi.*[510] In *Ramji Lal Modi*, the Supreme Court upheld the constitutionality of Section 295A, stating that the exception

508 AIR 1962 SC 955.
509 The Hoot. (2015, 18 March). Mere criticism is not seditious: Bombay High Court on Aseem Trivedi's cartoons. *The Hoot*. www.thehoot.org/media-watch/law-and-policy/mere-criticism-is-not-seditious-bombay-high-court-on-aseem-trivedi-s-cartoons-8177
510 Ramji Lal Modi v. State of Uttar Pradesh, AIR 1957 SC 620.

in Article 19(2) which reads, "in the interests of public order" was wide enough to include in its ambit Section 295A.

For an act to qualify as hate speech under Section 153A, it is not necessary to show intention to promote enmity or hatred. [511]If what is said or written is enough to show that it is of a nature that may create enmity or hatred, this is sufficient cause under Section 153A. Curiously, there is also no need to show that enmity or hatred in fact resulted.

Section 499, IPC defines defamation as:

> Whoever by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter excepted, to defame that person.

As the section makes clear, defamation is an offence where an individual makes or publishes an imputation regarding anyone, when it is intended harm the other person's reputation, or with the knowledge or reason that it will do so. Criminal defamation law is outdated in most countries. However, the offence is still in India's law books. In India, criminal defamation is wider in ambit than civil defamation. This is because under the IPC, it is possible to defame a group of persons, as well as a dead person.

Moreover, in India, truth is not an absolute defence in cases of criminal defamation; one must prove that the truth is for the public good. There are, however, some exceptions to defamation under the IPC. These are: truth when it is for the public good, public conduct of public servants, conduct of any person touching a public question, publication of proceedings of courts, an opinion expressed in good faith on the merits of a case or the merits of a public performance; censure made before a lawful authority in good faith.

6.1.2 The IT Act

The IT Act includes many provisions that impact and criminalise freedom of expression in India. Section 66A punishes anyone sending offensive messages through any communication service. What is considered offensive? Section 66A pro*vide*s the answer thus:

1. any information that is *grossly offensive or has menacing character*; or
2. any information which he knows to be false, but for the purpose of causing *annoyance, inconvenience, danger, obstruction, insult,* injury, criminal *intimidation, enmity, hatred or ill will*, persistently by making use of such computer resource or a communication device; or
3. any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages… (Emphasis added.)

As can be seen, many of the conditions that decide what is offensive under Section 66A are open to highly subjective interpretation. An instance in Mumbai resulted in two girls arrested and booked under Section 66A, where one of them had posted a critical view concerning the shutdown of the city due to the death of a well-known politician in Maharashtra, and the other had liked the post

511 *Gopal Vinayak Godse v. Union of India & Ors*, AIR 1971 Bom 56.

on Facebook.[512] A cartoonist, Aseem Trivedi, was arrested for his cartoons that "mocked Parliament and corruption on his website and Facebook page."[513] In fact, 375 cases were filed in Maharashtra alone. [514]

Under the IT Act, there are other provisions that target obscenity and the generation and transmission of sexually explicit photographs, or photographs of private areas of persons. These shall be discussed under the section on Gender Rights and Sexual Expression.

6.2 THREATS TO LEGITIMATE EXPRESSION: 2014-2017

In this section, we will look at three important aspects surrounding the criminalisation of free speech and expression: first, the instances of arrests and other governmental action under the guise of sedition and hate speech, and secondly, the striking down of Section 66A, IT Act as unconstitutional, and finally, the judgment in *Subramanian Swamy v. Union of India*, where the Supreme Court of India upheld the constitutionality of Section 499 and Section 500, IPC, the provisions on criminal defamation.

6.2.1 Instances of arrests for stated reasons of sedition and hate speech

In the last three years, there have been many arrests and other non-governmental assaults for reasons stated to be on account of sedition and hate speech. For instance, in May 2015, a student was arrested for allegedly posting messages on Twitter that stated that he would "kill around 3000 Muslims."[515] In July 2015 in Pune, a group of people along with the admin of a WhatsApp group were arrested for posting messages that "hurt religious sentiments." Again, in July 2015, seven young persons were arrested and booked for allegedly "hurting religious sentiments[516] by posting objectionable content" on Facebook.[517] Also in July 2015, a youth was arrested for posting allegedly objectionable content on Facebook regarding a political leader.[518]

In October 2015, the admin of a WhatsApp group was arrested for posting "objectionable content", though news reports do no make clear what the objectionable content was.[519] Again, in October 2015, a propagandist singer of a literary arts group was arrested and booked for "alleged sedition, uploading defamatory electronic content

512 Hindustan Times. (2015, 24 March). Facebook trouble: 10 cases of arrests under Sec 66A of IT Act. *The Hindustan Times.* www.hindustantimes.com/india/facebook-trouble-10-cases-of-arrests-under-sec-66a-of-it-act/story-4xKp9EJjR6YoyrC2rUUMDN.html

513 Bhardwaj, S. (2015, 25 March). Section 66A: Six Cases that Sparked Debate. *Livemint.* www.livemint.com/Politics/xnoW0mizd6RYbuBPY2WDnM/Six-cases-where-the-draconian-Section-66A-was-applied.html

514 Shaikh, Z. (2015, 20 December). 375 cases registered in Maharashtra for offensive messages online. *The Indian Express.* indianexpress.com/article/cities/mumbai/375-cases-registered-in-maharashtra-for-offensive-messages-online

515 DNA. (2015, 7 May). First-year engineering student arrested for posting spiteful message on social network. *DNA.* www.dnaindia.com/india/report-first-year-engineering-student-arrested-for-posting-spiteful-message-on-social-network-2083908#comments

516 Haygunde, C., & Kulkarni, S. (2015, 8 July). Cyber crime in Pune: Communal amity, family life take the worst hit. *The Indian Express.* indianexpress.com/article/cities/pune/cyber-crime-in-pune-communal-amity-family-life-take-the-worst-hit

517 TNN. (2015, 2 July). Seven booked for objectionable post on FB. *The Times of India.* timesofindia.indiatimes.com/city/allahabad/7-booked-for-objectionable-post-on-FB/articleshow/47910045.cms

518 PTI. (2015, 3 July). Youth Arrested for 'Objectionable' Facebook Post Against SP Leader. *The New Indian Express.* www.newindianexpress.com/nation/2015/jul/03/Youth-Arrested-for-Objectionable-Facebook-Post-Against-SP-Leader-778517.html

519 DNA. (2015, 8 October).Maharashtra: WhatsApp group admin arrested for objectionable content in Latur. *DNA.* www.dnaindia.com/india/report-maharashtra-whatsapp-group-admin-arrested-for-objectionable-content-in-latur-2132820

against Chief Minister J Jayalalithaa and disturbing public peace." [520]

In January 2016, the admin and a member of a WhatsApp group were booked under Sections 153A and 295A for allegedly posting objectionable content against the members of a particular community.[521] Again in January 2016, a man was arrested for posting derogatory comments on Facebook against the slain Lt. Col. Niranjan, one of the Pathankot martyrs; he was booked on sedition charges under Section 124A.[522]

In June 2016, an FIR was lodged against Tanmay Bhat, an Indian comedian and founder of All-India Bakchod, for creating a controversial *vide*o titled Sachin v. Lata Civil Wars; it is unclear what section of the IPC was used.[523] In September 2016, a man was arrested for posting allegedly defamatory content against Bharat Mata on a popular messaging service.[524] Again in September 2016, a blogger was arrested and booked under Section 295A, IPC, in Bengal for posting comments critical of Islam. [525]

In October 2016, seven individuals were booked for "spreading provocative messages through social media", on charges of promoting enmity between different groups on the basis of religion.[526] In December 2016, a young student was arrested in Hyderabad for posting comments on WhatsApp allegedly defaming an eatery in the city.[527]Again in December 2016, a Malayalam writer and theatre activist was taken into custody and booked on charges of sedition for allegedly insulting the national anthem.[528] In Kashmir, a young student was arrested and booked on charges of sedition for allegedly "sharing a Facebook post that praised slain Hizbul Mujahideen leader Burhan Wani."[529] Also, in July 2017, the All India Bakchod co-founder Tanmay Bhatt was booked on grounds of defamation for posting a photograph of Prime Minister Narendra Modi with a Snapchat filter with puppy ears.[530]

520 DNA. (2015, 16 November). Tamil Nadu: Court grants bail to Kovan who is facing sedition charge. *DNA*. www.dnaindia.com/india/report-court-grants-bail-to-kovan-who-is-facing-sedition-charge-2145869

521 Outlook India. (2016, 7 January). UP: WhatsApp Group Admin, Member Booked for 'Objectionable Content'. *Outlook India*. www.outlookindia.com/newswire/story/up-whatsapp-group-admin-member-booked-for-objectionable-content/926213

522 Zee News. (2016, 5 January). Man arrested for derogatory Facebook comment against Pathankot martyr Lt Col Niranjan. *Zee News*. zeenews.india.com/news/india/man-arrested-for-derogatory-facebook-comment-against-pathankot-martyr-lt-col-niranjan_1841887.html

523 The Indian Express. (2016, 1 June). Amul's new ad on Tanmay Bhat-Lata Mangeshkar controversy is spot on. *The Indian Express*. indianexpress.com/article/trending/trending-in-india/amuls-new-ad-on-tanmay-bhat-lata-mangeshkar-controversy-is-spot-on-2828874

524 Hindustan Times. (2016, 9 September). Man arrested for circulating 'objectionable' messages about 'Bharat Mata'. *The Hindustan Times*. www.hindustantimes.com/india-news/man-arrested-for-circulating-objectionable-messages-about-bharat-mata/story-pT7L4uOpLDsOQqN1cSg7gN.html

525 Mehta, P. (2016, 20 September). After TMC leader's complaint, blogger Tarak Biswas arrested in Bengal for mocking Islam. *DNA*. www.dnaindia.com/india/report-after-tmc-leader-s-complaint-blogger-tarak-biswas-arrested-in-bengal-for-mocking-islam-2257198

526 Sonawane, S. (2016, 16 October). 7 booked for cyber crime may get jail. *The Times of India*. timesofindia.indiatimes.com/city/nashik/7-booked-for-cyber-crime-may-get-jail/articleshow/54875620.cms

527 Times of India. (2016, 24 December). MBA student held over dog meat rumour on WhatsApp. *The Times of India*. timesofindia.indiatimes.com/city/hyderabad/mba-student-held-over-dog-meat-rumour-on-WhatsApp/articleshow/56153136.cms

528 Indian Express. (2016, 18 December). Malayalam writer Kamal C. Chavara taken into custody for 'insulting' national anthem. *The Indian Express*. indianexpress.com/article/cities/thiruvananthapuram/malayalam-writer-kamal-c-chavara-arrested-for-insulting-national-anthem

529 Chaturvedi, N. (2016, 3 October). Kashmiri Student Who Shared Facebook Post Praising Burhan Wani Booked For Sedition: Report. Huffington Post. www.huffingtonpost.in/2016/10/03/kashmiri-student-who-shared-facebook-post-praising-burhan-wani-b_a_21485016

530 Mangaldas, L. (2017, 17 July). How A Meme Of Indian PM Modi With Puppy Ears Provoked Police Complaints In India. *Forbes*. www.forbes.com/sites/leezamangaldas/2017/07/17/how-a-meme-of-indian-pm-modi-with-puppy-ears-provoked-police-complaints-in-india/#ff753dc6570d

As can be seen from the above examples, instances of arrests on grounds of sedition, hate speech and defamation on the internet are on the rise. Police use Section 124A, 153A and 295A often to book individuals who post constructive comments, opinions, or parodies that they think amounts to sedition or promoting enmity between different religious groups. In India, where opinions and constructive comments are an integral part of freedom of speech and expression, this is highly problematic and violative of fundamental rights.

6.2.2 Section 66A declared unconstitutional

Prior to 2015, Section 66A remained on the law books in India. Section 66A criminalises any "online communication that is "grossly offensive" or "menacing", or false information sent for the purposes of causing "annoyance, inconvenience, insult, injury, obstruction, enmity, hatred, ill will, etc."[531] These terms, which are undefined, leave it open to highly subjective interpretation. They make it difficult to predict what speech is permissible, and what speech is criminalised, under Section 66A. A chilling effect results from this, affecting the freedom of expression of individuals online. Moreover, the requirements of Section 66A fall foul of the justifications for restrictions detailed under Article 19(2) of the Indian Constitution.

A writ petition was filed in 2012, challenging, inter alia, the constitutionality of Section 66A. In the decision given in 2015[532], the Supreme Court of India struck down Section 66A as unconstitutional, on grounds of vagueness, excessiveness and the potential for a chilling effect on freedom of expression.

In coming to its decision, the Supreme Court distinguished between three types of speech: discussion, advocacy and incitement. The Court held that discussion and advocacy are integral to Article 19(1)(a), the provision guaranteeing freedom of opinion and expression. The government argued that Section 66A was saved by Article 19(2), the provision laying down the valid and legitimate restrictions on freedom of speech and expression. The government argued that public order, defamation, incitement to offence and decency and morality – the conditions enumerated in Article 19(2) – applied to make Section 66A valid and constitutional.

The Supreme Court, however, felt otherwise. It held that Section 66A makes no reference to any of the conditions laid down in Article 19(2), and also, does not amount to an incitement to an offence. Section 66A does not refer to a call to violence, does not refer to speech that could lead to imminent violence, and as such, is unconstitutional. Further, Section 66A is broad and vague, and gives way for highly subjective interpretation and misuse. The Court noted that Section 66A has, in fact, been misused, and mentioning the integrity of Article 19(1)(a), struck down the section as unconstitutional.

For freedom of speech and expression in India, the *Shreya Singhal* judgment, striking down Section 66A, is of monumental importance. It takes away the possibility of a chilling effect on speech, due to the arbitrariness, vagueness and excessiveness of Section 66A, and therefore, makes freedom of speech and expression a stronger, more integral value. However, interestingly, even after Section 66A has been struck down, we find that police have utilised the provision to file cases. For instance, in Maharashtra, the police registered a complaint against individuals under Section 66A, despite the provision being struck down in March 2015.[533] While cases under Section 66A have

531 Hariharan, G. (2015, 26 March). What the 66A Judgment Means for Free Speech Online. *Huffington Post*. www.huffington-post.in/geetha-hariharan/what-66a-judgment-means-f_b_6938110.html
532 Shreya Singhal v. Union of India, AIR 2015 SC 1523.
533 Shivadekar, S. (2015, 7 September). Nashik cops register case under Section 66A of IT Act despite SC scrapping it in March. *Mumbai Mirror*. https://mumbaimirror.indiatimes.com/mumbai/cover-story/Nashik-cops-register-case-under-Sec-66A-of-IT-Act-despite-SC-scrapping-it-in-March/articleshow/48851393.cms

dropped drastically – indeed, stopped – the provisions on sedition, hate speech and defamation continue to be widely used.

6.2.3 Criminal defamation upheld as constitutional

The case of *Subramanian Swamy* v. Union of India was a watershed in the issue surrounding the constitutionality of criminal defamation, the provisions Section 499 and Section 500, IPC. In May 2016, the Supreme Court upheld the constitutionality of criminal defamation in India, stating that in Article 19(2), "defamation" is a valid ground for reasonable restrictions on freedom of speech and expression.

The petition was filed by the Bharatiya Janata Party politician *Subramanian Swamy*. Later, politicians Rahul Gandhi, Arvind Kejriwal and others became parties to the case. The petition *Subramanian Swamy* challenged the constitutionality of criminal defamation on the grounds that criminal defamation goes beyond the grounds pro*vide*d in Article 19(2), and is excessive. The petitioners argued that defamation is essentially a private wrong, and in creating a criminal offence, it transforms this private wrong into a public one. It creates a chilling effect on freedom of speech and expression, and creates a strange situation where the threshold for prosecution under Sections 499 and 500 is lower than that for civil defamation. Many commentators have argued that the judgment is a retrograde one, when many countries are on the path to decriminalising defamation.[534] While the Supreme Court held that defamation is not merely a private wrong, as Gautam Bhatia argues, though Article 19(2) mentions defamation as a valid ground for reasonable restriction on free speech, the provision makes no distinction between defamation as a civil remedy and a criminal offence.[535]

534 Arun, C. (2016, 25 May). A question of power. *The Indian Express.* indianexpress.com/article/opinion/columns/criminal-defamation-law-supreme-court-2817406; Bhatia, G. (2016, 18 May). Why the Supreme Court's Criminal Defamation Judgment is Per Incuriam. *Indian Constitutional Law and Philosophy.* indconlawphil.wordpress.com/2016/05/18/why-the-supreme-courts-criminal-defamation-judgment-is-per-incuriam; Bhanu Mehta, P. (2016, 18 May). Supreme Court's judgment on criminal defamation is the latest illustration of a syndrome. *The Indian Express.* indianexpress.com/article/opinion/columns/supreme-court-criminal-defamation-law-subramanian-swamy-2805867

535 Bhatia, G. (2016, 13 May). The Supreme Court's Criminal Defamation Judgment: Glaringly Flawed. *Indian Constitutional Law and Philosophy.* indconlawphil.wordpress.com/2016/05/13/the-supreme-courts-criminal-defamation-judgment-glaringly-flawed

SECTION 7
INTERNET SHUTDOWNS

A relatively new phenomenon, internet shutdowns (or disconnecting users from the internet) have fast become a popular control method in the hands of the Indian government and its state governments. In this section, the Report looks at, first, the law on internet shutdowns in India, and secondly, the various instances where the Indian government has resorted to disconnecting users from the internet – most often, mobile internet services.

7.1 THE LAW ON INTERNET SHUTDOWNS

An expert definition of internet shutdowns reads:[536]

> An internet shutdown is an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information.

An internet shutdown is a "Government-imposed disablement of access to the Internet as a whole within a particular locality or localities for any duration of time."[537] In most cases, ISPs are ordered by a government agency or a court to disable access to the internet for any duration of time, ranging from a few hours to blackouts lasting days. An internet shutdown differs from content-blocking or takedown of web content in that it is a complete ban on internet services – mobile and/or broadband.

In India, internet shutdowns are, under most circumstances placed through a mechanism available in the Code of Criminal Procedure, 1973 ("CrPC"). Section 144 of the CrPC enables a district magistrate or other competent magistrate to direct any person to do or not to do certain acts, if he/she is satisfied that such direction is likely to prevent a riot, affray, disturbance to public tranquility etc. Section 144 reads:

536 *#Keepiton. Access Now.* https://www.accessnow.org/keepiton
537 About, Internet Shutdowns, slfc.in. internetshutdowns.in/about

> (1) In cases where, in the opinion of a District Magistrate, a Sub-divisional Magistrate or any other Executive Magistrate specially empowered by the State Government in this behalf, there is sufficient ground for proceeding under this section and immediate prevention or speedy remedy is desirable, such Magistrate may, by a written order stating the material facts of the case and served in the manner pro*vide*d by section 134, direct any person to abstain from a certain act or to take certain order with respect to certain property in his possession or under his management, if such Magistrate considers that such direction is likely to prevent, or tends to prevent, obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquility, or a riot, of (sic) an affray.
>
> … (3) An order under this section may be directed to a particular individual, or to persons residing in a particular place or area, or to the public generally when frequenting or visiting a particular place or area.

As the section notes, the Magistrate may direct any person to do or not to do certain acts, if he is of the opinion that such a direction will prevent:

1. obstruction,
2. annoyance or injury to any person lawfully employed, or
3. danger to human life, health or safety, or
4. a disturbance of the public tranquility, or
5. a riot, or
6. an affray.

In such a situation, a magistrate may pass order under Section 144(1), CrPC. It may be directed towards an individual, or to a group of people in a particular locality. It is important to note that such an order may stay in place for a maximum of two months, unless the state government considers it necessary, in which case it may extend for a further six months.

One may wonder how such a broadly worded section enables an internet shutdown. In theory, it may be argued that an ISP has "certain property in his possession or under his management" – that is, the infrastructure that makes access to the internet possible. Therefore, an order under Section 144 presumably directs an ISP to do an act with respect to property under his management. The legality and constitutionality of this remains under question.

Internet shutdowns violate freedom of expression and access to information. Using the test for international standards, shutdowns or internet bans are disproportional. While they are enabled by law and possibly the presence of a legitimate reason (imminent riot, affray etc.), bans create a disproportional impact on freedom of expression and access to information, as they are not a narrowly tailored restriction.

7.2 INSTANCES OF INTERNET SHUTDOWNS IN INDIA

Since 2012, India has recorded 73 internet shutdowns across different states and localities. [538]Of the 73, 49 targeted mobile internet services, while 10 targeted both mobile and fixed-line services.[539] 37 of the shutdowns were preventive in nature, anticipating law and order problems, while the remaining 36 were reactive, in response to a law and order situation.

The state of Jammu and Kashmir has seen the maximum number of shutdowns so far, which counts to 48. Rajasthan has seen 11, Gujarat 10 and Haryana nine shutdowns respectively. Most of these are not imposed state-wide, but in localities where authorities anticipate law and order problems, or where law and order problems are ongoing.

One of the most highlighted cases on internet shutdowns was those following the Hardik Patel agitation in Gujarat.[540] A politically and economically influential group, the Patels or Patidars have had several members holding top political, bureaucratic and industrial positions.[541] In 2015, they demanded to be granted status as Other Backward Classes (OBC), which would make them eligible for reservations and quotas in educational institutions and for government jobs. Multiple rallies were organised across Gujarat in August 2015,[542] with the largest rally, the *Kranti Rally*, being organised in Ahmedabad. The leader of the agitation, the young Hardik Patel, went on a hunger strike demanding that the Patidar demands be met by the government, and was arrested.[543] Violence and agitation broke out, and many were injured, businesses suffered and property was destroyed.[544] The government deployed the army, and imposed curfew across the state for a few days.

The state government also imposed an internet shutdown across different parts of Gujarat.[545] Citing "concerns of rumour-mongering and crowd mobilisation through WhatsApp" as a reason, the police sought a shutdown on mobile internet services under Section 144, CrPC.[546] The shutdown lasted six days in most of Gujarat, while Surat and Ahmedabad saw longer shutdowns.[547] The government stated that the ban was to prevent anti-social elements from using social media platforms to spread rumours.[548]

Interestingly, a Public Interest Litigation was filed before the Gujarat High Court against the internet shutdowns in Gujarat. The petitioner argued that the internet shutdown violated Articles 14, 19 and 21 of the Constitution by violating citizens' right to free speech,

538 Internet Shutdown Tracker, sflc.in. internetshutdowns.in
539 The targets of 14 shutdowns are unknown. Internet Shutdown Tracker, sflc.in. internetshutdowns.in
540 Hariharan, G. & Baruah, P. (2015, 8 October). The Legal Validity of Internet Bans: Part I. *CIS India Blog.* cis-india.org/internet-governance/blog/the-legal-validity-of-bans-on-internet-part-i
541 Kateshiya, G. (2015, 27 August). Gujarat protests: Who are the Patidars, and why are they angry? *The Indian Express.* indianexpress.com/article/explained/simply-put-who-are-gujarats-patidars-and-why-are-they-angry
542 Indian Express. (2015, 1 August). Demand for OBC status: Patidars' stir spreads to Saurashtra. *The Indian Express.* indianexpress.com/article/cities/ahmedabad/demand-for-obc-status-patidars-stir-spreads-to-saurashtra
543 PTI. (2015, 19 September). Hardik Arrested in Surat; Mobile Internet Banned. *The New Indian Express.* www.newindianexpress.com/nation/2015/sep/19/Hardik-Arrested-in-Surat-Mobile-Internet-Banned-817241.html
544 International Business Times. (2015, 26 August). Gujarat Patel Rally Turns Violent: Curfew in Ahmedabad, Surat, Mehsana, After Police Detains Hardik Patel. *The International Business Times.* www.ibtimes.co.in/gujarat-rioting-reported-several-parts-ahmedabad-patel-rally-event-turns-violent-644192; PTI. (2015, 27 August).Patidar agitation: Uneasy calm in violence-hit Gujarat, death toll rises to 10. *The Times of India.* timesofindia.indiatimes.com/india/Patidar-agitation-Uneasy-calm-in-violence-hit-Gujarat-death-toll-rises-to-10/articleshow/48699151.cms
545 PTI. (2015, 19 September). Op. cit.
546 Bhan, R. (2015, 26 August). After Clashes Over Hardik Patel's Detention, No WhatsApp in Parts of Gujarat. *NDTV.* www.ndtv.com/india-news/after-clashes-over-hardik-patels-detention-no-whatsapp-in-gujarat-1211058?pfrom=home-lateststories
547 International Business Times. (2015, 1 September). Gujarat Patel Agitation: Ban on Mobile Internet, WhatsApp Lifted in Ahmedabad? *The International Business Times.* www.ibtimes.co.in/gujarat-patel-agitation-ban-mobile-internet-whatsapp-lifted-ahmedabad-644924
548 PTI. (2015, 2 September). Patel stir: Mobile internet ban lifted in Gujarat except in Ahmedabad. *Economic Times.* economictimes.indiatimes.com/news/politics-and-nation/patel-stir-mobile-internet-ban-lifted-in-gujarat-except-in-ahmedabad/articleshow/48765090.cms?intenttarget=no

being arbitrary and excessive, and causing businesses to suffer. In any event, petitioners argued, Section 69A grants the government the power to block websites such as Facebook and WhatsApp, as a result of which the government's shutdown was excessive and arbitrary. However, the state argued that there was "sufficient valid ground for exercise of power" under Section 144, CrPC to impose a mobile internet shutdown, and in any event, broadband and WiFi services continued to be active. In its order dismissing the public interest petition, the Gujarat High Court agreed with the government that the power under Section 144, CrPC had been used as a last resort.[549]

Since then, India has seen multiple internet shutdowns. For instance, in September 2015, mobile internet services were suspended as a precautionary measure in Godhra after a derogatory message about Islam made rounds on WhatsApp.[550] This lasted for a period of 24 hours. In November 2015, internet services (all except for BSNL broadband) were shut down in the Kashmir Valley in the wake of Prime Minister Modi's rally.[551] Jammu and Kashmir saw more internet shutdowns in the wake of tensions on account of the beef ban imposed in several parts of the country,[552] as well as to prevent violence ahead of the Eid celebrations.[553] Militant activities also resulted in a shutdown of internet services, as a precautionary measure ahead of Independence Day celebrations.[554] Following the death of separatist militant Burhan Wani, Kashmir experienced a complete information blackout, with even Facebook actively removing content related to Wani.[555] Similarly, the Nagaland government blocked all internet and mobile data services in the state, in the wake of a brutal lynching of an alleged rapist, to stop the *vide*os of the lynching from circulating.[556] The Rajasthan government shut down mobile internet following communal clashes in the districts of Nagaur, Dungarpur, Udaipur, Bhilwara and other parts of the state.[557]

As can be seen, internet shutdowns have become a popular tool in the hands of the government under many circumstances, ranging from genuine threats to law and order, to precautionary measures that may not stand up to the scrutiny of the law. As a complete ban on internet services disconnects users and prevents them from accessing vital information – including information regarding health services – this is a matter of pressing concern to human rights in India.

549 *Gauravbhai Sureshbhai Vyas v. State of Gujarat.* indiankanoon.org/doc/29352399
550 Indian Express. (2015, 25 September). Gujarat: Internet services in Godhra suspended for 24 hours. *Indian Express.* indianexpress.com/article/india/gujarat/gujarat-internet-services-in-godhra-suspended-for-24-hours/.
551 PTI. (2015, 7 November). Mobile internet services blocked in Kashmir for PM Modi's rally in Srinagar. *Firstpost.* www.firstpost.com/india/mobile-internet-services-blocked-in-kashmir-for-pm-modis-rally-in-srinagar-2498760.html
552 DNA. (2015, 8 October). Beef ban: Mobile internet services cut in Jammu after tension in Udhampur. *DNA India.* www.dnaindia.com/india/report-beef-ban-mobile-internet-services-cut-in-jammu-after-tension-in-udhampur-2132781
553 Ehsan, M., & Sharma, A. (2015, 25 September). J&K suspends internet services in the state for 2 days. *The Indian Express.* indianexpress.com/article/india/india-others/to-avoid-tension-during-eid-ul-zuha-govt-ban-internet-in-jk-for-two-days-from-tomorrow
554 PTI. (2015, 15 August). Mobile phone, internet services snapped in Valley on Independence Day. *Economic Times.* economictimes.indiatimes.com/news/politics-and-nation/mobile-phone-internet-services-snapped-in-valley-on-independence-day/articleshow/48495081.cms?intenttarget=no
555 Doshi, V. (2016, 19 July). Facebook under fire for 'censoring' Kashmir-related posts and accounts. *The Guardian.* www.theguardian.com/technology/2016/jul/19/facebook-under-fire-censoring-kashmir-posts-accounts
556 Kalita, P. (2015, 9 March). Nagaland blocks internet services, imposes curfew in tense Dimapur. *The Times of India.* timesofindia.indiatimes.com/india/Nagaland-blocks-internet-services-imposes-curfew-in-tense-Dimapur/articleshow/46497164.cms
557 Mehta, A. (2015, 20 December). Rajasthan police to ban internet usage as per needs to maintain communal harmony. *The Times of India.* timesofindia.indiatimes.com/india/Rajasthan-police-to-ban-internet-usage-as-per-needs-to-maintain-communal-harmony/articleshow/50258271.cms

SECTION 8
GENDER RIGHTS AND SEXUAL EXPRESSION

In this section, the report first looks at the existing framework of law that criminalises sexual expression and affects gender rights, including online harassment, focusing on the situation in 2014. Secondly, the report considers the major changes that have taken place between 2014 and 2017.

8. 1 LEGAL FRAMEWORK FOR SEXUAL EXPRESSION

In India, laws on obscenity govern sexual expression, both offline and online. In the Indian Penal Code, 1860 (IPC), Section 292 deals with obscenity, while Section 354 deals with assault or criminal force upon a woman with the intent to outrage her modesty. There also exists a separate legislation, the Indecent Representation of Women (Prohibition) Act 1986, which prohibits indecent representation of women through advertisement or in publications, writings, paintings, figures or in any other manner. Under the IT Act, there are several provisions that criminalise obscenity and pornography, including child pornography.

8.1.1 The Indian Penal Code and Indecent Representation of Women (Prohibition) Act

Section 292 of the IPC criminalises the sale, distribution, public exhibition etc. of obscene books, and also criminalises solicitation. While the section does not criminalise private consumption of obscene or pornographic material, if found guilty, a person can be punished, "on first conviction with imprisonment… for a term which may extend to two years, and with fine which may extend to two thousand rupees (USD 30), and, in the event of a second or subsequent conviction, with imprisonment… for a term which may extend to five years, and also with fine which may extend to five thousand rupees (USD 77)."[558]

What is obscene? The section states that if a book, pamphlet, paper, writing, drawing or painting representation is "lascivious or appeals to the prurient interest", or tends to "deprave and corrupt persons" who read or are likely to read the above stated material, then this material is considered obscene.[559]

The constitutionality of Section 292 was challenged in a 1965 case, Ranjit Udeshi v. State of Maharasthra.[560] Ranjit Udeshi concerned the sale of D.H. Lawrence's book Lady Chatterley's Lover. The Supreme Court found that Section 292 was protected by the terms "decency or morality" under Article 19(2) of the Indian Constitution, which lists out conditions under which freedom of speech and expression may be reasonably restricted. Holding the section to be constitutional, the Supreme Court arrived at a definition of "obscenity":

558 Indian Penal Code. (1860). Section 292.
559 Ibid., Section 292(1).
560 AIR 1965 SC 881.

> [T]reatment of sex in a manner offensive to public decency and, judged by our national standards, considered likely to pander to lascivious, prurient or sexually precocious minds, must determine the result.[561]

The Court adopted the "Hicklin Test", which held that a work or material could be banned if it had a tendency to "deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall."[562] That is, if those who are vulnerable to moral depravity or corruption read a certain work, and there is a likelihood of the work leading to such depravity or corruption, then the whole work may be banned. In India, however, the Supreme Court held that if the work has independent artistic or aesthetic merit, then the work would be saved.

In 2014, the Supreme Court moved away from the Hicklin Test, and adopted the "community standards test". The *Aveek Sarkar* case concerned a nude photograph of the tennis player Boris Becker and his fiancée, which was meant to be in support of inter-racial relationships. The Supreme Court found that nudity is not *per se* obscene, unless it had the tendency to "arouse feeling or revealing an overt sexual desire."[563] The Court held:

> Only those sex-related materials which have a tendency of "exciting lustful thoughts" can be held to be obscene, but the obscenity has to be judged from the point of view of an average person, by applying contemporary community standards.

Under the community standards test, the Court held that three things need to be considered. First, whether an average person will find the work to be of prurient interest, applying contemporary community standards; secondly, whether the work had artistic, literary or scientific value; thirdly, whether sex or sexual conduct was depicted in a "patently offensive way". With *Aveek Sarkar,* the Supreme Court held the Hicklin Test to no longer be good law.

Under the Indecent Representation of Women (Prohibition) Act, "indecent representation of women" is defined as:

> [T]he depiction in any manner of the figure of a woman; her form or body or any part thereof in such way as to have the effect of being indecent, or derogatory to, or denigrating women, or is likely to deprave, corrupt or injure the public morality or morals.[564]

As can be seen, the tendency to deprave or corrupt continues to be a part of obscenity law in India. Interestingly, in India, offline laws do not make pornography illegal *per se*. It is the sale or distribution of obscene material that is made illegal, and private consumption of pornographic or obscene material remains legal. While there are strong parallels between the IPC and the IT Act, it is important to note that under the IT Act, punishments for dealing in obscene material are far stronger.

8.1.2 The IT Act

Several sections of the IT Act criminalise dealing in obscene material. Section 66E punishes violation of privacy. If anyone "intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent," he/she can

561 *Ranjit D. Udeshi v. State of Maharashtra,* AIR 1965 SC 881.
562 *R v. Hicklin,* L.R. 3 Q.B. 360 (1868).
563 *Aveek Sarkar v. State of West Bengal,* (2014) 4 SCC 257.
564 Indecent Representation of Women (Prohibition) Act (1986). Section 2(c).

be sent to jail for a maximum of three years, and/or fined for an amount that may go up to Rs. 2 lakhs (Rs. 200,000, USD 3,063).

Similarly, if anyone publishes on transmits in electronic form any material that is "lascivious or appeals to the prurient interest," or if the material has the effect of tending to "deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it," then he/she can be punished with imprisonment which may last for five years, and fined for an amount that may go up to Rs. 100,000 (USD 1,532).[565] If there is a second conviction, then he may be imprisoned for a maximum of 10 years, and fined for an amount not exceeding Rs. 200,000 (USD 3,063). One may notice that Section 67, IT Act bears a strong resemblance to Section 292, IPC. Despite this similarity, the punishments under Section 67, IT Act far exceed the punishments prescribed under Section 292, IPC.

Not only does the IT Act criminalise electronic material that may be "lascivious or prurient," but it also punishes anyone who publishes or transmits material that contains any "sexually explicit act or conduct."[566] Moreover, the IT Act criminalises child pornography. Anyone who publishes or transmits material containing children "engaged in sexually explicit act or conduct", or "creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material… or records" material that contain the same, or facilitates online child abuse, then he/she may, upon first conviction, go to jail for five years and/or be fined for Rs. 1,000,000 (USD 153,171), or upon second conviction, be imprisoned for up to seven years and/or be fined for Rs. 1,000,000 (USD 153,171).[567]

8.2 GENDER RIGHTS AND SEXUAL EXPRESSION: 2014 TO 2017

In the last three years, two issues stand out: first, the increasing harassment of women and LGBTQI individuals online, and secondly, the decision of the Supreme Court, upholding the constitutionality of Section 377, IPC, which criminalises even consensual sexual involvement among LGBTQI individuals.

8.2.1 Online harassment of women

The harassment of women online has been a serious problem since the advent of social media. In her paper, *Keeping Women Safe? Gender, Online Harassment and Indian law,* Richa Kaul Padte argues that India places undue emphasis on the representation of the female body and female sexuality.[568] Women who make their views on these issues public – indeed, women who speak up about social or political issues – are subjected to disproportionate abuse and harassment at the hands of trolls.[569]

The legal system is also not very supportive of women. Members of the police opine that women should be very careful of what they say and do on the internet, and in many instances, resort to blaming the victim.[570] Moreover, the police are hesitant to take First Information Reports (FIRs), for if they do, then the case must proceed to its logical conclusion, i.e., a trial in court.[571] In any event, such a case may take as many as three to four years, and in all this process, the abuser remains the least affected.[572]

In India, online harassment and abuse of women has been on the rise in the last three years. For instance, in May 2015, a woman was harassed on Facebook through its private

565 IT Act. Section 67.
566 Ibid., Section 67A.
567 Ibid., Section 67B.
568 Padte, R. K. (2013). *Keeping Women Safe? Gender, Online Harassment and Indian Law.* internetdemocracy.in/reports/keeping-women-safe-gender-online-harassment-and-indian-law
569 Kovacs, A., Padte, R. K. & Shobha, S. V. (2013). *Don't Let It Stand! An Exploratory Study of Women and Online Abuse in India.* internetdemocracy.in/wp-content/uploads/2013/12/Internet-Democracy-Project-Women-and-Online-Abuse.pdf
570 Padte, R.K. (2013). Op. cit.
571 Soni, A. (2016, 7 January). Online harassment towards women: A growing menace. *Internet Democracy Project.* internetdemocracy.in/media/online-harassment-towards-women-boomlive
572 Ibid.

messaging platform.[573] Though she publicly humiliated her abuser, many women do not enjoy such a privilege. In April 2016, a man was arrested on grounds of stalking (Section 345D) and outraging the modesty of a woman (Section 354, IPC), when he posted "derogatory language while posting comments about her and is also raising questions regarding her integrity and efficiency (sic)" on Facebook.[574] In May 2016, actress Priyamani shared her thoughts and feelings regarding the brutal gang-rape of a law student in Kerala. The actress was heavily trolled, and even labeled anti-national, until she retracted her statement and clarified that she was not criticising India, but the crime.[575] In another instance, a woman filed an FIR against an abuser who sent harassing messages to her Facebook account.[576]

8.2.2 Suresh Koushal and LGBTQI Rights

In 2009, the Delhi High Court delivered a judgment of vital importance to the LGBTQI community. In *Naz Foundation v. Government of NCT of Delhi*,[577] the constitutionality of Section 377 was challenged. Section 377 criminalises and punishes "unnatural offences". The section reads:

> Whoever voluntarily has carnal intercourse against the order of nature with any man, woman or animal, shall be punished with imprisonment for life, or with imprisonment of either description for a term which may extend to ten years, and shall also be liable to fine.

In a landmark decision, the Delhi High Court found Section 377 to be violative of Articles 14, 15 and 21 of the Constitution. The Court read down Section 377 to decriminalise consensual sexual activity between any individuals above 18 years of age. The matter went in appeal before the Supreme Court. In *Suresh Kumar Koushal*,[578] the Supreme Court overturned the decision of the Delhi High Court, and upheld the constitutionality of Section 377. The Court held that there is no violation of Article 14 (the right to equality), as there is an intelligible differentia between sexual acts against the order of nature, and acts in accordance with the order of nature, and did not address important other reasoning that the Delhi High Court went into. The *Suresh Koushal* decision is a blow to the LGBTQI community in India, as it recriminalises consensual sexual acts amongst a class of individuals that Section 377 targets – the LGBTQI community.

However, in *Justice K.S. Puttaswamy* v. Union of India,[579] the Supreme Court reverses its position. It holds incontrovertibly that sexual orientation is an essential attribute of the right to privacy, and while it does not overturn *Koushal*, it provides an indicator of the way the wind blows at the Supreme Court. *Koushal* is currently being heard by a larger bench of the Supreme Court.

573 Anand, A. (2015, 17 May). Woman's bold response to her online harasser on Facebook goes viral. *The Indian Express.* indianexpress.com/article/trending/womans-brave-response-to-her-online-harasser-on-facebook-goes-viral
574 Akhef, M. (2016, 26 April). Man booked for attempt to defame gramsevak. *The Times of India.* timesofindia.indiatimes.com/city/aurangabad/Man-booked-for-attempt-to-defame-gramsevak/articleshow/51988706.cms
575 Zee News. (2016, 10 May). Priyamani from 'Chennai Express' trolled, labelled 'anti-Indian' for speaking against Jisha gang-rape. *Zee News.* zeenews.india.com/entertainment/celebrity/priyamani-from-chennai-express-trolled-labelled-anti-indian-for-speaking-against-jisha-gang-rape_1883733.html.
576 Sarkar, G. (2016, 29 July). Woman names, shames Facebook perverts, files FIR. *Mid-day.* www.mid-day.com/articles/woman-names-shames-facebook-perverts-files-fir/17476166
577 160 DLT 277.
578 *Suresh Kumar Koushal v. Naz Foundation*, (2014) 1 SCC 1.
579 Writ Petition (Civil) No. 494 of 2012.

SECTION 9
INTERNET GOVERNANCE

In this section, the report first looks at the existing framework of law and policy for internet governance, focusing on the situation in 2014. Secondly, the report considers the major changes that have taken place between 2014 and 2017.

9.1 THE SITUATION UNTIL 2014

In the 1990s, John Perry Barlow, founder of the Electronic Frontier Foundation, wrote an idealistic Declaration of the Independence of Cyberspace. In it, he extolled the virtues of the internet, declaring that governments had no place in governing the online space. Calling it a "civilization of the mind", Barlow told governments, "You have no sovereignty where we gather."[580]

The debates about internet governance have continued ever since then. It is now understood as a matter of fact that governments *do*, in fact, have a role in governing the internet and how it works. Two concepts are of relevance when we speak of internet governance: governance on the internet, and governance *of* the internet.[581] Governance on the internet refers to governing the content that the internet provides. That is, restricting the content on the internet through laws such that those on sedition, hate speech, obscenity etc. Governance *of* the internet refers to laws and policies that govern internet infrastructure, such as spectrum, telecommunications, the Internet Corporation for Assigned Names and Numbers (ICANN), among others. When we speak of internet governance, we largely mean the latter, i.e., governance of the internet.

We now consider the Indian government's positions on internet governance. India's positions are decided by the Ministry of External Affairs (MEA), the Department of Telecommunications (DOT) and the Department of Electronics and Information Technology (DeitY) – both departments are within the Ministry of Communications and Information Technology (MCIT). While India's positions on internet governance are a matter of some confusion, it is clear that the MEA and DOT have cautiously supported a diluted form of multistakeholderism, while the DeitY has been more open.

India has repeatedly emphasised Paragraph 35 of the Tunis Agenda. The Tunis Agenda came out of the World Summit on Information Society, a UN-organised conference (the first of its kind) on internet governance and information societies. The World Summit on Information Society was organised through two conferences, in 2003 in Geneva and in 2005 in Tunis. They produced the Geneva Action Plan (2003), which delineates an action plan to achieve information society, and

580 Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. www.eff.org/cyberspace-independence
581 Kurbalija, J. (2004). *The Classification of Internet Governance*. DiploFoundation. www.diplomacy.edu/sites/default/files/Internet_Governance_Classification_ver_07102004.pdf

the Tunis Agenda, which speaks, inter alia, of internet governance. Paragraph 35 of the Tunis Agenda reads:

35. We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect it is recognized that:

1. Policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues.
2. The private sector has had, and should continue to have, an important role in the development of the Internet, both in the technical and economic fields.
3. Civil society has also played an important role on Internet matters, especially at community level, and should continue to play such a role.
4. Intergovernmental organizations have had, and should continue to have, a facilitating role in the coordination of Internet-related public policy issues.
5. International organizations have also had and should continue to have an important role in the development of Internet-related technical standards and relevant policies.

It is, therefore, clear that India supported a largely multilateral perspective on internet governance, when it supported that "policy authority for Internet-related public policy issues is the sovereign right of States." Moreover, a proposal was presented at the 66th session of the UN General Assembly, concerning a Committee on Internet-Related Policies.[582] It proposed that a UN committee be established comprising 50 member-states to deal with concerns regarding internet-related matters. It also supported, in a spirit of multistakeholderism, the establishment of advisory groups including the private sector and civil society.[583]

The Internet Governance Forum (IGF) is a multi-stakeholder platform for the discussion and learning exchange on internet governance. In 2011, India proposed that the IGF have an "outcome orientation", wherein it would contribute to the development of international law surrounding internet governance.[584] In so doing, India supported the views of many, while at the same time, accepting and supporting the multi-stakeholder nature of the IGF. However, at the IGF, India presented two different views, one supporting the multi-stakeholder nature of internet governance, and the other upholding the Tunis Agenda.

At the World Conference on Telecommunications, 2012 (WCIT), again, India presented two opposing views. On the one hand, the DOT recognised the "multi-stakeholder nature of the Internet",[585] while the MEA supported a more multi-lateral view. However, in 2013, at the IGF in Bali, the DOT sought to establish India's credibility as regards multistakeholderism, citing examples in the national fora, such as the National Telecom Policy, 2012.[586] Moreover, at the meeting of the Working Group on Enhanced Cooperation, India supported multistakeholderism.

582 India's Statement Proposing UN Committee for Internet-Related Policy. (2011, 13 October). *CIS India Blog.* cis-india.org/internet-governance/blog/india-statement-un-cirp

583 Hariharan, G. (2014, 28 October). Good Intentions, Recalcitrant Text - I: Why India's Proposal at the ITU is Troubling for Internet Freedoms. *CIS India Blog.* cis-india.org/internet-governance/blog/good-intentions-going-awry-i-why-india2019s-proposal-at-the-itu-is-troubling-for-internet-freedoms

584 TS Workshop 10: Reflection on the Indian Proposal Towards an IGF 2.0. www.intgovforum.org/cms/71-igf2011/transcripts-/913-ts-workshop-10-reflection-on-the-indian-proposal-towards-an-igf-20

585 India's Submission to the WCIT, Department of Telecom. (2012, 14 December). pib.nic.in/newsite/erelease.aspx?relid=90748

586 Indian Ministry of Communication and Technology Open Forum: Connecting a Billion Online- Learnings and Opportunities for the World's Largest Democracy. (2013, 24 October). Bali. www.intgovforum.org/cms/2013-bali/igf-2013-transcripts/121-igf-2013/preparatory-process-42721/1485-indian-ministry-of-communication-open-forum-connecting-a-billion-online-learnings-and-opportunities-for-the-worlds-largest-democracy

9.2 INTERNET GOVERNANCE: 2014 TO 2017

At NETmundial, a multistakeholder conference on internet governance, the Indian government's contribution spoke about ¶ 35 of the Tunis Agenda, which explains the different roles and responsibilities of respective stakeholders – governments ("sovereign policy authority"), the private sector (technical and economic development of the internet) and civil society (grassroots participation).[587]

However, at the 2014 IGF, India expressed "no doubt that Internet Governance mechanism require the involvement of all the stakeholders, since the evolution of Internet has been a product of many different diverse groups working together in a loosely coordinated manner," again supporting multistakeholderism and referring to the Indian Internet Governance Forum as an example of multistakeholder engagement in India.[588] Similarly, at the Plenipotentiary Conference of the International Telecommunications Union, India expressed a nuanced view, supporting a diluted form of multistakeholderism.[589]

Within India as well, the government has moved closer to multistakeholder engagements. The Telecom Regulatory Authority of India (TRAI) routinely holds multi-stakeholder consultations regarding various issues, including most recently, net neutrality. The TRAI received over 100,000 comments on its first consultation, and it continued to receive a large number of responses for later consultations. Further, India proposed to hold a national Internet Governance Forum. For this purpose, it convened a multi-stakeholder consultation in 2014, where representatives from civil society and the private sector participated. The India IGF has not yet been organised, however.

When it comes to India's participation in the international internet governance platforms, such as the WSIS, ITU, IGF and ICANN, the government has recently organised consultations where civil society and the private sector have participated. Moreover, the government's representatives routinely take part in consultations on internet governance, net neutrality, cyber security and other issues that civil society organises.

587 Government of India's initial submission to Global Multistakeholder Meeting on the Future of Internet Governance. (2014, 23-24 April). Sao Paulo, Brazil. content.netmundial.br/contribution/government-of-india-s-initial-submission-to-global-multistakeholder-meeting-on-the-future-of-internet-governance-sau-paulo-brazil-april-23-24-2014/138
588 Main Session, Evolution of the Internet Governance Ecosystem and the Future of the IGF, Main Room. (2014, 4 September). www.intgovforum.org/cms/174-igf-2014/transcripts/1977-2014-09-04-ms-evolution-of-the-ig-main-room
589 Hariharan, G. (2014, 1 November). Good Intentions, Recalcitrant Text - II: What India's ITU Proposal May Mean for Internet Governance. *CIS India Blog*. cis-india.org/internet-governance/blog/good-intentions-recalcitrant-text-2013-ii-what-india2019s-itu-proposal-may-mean-for-internet-governance

SECTION 10
FINDINGS AND RECOMMENDATIONS

This report makes clear that there are areas in which the Indian government falls short of its obligations under the International Covenant on Civil and Political Rights, as far as the internet is concerned. It also falls short, at various instances, of protecting the rights to freedom of speech and expression, assembly and association, and of privacy guaranteed to India's citizens under our Constitution. It is, however, heartening to note the increased engagement of the government with civil society and other organisations in a spirit of multistakeholderism. Placing our faith in this increased engagement, we offer the following recommendations to the government.

1. Transparency and accountability in the execution of public projects for access to the internet, such as the NOFN and Digital India Plan are essential to foster public trust. At the moment, while the public are aware of the budget outlay for the project, there is no transparency or accountability as to how the money is spent. While it may be argued that such information is available under the Right to Information Act 2005, it is strongly recommended that the government proactively disclose this information.

2. Introduce a measure of transparency in the takedown requests – as well as requests for user information – sent by the government to the intermediaries. At present, takedown requests are not made public, and even private intermediaries such as Google, Facebook and Twitter do not offer detailed explanations. Transparency in this area would go a long way in assuring citizens of the legitimate justifications for takedown of content and requests for user information.

3. It is a matter of victory that the Supreme Court has upheld the right to privacy as a fundamental aspect of Article 21. However, the declaration, while golden, is insufficient unless methods are put in place to protect the privacy of citizens. It is recommended that the government introduce transparency in its surveillance requests – at the very least, post-surveillance. This would offer to those surveilled a potential to challenge surveillance, a remedy that is currently unavailable. Also, strong checks and accountability regarding the use and sharing of data gathered upon surveillance must be put in place.

4. It is important that blocking requests and orders are made transparent. Also, a list of websites ordered to be blocked should be made public, so that we are aware of governmental requests to intermediaries. At the moment, it is only in rare instances that the public is aware of what websites have been blocked – that too, since such lists have been leaked. This must be remedied at the earliest instance.

5. It is recommended that the government decriminalise defamation, while allowing it to remain a civil remedy alone. India is among few nations yet to decriminalise defamation. It is further recommended that judicial permission be made mandatory before individuals are arrested and/or booked under charges of sedition and hate speech. At the moment, there are far too many cases of individuals wrongly accused of sedition and promoting enmity between groups, and it is a matter of utmost importance that this be checked.

6. It is strongly recommended that the practice of internet shutdowns cease in India. Such shutdowns are a clear violation of individuals' freedom of expression and access to information, including information of vital importance to the health and safety of the population. The internet, as a popular and widespread mode of communication, particularly in urban areas, is fundamental to the way people communicate. Shutting down the internet interferes with people's ability to locate information. As such, it is recommended that other, narrowly tailored, proportionate methods be pursued by government – such as website-blocking or, under extreme circumstances, takedown of content.

7. It is recommended that the government immediately decriminalise consensual sexual acts between any two individuals above 18 years of age. Section 377, which criminalises such acts, adversely impacts a class of individuals – the LGBTQI community. As such, Section 377 is unconstitutional on grounds of Article 14, 15 and 21, and must be struck down from the law books. Moreover, the government must institute special police cells and fast-track courts to deal with the matter of online harassment of women. It is a class of individuals – women – who are so affected that their right to freedom of speech and expression is curtailed due to online abuse and harassment.

8. It is a positive sign that the government engages in multistakeholder consultations on matters concerning internet governance. We encourage the government to continue and expand this process, until a robust engagement between civil society, private sector, academia and the government is well established.

CHAPTER 4

COUNTRY REPORT: MALAYSIA

SECTION 1
INTRODUCTION

1.1 OVERVIEW: FREEDOM OF EXPRESSION ONLINE IN MALAYSIA

The 2016 Freedom on the Net report by Freedom House rated Malaysia as "partly free", noting that internet freedoms "declined amid corruption allegations, as the government implemented political censorship for the first time and prosecuted critics for online speech." Though not entirely accurate, this assessment is generally true, as internet users have been arrested, investigated and prosecuted over varying forms of online speech,[590] including allegedly insulting a member of royalty by football-related trash-talking and allegedly insulting religion by commenting on the death of a divisive political figure.

While the persecution of internet users by the state loomed large in 2016 and 2017, non-state actors have become more visible as threats to freedom of expression online, particularly in cases of moral policing. Where human rights defenders and members of the opposition were more prominent as targets in 2015, ordinary internet users have now increasingly found themselves under fire for online expression.

An examination of the state of freedom of expression and related rights online in Malaysia will necessarily be grounded in the political realities and sociocultural norms of the country. This report does not claim to be comprehensive, as it is limited in its framework and scope, rather it seeks to assess the 2016 to 2017 period in the context of legal and political developments relevant to the APC-La Rue Framework.[591] Much of the information contained in EMPOWER's 2015 report remains applicable to the situation in 2017, and it can be said that the erosion of internet freedoms has since accelerated.

1.2 OVERVIEW OF THE RESEARCH

This report is an update of an earlier baseline report, State of internet freedoms in Malaysia (2015), on the state of specific rights online in Malaysia prepared by applying the APC-La Rue Framework for assessing freedom of expression and related rights on the internet. The framework is a checklist of indicators developed by the Association for Progressive Communications (APC) based on the work and recommendations of Frank La Rue, former United Nations Special Rapporteur on freedom of opinion and expression.

As in the 2015 report, this update uses a customised version of the APC-La Rue Framework to assess Malaysia's record regarding arbitrary blocking or filtering of content, criminalising of legitimate expression, imposition of internet intermediary liability, the implications of disconnecting users from the internet, cyberattacks, privacy and data protection and internet access. However, it also seeks to add to the existing indicators by considering gendered experiences of internet rights, as well as framing access in terms of freedom of information.

The 2015 report covered the period from 1 January 2014 to 15 May 2015. This report will take into account available information and reported incidents from 1 January 2016 to 12 September 2017.

---

590 https://freedomhouse.org/report/freedom-net/2016/malaysia

591 Association for Progressive Communications. (2013). *APC-La Rue Framework for assessing freedom of expression and related rights on the internet.* https://www.apc.org/sites/default/files/APC-La_Rue_Framework_digital.pdf

SECTION 2
GENERAL PROTECTION OF FREEDOM OF EXPRESSION

2.1 LEGAL AND POLICY ENVIRONMENT SINCE 2015

Of immediate and direct concern are proposed amendments to the Communications and Multimedia Act (CMA), which were announced in 2015,[592] and potentially other new legislation that would regulate online spaces and expression. The amendments were due to be tabled in 2016,[593] but were ultimately delayed pending a review of "other relevant laws."[594]

The Malaysian Communications and Multimedia Commission (MCMC) had announced in August 2015 that it would meet with 45 stakeholders "in the internet service"[595] before the CMA amendments were made. However, according to information obtained from Net Merdeka,[596] these stakeholders do not appear to include any civil society organisations (CSOs) working on internet or digital rights, such as EMPOWER, the Centre for Independent Journalism (CIJ) or the Sinar Project. Furthermore, although the government has kept the text of the amendments secret, they reportedly include higher penalties for offences under the CMA, mandatory registration of "political" bloggers and online news portals and greater powers accorded to the MCMC for taking down online content and blocking websites.[597]

It is unclear when the CMA amendments will be tabled. However, in August 2017 Communications and Multimedia Minister Salleh Said Keruak announced that his Ministry was in "the final stages" of submitting a proposal to the Attorney-General's Chambers to consider registering online portals with "high traffic," allegedly to curb "fake news or slander" and to ensure that online media reporting does not "disrupt the safety of the country or create racial disunity and play up religious sentiments."[598]

592 Net Merdeka. (2016, 15 May). Keep the internet free: Parliament should not pass problematic amendments to CMA. www.netmerdeka.org/2016/05/15/keep-the-internet-free-parliament-should-not-pass-problematic-amendments-to-cma
593 Astro Awani. (2016, 22 February). Amendment to Communications and Multimedia Act 1998 in March. *Astro Awani.* english.astroawani.com/malaysia-news/amendment-communications-and-multimedia-act-1998-march-95481
594 The Star Online. (2017, 14 January) Salleh: Govt to review all cyber-related laws to spur internet economy. *The Star Online.* www.thestar.com.my/news/nation/2017/01/14/salleh-govt-to-review-all-cyber-related-laws-to-spur-internet-economy
595 Bernama. (2015, 4 August). MCMC to meet stakeholders before amendments to communications' Acts. *The Malaysian Times.* www.themalaysiantimes.com.my/mcmc-meets-internet-stakeholders-before-amendments-to-communications-acts-jailani
596 Net Merdeka is a coalition of civil society organisations, including EMPOWER, advocating for freedom of expression and the media.
597 Joint Action Group for Gender Equality. (2016, 15 May). Consultation before Amendments: Keep the Internet Free. *Net Merdeka.* www.netmerdeka.org/2016/05/16/consultation-before-amendments-keep-the-internet-free
598 Kaur, M. (2017, 28 August). Proposal to register high traffic online sites in final stages. *Free Malaysia Today.* www.freemalaysiatoday.com/category/nation/2017/08/28/proposal-to-register-high-traffic-online-sites-in-final-stages

In August 2016, the National Security Council Act (NSC Act) came into force.[599] This law had been rushed through Parliament in December 2015[600] despite criticisms that it gave sweeping powers to a council headed by the prime minister, authorising it to establish "security areas" that could have any geographical extension and be located anywhere in Malaysia. This would entail that within such areas many checks on police and military powers would be suspended, thus allowing for arrest, search and seizure without warrant[601] merely on the suspicion of an "offence under any written law." The law also authorises security forces to limit freedom of movement into and within the security area, raising concerns over public accountability and a lack of oversight.

While the NSC Act in itself does not specifically address digital content, such as messages sent over chat applications or *vide*o recordings, it must be seen within the context of how multiple laws are used to criminalise expression. These include the Communications and Multimedia Act 1998, the Sedition Act 1948, the Penal Code and even state-level enactments such as those that establish offences under sharia law. EMPOWER's 2015 report notes that "these laws are not used in isolation from each other" and that there are similar provisions across different laws, making it possible for state authorities to choose from a buffet of legislation should any given law not be sufficient to investigate or charge an individual. Taken together, these new and proposed laws would likely further restrict online spaces for expression, which are relatively free (though increasingly regulated) compared to physical spaces.

Further, on 1 February 2017, the National Cyber Security Agency (NCSA) was implemented under the National Security Council and invested with existing legal powers, including those pro*vide*d by the CMA, the Sedition Act 1948 and the Defamation Act 1957. Cyber security is now regarded by the Malaysian government as part of its national security agenda. Seeing that there were no specific laws on cyber security in Malaysia, the government proposed a new law aimed at "protecting Malaysians from cyber security threats."[602] This would include consolidating efforts around cyber security and threats in the NCSA as the single agency. The new bill (which remained unavailable to the public at the time of writing) is expected to be tabled in the November 2017 Parliament session.

2.2 MISSING FROM THE PICTURE

There is a tendency for human rights advocacy to view freedom of expression solely within the context of political or religious expression and state obligations, without teasing out the nuances of diverse experiences based on societal norms and power differentials. When EMPOWER embarked on the research based on the APC-La Rue Framework, it found that an overwhelming majority of reported FOE-related cases identified using the framework involved men. This led EMPOWER to reconsider the framework, as it was aware of the impact of technology-related gender-based violence, such as cyberstalking and online harassment of women, through its previous work with Take Back the Tech,[603] as well as anecdotal information obtained from women's human rights organisations working on gender-based violence.

A case cited in the 2015 report is instructive: "Section 29 on public indecency in the Syariah Criminal Offences (Federal Territories) Act

599 Shaffer, L. (2016, 31 July). Malaysia's new national security law gives Najib, army, police new powers, amid 1MDB probe. CNBC. www.cnbc.com/2016/07/31/malaysias-new-national-security-law-gives-najib-army-police-new-powers-amid-1mdb-probe.html

600 Palatino, M. (2015, 4 December). Malaysia's New National Security Law: A Step Toward Dictatorship? *The Diplomat*. thediplomat.com/2015/12/malaysias-new-national-security-law-a-step-toward-dictatorship

601 Human Rights Watch. (2016, 2 August). Malaysia: New Law Gives Government Sweeping Powers. *Human Rights Watch*. *www.hrw.org/news/2016/08/02/malaysia-new-law-gives-government-sweeping-powers*

602 Farhaan Shah, M. (2017, 9 June). Zahid: Malaysia to introduce new cybersecurity law. *The Star Online*. www.thestar.com.my/news/nation/2017/06/09/zahid-malaysia-to-introduce-new-cybersecurity-law

603 www.takebackthetech.net/mapit

1997 was cited as the basis for investigating an incident where photos of three Muslim girls being hugged on stage by Korean pop singers were circulated. There were initial accusations that the girls were molested – however, rather than treating the incident as a possible case of sexual harassment, the Islamic authorities threatened to obtain warrants of arrest against the girls if they did not come forward."[604]

Is hugging Korean pop stars a form of legitimate expression protected under a human rights framework? It is a question that may initially seem ridiculous, but in unravelling possible answers we begin to see the different forms of restrictions to expression that women face online, from both state and non-state actors. EMPOWER is currently conducting research into technology-related gender-based violence and its initial findings point to complex intersections of gender, religion and race politics. Malaysian Malay-Muslim women are particularly targeted for vicious and sustained abuse online by non-state actors due to societal expectations of how they should behave – women who are outspoken, who identify as feminists or do not wear the hijab are singled out for moral policing and trolling.[605]

Cultural norms dismiss women's voices as "less important", yet the backlash against a woman with an opinion online can be overwhelmingly disproportionate. It creates a chilling effect on other women online, particularly when they are driven offline to escape the abuse. The aggressors in these instances often appear to be non-state actors: individual internet users. In the case cited above, religious authorities involved themselves in an otherwise unremarkable instance of pop singers hugging their fans in a meet-and-greet[606] after the photos were re-posted with a provocative headline on a local pop culture-focused Facebook page with no obvious affiliation with the state.

What amounts to political expression is often narrowly understood within the male experience, or the classic trope of "(male/ungendered) activist versus the state". Consider a country like Malaysia, where a woman's behaviour is surveilled and policed by her community and both religious and secular authorities, and where the backlash can exact a severe psychological and even physical price.[607] In this context, publicly posting selfies and hugging one's pop idols – behaviour often coded as feminine[608] and dismissed as trivial – can be read as acts of defiance and, indeed, political expression in the larger sense.

There is a need for more indicators within the APC-La Rue Framework to assess freedom of expression and related rights online that take into account how non-state actors can be a more present threat against legitimate expression for women, LGBT persons and other minorities. There is also the issue of the legitimisation of sexist and misogynist speech under the pretext of the right to freedom of expression, often seen in criticisms of prominent public figures who are women.[609]

604 EMPOWER. (2015). *Status of Freedom of Expression Online. Country Report: Malaysia*. https://www.apc.org/en/pubs/status-freedom-expression-online-malaysia
605 BBC News. (2017, 21 August). The online abuse hurled at Malaysia's Muslim women. *BBC News*. www.bbc.com/news/world-asia-40337326
606 Adrina. (2014). #B1A4: The Aftermath of the Controversial Special Fanmeeting in Malaysia. *hype*. hype.my/2015/37386/recap-the-aftermath-of-the-controversial-b1a4-special-fan-meeting-in-malaysia
607 BBC News. (2017, 21 August). Op. cit.
608 Tatum E. (2014, 28 April). Selfies and Misogyny: The Importance of Selfies as Self-Love. *Everyday Feminism Magazine*. https://everydayfeminism.com/2014/04/selfies-as-self-love
609 malaysiakini. (2015, 8 November). 'Bash Azalina, but don't be sexist, misogynist or other -ist'. *malaysiakini*. www.malaysiakini.com/news/318788

SECTION 3
RESTRICTION OF ONLINE CONTENT

3.1 ARBITRARY BLOCKING AND FILTERING

There is still little publicly available information on blocked websites in Malaysia, aside from occasional announcements in the media by the MCMC and the Communications and Multimedia Ministry.[610] A number of commentators and legal practitioners have questioned whether the CMA in fact gives the MCMC the legal authority to unilaterally block or filter online content,[611] However, Section 263(2) provides that Malaysian internet service providers (ISPs) are to assist the MCMC "as far as reasonably necessary in preventing the commission or attempted commission of an offence."[612] In practice, whatever the written law, ISPs generally comply with requests from the MCMC.

Early in 2016 the online publishing platform *Medium* was blocked for refusing to remove content by whistleblower site *Sarawak Report* "until it receives an order from 'a court of competent jurisdiction' to do so."[613] Also blocked were a number of blogs and the online news portal *Asia Sentinel*, for publishing news reports based on content from *Sarawak Report*,[614] though the block on *Asia Sentinel* appears to be only sporadically enforced by Malaysian ISPs.[615] *Sarawak Report* itself was blocked in 2015.[616]

On 25 February 2016, the online news portal *The Malaysian Insider* (TMI) was blocked by several Malaysian ISPs following instructions from the MCMC, over the allegation that it breached Section 233 (improper use of network facilities) of the CMA.[617] This followed reports published in TMI on the investigations into 1Malaysia Development Berhad (1MDB), a state investment fund, and the USD 680 million deposit in the personal bank accounts of Prime Minister Najib

610 Albakri, D. (2015, 10 November). Access to most popular porn websites blocked. *The Star Online*. www.thestar.com.my/news/nation/2015/11/10/most-popular-porn-sites-blocked
611 The Malaysian Insider. (2016, 26 February). MCMC has no business blocking TMI, says lawyer. *Yahoo News*. sg.news.yahoo.com/mcmc-no-business-blocking-tmi-050112034.html
612 Hong, B. (2017, 9 September). MCMC had no authority to block Steam, say legal experts. *The Malaysian Insight*. www.themalaysianinsight.com/s/14044
613 Free Malaysia Today. (2016, 29 January). MCMC blocks Medium for posting S'wak Report article. *Free Malaysia Today*. www.freemalaysiatoday.com/category/nation/2016/01/29/mcmc-blocks-medium-for-posting-swak-report-article
614 Berthelsen, J. (2016, 3 March). UN, US Call for Answers on Malaysian Press Blockages. *Asia Sentinel*. www.asiasentinel.com/politics/un-us-call-answers-malaysia-press-blockages
615 Free Malaysia Today. (2016, 21 January). Putrajaya blocks access to Asia Sentinel, says portal. *Free Malaysia Today*. www.freemalaysiatoday.com/category/nation/2016/01/21/putrajaya-blocks-access-to-asia-sentinel-says-portal
616 Persatuan Kesedaran Komuniti Selangor (EMPOWER). (2016, February). EMPOWER Malaysia: "Stop censoring information." *Association for Progressive Communications*. https://www.apc.org/en/pubs/empower-malaysia-stop-censoring-information
617 The Malaysian Insider. (2016, 2 March). Blocked websites should sue MCMC, say lawyers. *The Malaysian Insider*. www.theedgemarkets.com/article/blocked-websites-should-sue-mcmc-say-lawyers

Razak[618]. Communications and Multimedia Minister Salleh Said Keruak even described TMI's content as being equally undesirable as that of pornographic websites.[619] In March of the same year, TMI announced that it would be shutting down due to "months of pressure from the government to dissuade advertisers from working with it," with the block being the killing blow.[620]

In September 2017, the gaming platform *Steam* was blocked for not complying with the government's demand to remove access by Malaysian users to a game that allegedly threatened the sanctity of religion and racial harmony in Malaysia.[621] The game, called "Fight of Gods", depicts religious and mythological figures as characters in player-versus-player fights. The block was eventually lifted when *Steam* disabled downloads of the game for users in Malaysia.[622]

3.2 CRIMINALISING LEGITIMATE EXPRESSION

Where human rights defenders were the main focus of concern in 2015, 2016 and 2017 saw a greater visibility of ordinary internet users investigated and charged for online expression.

A significant number of reported cases involved charges for allegedly insulting members of royalty under Section 4(1) of the Sedition Act, Section 233 of the CMA and Penal Code provisions. Information obtained from the Centre for Independent Journalism's media monitoring show 27 cases involving comments regarding members of the royal family in 2017, most of them on social media platforms such as Facebook and Twitter. A significant number of these cases appear to centre around the Johor royal family and football rivalries. One such example is the case of a 46-year-old Kelantanese fisherman, Nik Pa, who was arrested in May 2016, while at sea, for posting allegedly insulting comments about the Johor crown prince in response to the arrest of Pahang football[623] supporter Masyur Abdullah.[624] He was investigated under Section 233 of the CMA. His son was also arrested for allegedly insulting the Johor crown prince on Facebook.[625]

Internet users posting content critical of the government were also targeted for arrests and investigations. In one such case, a 21-year-old Sarawakian homemaker was arrested and investigated in June 2016 under Section 507 of the Penal Code and Section 233 of the CMA for posting an allegation of police bribery related to online gambling, extortion

618 Mollman, S. (2016, 14 March). A news website that reported on the Malaysian prime minister's alleged corruption is shutting down. *Quartz*. http://qz.com/638369/a-news-website-that-reported-on-the-malaysian-prime-ministers-alleged-corruption-is-shutting-down

619 Kanyakumari, D. (2016, 22 March). Salleh Keruak: TMI "undesirable" just like porn sites. *The Star Online*. www.thestar.com.my/news/nation/2016/03/22/salleh-keruak-tmi-undesirable-just-like-porn-sites

620 Holmes, O. (2016, 15 March). Independent Malaysian news site closes amid government clampdown on media. *The Guardian*. www.theguardian.com/world/2016/mar/15/independent-malaysian-insider-news-site-closes-government-media-clampdown

621 Channel NewsAsia. (2017, 8 September). Malaysia blocks 'Fight of Gods' video game for threatening religious, racial harmony. *Channel NewsAsia*. www.channelnewsasia.com/news/technology/malaysia-blocks-fight-of-gods-video-game-for-threatening-9199460

622 Jones, A. (2017, 13 September). Fight of Gods is now banned in Thailand, too. *PCGamesN*. www.pcgamesn.com/fight-of-gods/steam-blocked-malaysia-fight-of-gods

623 Malay Mail Online. (2016, 31 May). Fisherman nabbed for allegedly insulting TMJ via Facebook. *Malay Mail Online*. www.themalaymailonline.com/malaysia/article/fisherman-nabbed-for-allegedly-insulting-tmj-via-facebook

624 The football rivalry between Johor and Pahang has recently worsened due to politics. For further context, see: Vick, V. (2017, 30 March). Asia's Biggest Rivalries: Johor Darul Ta'zim vs Pahang FC. *FourFourTwo*. www.fourfourtwo.com/my/features/asias-biggest-rivalries-johor-darul-tazim-vs-pahang-fc?page=0%2C1

625 Ashraf, K. (2016, 16 June). Rakyat Johor lapor polis kerana sayangkan TMJ. *Free Malaysia Today*. www.freemalaysiatoday.com/category/bahasa/2016/06/16/rakyat-johor-lapor-polis-kerana-sayangkan-tmj

of foreign workers and traffic offences on the Miri Complaint Community Facebook page on 5 June 2016.[626] In November 2016 opposition assemblyman Abdul Yunus Jamhari was investigated by the MCMC under Section 233 of the CMA for allegedly insulting the prime minister on 22 October in posts on his Facebook page "Rakyat Marhaen". Access to the Facebook account was allegedly blocked after he posted Fahmi Reza's satirical clown caricature of the prime minister with the caption "Bapa Songlap Negara" (translated as "Father of Corruption", with "songlap" being a colloquial term for taking something without permission, usually money).[627]

Religion continued to be a flashpoint throughout the monitoring period. Former journalist Sidek Kamiso was arrested on 19 September 2016 under Section 298A of the Penal Code and Section 233 of the CMA for posting what was considered an offensive comment on Twitter. The tweet, which alluded to the death of the spiritual leader of the Islamic Party of Malaysia (PAS), Haron Din, read: "Someone who made his career out of selling air jampi[628] for any illness succumbed to his illness in a modern hospital in San Francisco. #irony."

The police failed to get an extension to remand him under Section 117 of the Criminal Procedure Code. He was, however, rearrested on 29 September 2016 following a police report against him for allegedly insulting Islam.[629] At least two other individuals were also arrested for similar allegedly insulting posts in their social media regarding Haron Din's death.[630]

While it is largely social media users who have been targeted, messages sent through chat applications, even in private, may also be subject to prosecution. Malaysians are large consumers of news through the chat application WhatsApp,[631] and this may make them especially vulnerable to crackdowns on chat applications. In July 2016, a 76-year-old man was arrested and remanded for six days for investigation under Section 233 of the CMA on charges of circulating an allegedly offensive image of the prime minister in a WhatsApp political discussion chat group. The arrest was made after a police report was filed by another member of the chat group.[632] Almost a year later, on 28 April 2017, Deputy Communications and Multimedia Minister Jailani Johari warned WhatsApp chat group administrators that they could face prosecution if members of their groups posted "fake news".[633] Following his statement, on 3 May the MCMC issued advisory guidelines for administrators of WhatsApp chat groups.[634]

It is noted that there was at least one arrest connected to what appears to be a genuine case of incitement to violence or hate speech. Hardliner politician Jamal Md Yunos was remanded for two days for investigation under Sections 500 and 503 of the Penal Code and Section 233 of the CMA over a Facebook post threatening participants of the then-upcoming Bersih 5 rally:

626 The Malay Mail Online. (2016, 6 June). Housewife who made allegations against Miri police on Facebook arrested. *The Malay Mail Online*. www.themalaymailonline.com/malaysia/article/housewife-who-made-allegations-against-miri-police-on-face-book-arrested

627 Mat Arif, Z. (2016, 1 November). PKR assemblyman gives statement to MCMC over Facebook post. *New Straits Times*. www.nst.com.my/news/2016/11/184941/pkr-assemblyman-gives-statement-mcmc-over-facebook-post

628 "Air jampi" is a form of treatment rooted in folk religion, considered to be a cure-all.

629 The Malay Mail Online. (2016, 29 September). Catch and release again for ex-journalist Sidek Kamiso. *The Malay Mail Online*. www.themalaymailonline.com/malaysia/article/catch-and-release-again-for-ex-journalist-sidek-kamiso

630 Azlee, A. (2016, 19 September). IGP: Police probing Jeff Ooi over Haron Din tweet. *Malay Mail Online*. www.themalaymailonline.com/malaysia/article/igp-police-probing-jeff-ooi-over-haron-din-tweet and SUARAM Human Rights Report Overview 2016, p. 19, www.suaram.net/wordpress/wp-content/uploads/2016/12/Overview-2016-Digital-Edition.pdf

631 The Malaysian Insight. (2017, 11 September). Malaysians top WhatsApp news consumers. *The Malaysian Insight*. www.themalaysianinsight.com/s/14206

632 The Star Online. (2016, 3 July) Senior citizen held over insulting photo of PM. *The Star Online*. www.thestar.com.my/news/nation/2016/07/03/senior-citizen-held-over-insulting-photo-of-pm

633 Zainal, F., Chiam Shiying, C. and Aravinthan, R. (2017, 28 April). WhatsApp admins may face action. *The Star Online*. www.thestar.com.my/news/nation/2017/04/28/whatsapp-admins-may-face-action-they-can-be-punished-for-spreading-fake-news

634 Official Portal of the Malaysian Communications and Multimedia Commission. www.mcmc.gov.my/media/announcements/peringatan-untuk-pentadbir-kumpulan

> "Saya berjanji Tragedi 13 MAY akan berulang dan PARANG TERBANG akan terjadi jika BERSIH 5 dibuat pada masa, tarikh dan tempat yang sama dengan perhimpunan #BERSIH5 yang dijadualkan pada 19 November ini. Hidup Melayu!"
>
> Translation:
>
> *I promise that the tragedy of 13 May635 will repeat itself and that machetes will fly if Bersih 5 takes place at the same time, date, and place as the #BERSIH5 rally scheduled on 19 November. Long live Malays!*

He later denied posting the statement and claimed that his Facebook account had been hacked.[636] Cases such as this appear to be extremely rare, however, in comparison with the overwhelming number of cases where legitimate expression was targeted by the authorities. Mere rudeness, irreverence (such as graphic artist Fahmi Reza's satirical caricatures of the prime minister[637]) or allegedly unwarranted criticism do not meet the criteria for hate speech, regardless of how they are defined in the context of Malaysia's norms and diverse cultures.

3.3 IMPOSITION OF INTERNET INTERMEDIARY LIABILITY

It is difficult to accurately assess the extent to which Malaysia meets the criteria under internet intermediary liability in the APC-La Rue Framework, as the MCMC does not always disclose content removal requests and instructions sent out to ISPs. As noted above, Malaysian ISPs generally comply with instructions from the MCMC on blocking websites and, as was the case with *Medium* and *Steam*, the Malaysian government has been reported to have requested that content be removed even when it is hosted outside the country.

As noted in EMPOWER's 2015 report, under the 2012 amendments to the Evidence Act, owners, administrators, and editors of websites open to public contributors (including comments), web hosting or internet access providers and owners of devices used to publish content online are liable for content published through their sites, services or devices.[638] Neither EMPOWER nor the CIJ recorded any cases during the monitoring period in which Section 114A was used against internet users or service providers; however, state authorities have an embarrassment of legislative riches to use against them, as well as accepted practices that are not written law.

3.4 DISCONNECTING USERS FROM THE INTERNET

No available updated data.

3.5 CYBERATTACKS

The Malaysian government has not been known to directly carry out cyberattacks. However, the Najib administration has

635 A series of racial riots in 1969, largely centred in the capital city of Kuala Lumpur.
636 The Malay Mail Online. (2016, 6 August). Policeman detained over racist comments on Facebook. *The Malay Mail Online*. www.themalaymailonline.com/malaysia/article/policeman-detained-over-racist-comments-on-facebook
637 Looi, S. (2016, 10 June). Fahmi Reza in the dock again over posting offensive image. *New Straits Times*. www.nst.com.my/news/2016/06/150920/fahmi-reza-dock-again-over-posting-offensive-image
638 Smith, D. (2012, 14 August). Internet Blackout in Malaysia: Netizens Protest Evidence Act Amendment S114A. International Business Times. www.ibtimes.com/internet-blackout-malaysia-netizens-protest-evidence-act-amendment-s114a-743134

been assiduously courting social media influencers,[639] including an app launched in 2016,[640] and the ruling regime has long been accused of supporting "cybertroopers" who attack opposition politicians and critics.[641]

It should also be emphasised that not all attacks carried out by "cybertroopers" and trolls could be said to be state-sponsored – rather, the point is that the Malaysian government has created an environment of impunity for cyberattacks that do not threaten the religious and sociopolitical status quo. This is one area where the APC-La Rue Framework could be updated to take into account the "outsourcing" of cyberattacks to non-state actors, as well as cyberattacks independently initiated by non-state actors. Much of the attention on cyberattacks has focused on political expression and less so on, for example, Malaysian Malay-Muslim women who face sustained attacks, such as constant trolling and attempted cracking of their social media accounts, for expressing opinions that do not conform to societal expectations.[642]

3.6 PROTECTION OF THE RIGHT TO PRIVACY AND DATA PROTECTION

The Personal Data Protection Act 2010 offers limited protection in the context of commercial transactions: however, there are no safeguards or checks on state use of personal data.

State surveillance remained a concern throughout 2016-2017, including social media surveillance by the police. Since it was established in 2016, the Police Cyber Investigation Response Centre (PCIRC) has tweeted out warnings to Malaysian Twitter users through its account @OfficialPcirc. In January 2016 it made several announcements of investigations into numerous users and "tagged twitter user @IzzatCheng, informing him that he was under police observation for calling them unflattering names and accusing them of corruption."[643]

There have also been incidences of internet users being ordered to surrender the passwords of their social media accounts to facilitate police investigations. Section 116B of the Criminal Procedure Code empowers the police to request passwords, encryption codes, decryption codes, software or hardware to enable access to any computerised data. In May 2016, Yeu Bang Ken, an independent candidate for the Bawang Assan constituency in Sarawak, was charged under Section 249 of the CMA for refusing to hand over his Facebook username and password in a police investigation conducted the year before as a result of a comment posted on his Facebook page.[644]

Also of concern are issues of internet users, particularly women, being doxxed and stalked by organised trolls; however, this needs more research. The issue of doxxing can be considered in an expansion and update of the APC-La Rue Framework, given its use both to violate human rights as well as to expose perpetrators of violations.[645]

639 The Star Online. (2017, 12 June). Najib reminds social media users to spread positive news about country. *The Star Online*. www.thestar.com.my/news/nation/2017/06/12/najib-reminds-social-media-users-to-spread-positive-news-about-country
640 Asian Correspondent Staff. (2016, 12 October). PM Najib reaches out to social media users with new mobile app. *Asian Correspondent*. http://asiancorrespondent.com/2016/10/malaysia-pm-najib-reaches-social-media-users-new-mobile-app
641 Kit Siang, L. (2012, 16 July). Najib's 1Malaysia Social Media Conventions to raise an army of over 10,000 UMNO/BN cyber-troopers most anti-national in their utter disregard of 1Malaysia objective to create an united, harmonious and ethical Malaysian society. *Lim Kit Sian for Malaysia*. blog.limkitsiang.com/2012/07/16/najibs-1malaysia-social-media-conventions-to-raise-an-army-of-over-10000-umnobn-cybertroopers-most-anti-national-in-their-utter-disregard-of-1malaysia-objective-to-create-an-united-harmon
642 BBC News. (2017, 21 August). Op. cit.
643 malaysiakini. (2016, 3 February). Meet Malaysia's new Twitter police - @OfficialPcirc. *malaysiakini*. www.malaysiakini.com/news/329176
644 The Borne Post. (2016, 7 May). Independent candidate Yeu facing charge under Communication and Multimedia Act 1998. *The Borne Post*. www.theborneopost.com/2016/05/07/independent-candidate-yeu-facing-charge-under-communication-and-multimedia-act-1998
645 Bowles, N. (2017, 30 August). How 'Doxxing' Became a Mainstream Tool in the Culture Wars. *The New York Times*. mobile.nytimes.com/2017/08/30/technology/doxxing-protests.html

SECTION 4
ACCESS

4.1 ACCESS TO THE INTERNET

According to 2016 statistics obtained from the MCMC,[646] the broadband penetration rate for Malaysia per 100 households stands at 81.5 percent, with mobile broadband making up 92 percent of broadband subscriptions. Internet access, however, is not distributed equally: despite Malaysia's population being split almost evenly between men and women, less than half (42.6 percent) of internet users are women. A majority of internet users are within the 20 to 34 age range, with numbers dropping off after the 40-year mark.

There are also differences between Malaysian states. While access to computers does not necessarily correlate with access to the internet, there is a clear difference in *quality* of access between a mobile device and a personal computer. In Selangor, Malaysia's wealthiest state, 82.5% of all households have access to computers. In comparison, only 50.3% of households in Kelantan have computer access.

4.2 ACCESS TO INFORMATION

EMPOWER's 2015 report touched on access to information as a component for assessing freedom of expression and related rights on the internet and the limited legislative framework for freedom of information (FOI) in Malaysia.

Since the publication of the report, EMPOWER has carried out research into freedom of information online in Malaysia, including under FOI enactments in the states of Selangor and Penang. The unpublished research paper notes that the weaknesses of state-level enactments could be overcome through the use of the internet. It states:

> Proactive disclosure of information online would reduce the need to pay costly fees for the information and a centralised website of released information would cut costs and remove the restrictions on the use of information for specified purposes.[647]

Both Selangor and Penang impose fees for FOI requests, but when a CSO did a number of test cases in Selangor, it found that the fee of RM 12 (about USD 3) was usually waived for their FOI requests. Penang imposes a significantly higher application fee of RM 50 (about USD 12) per document for information from the current year, and RM 100 (about USD 24) for information from past years.[648]

Unlike Selangor, before releasing any information to FOI applicants Penang also requires that they sign statutory declarations stating what they intend to do with the information. An applicant in Penang who uses "any information obtained under this Enactment contrary to the reasons and purposes of such information was applied for" may be liable to a fine not exceeding RM 50,000 (about USD 12,033) or to imprisonment for a term of no more than two years, or both, if convicted.

646 Official Portal of the Malaysian Communications and Multimedia Commission. www.mcmc.gov.my/skmmgovmy/media/General/pdf/Statistical-Pocket-Book-2016-Special-Edition_latest.pdf
647 EMPOWER, unpublished paper.
648 malaysiakini. (2015, 3 August). Reduce exorbitant FOI fees, Penang told. *malaysiakini*. www.malaysiakini.com/news/307146

SECTION 5
RECOMMENDATIONS

5.1 A STRATEGIC DILEMMA?

The situation in Malaysia poses a dilemma for CSOs and activists working to better protections for human rights online. It is clear that the political trend does not favour legislative solutions, given the historical tendency to abuse overly broad laws to suppress dissent. There is also a risk that legislation aimed at rights protection will be used by the Malaysian government as leverage[649] to consolidate political power.

Repealing laws cannot be the only advocated solution. Specific and actionable measures are needed to address technology-related violence, particularly in cases of gender-based violence[650] where available laws are inadequate[651] and/or weakly enforced and where violence against specific groups of people targeted for their gender identity and expression (including trans women) is tolerated.[652] A survey conducted by the Malaysian Centre for Constitutionalism and Human Rights (MCCHR) through the PeopleACT coalition found that slightly more than half (50.4%) of the 522 respondents had experienced online harassment at least once and that women were more likely to experience online sexual harassment and death or rape threats.[653] This points to a need for solutions that address the problems at the societal level, as well as some measure of legal reforms.

The state has the resources to implement long-term policy solutions aimed at strengthening human rights online and offline, such as overhauling the education system to introduce a rights-based education, working together with CSOs. It is thus a question of political will on the part of the state and further discussions and capacity-building on the part of civil society.

5.2 RECOMMENDATIONS

FOR THE GOVERNMENT:

a. Repeal repressive laws and amend legislation to strengthen protection for the right to freedom of expression.

> Legal provisions that impose limits to freedom of expression must be amended so that limitations are predicated on demonstrable, direct and immediate threats to persons, groups and national security, not vague or entirely subjective definitions such as "insult", "ill-will" and "disharmony."

649 malaysiakini. (2017, 4 September). Give us two-thirds to end unilateral conversion, Najib tells women.
650 Joint Action Group for Gender Equality (JAG). (2017, 4 April). Press Statement: Changes to Domestic Violence Law Good; Now Step-Up Enforcement. *Women's Aid Organisation.* www.wao.org.my/news_details.php?nid=393&ntitle=Press+Statement:+Changes+to+Domestic+Violence+Law+Good;+Now+Step-Up+Enforcement
651 Kaur, M. (2017, 25 July). Amendment to Domestic Violence bill passed. *Free Malaysia Today.* www.freemalaysiatoday.com/category/nation/2017/07/25/amendment-to-domestic-violence-bill-passed
652 Committee on the Elimination of Discrimination against Women (CEDAW). (2017). Critical issues and questions to be raised with the Malaysian government at the 69th CEDAW Pre-Sessional Working Group. UN Treaty Body Database. tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/MYS/INT_CEDAW_NGO_MYS_27648_E.pdf
653 PeopleACT. (2017, 3 April). Survey on how cyberharassment affects Malaysians 2016. People *Against Cyber Threats/Harassment (PeopleACT).* http://cdn.lb.my/sites/9/20170407164521/SURVEY-ON-HOW-CYBERHARASSMENT-AFFECTS-MALAYSIANS_FINAL.pdf

b. Establish and implement human rights education at the primary level.

Human rights education should be integrated into school curriculums to further strengthen respect for and protection of the right to freedom of expression, with the aim of fostering equality and non-discrimination as democratic values rather than threats to religion and culture.

c. Encourage dispute resolutions through private remedies.

Rather than criminal prosecutions or civil suits, an independent multistakeholder body can be created to mediate disputes on online content.

d. Enact freedom of information legislation and provide freely accessible key documents online.

Freedom of information legislation must be premised on the idea that information belongs to the people, not governments. Key documents on issues of public interest such as government tenders and amendments to laws must be made available online in a timely manner. Proposed amendments to laws and draft bills should be made public a few months before they are tabled and debated in Parliament. Documents such as environmental impact assessment reports and electoral boundary maps should be freely available online.

e. Incorporate a human rights framework into the work of the Attorney-General's Chambers, based on international human rights instruments and norms.

Any new laws that are drafted must be consistent with international human rights standards, including "cyber security" laws, and enhance rather than curtail individual enjoyment of human rights.

f. Set up multi-stakeholder bodies for policy-making on human rights online.

Government policies should be drafted and/or considered by diverse multistakeholder bodies from the initial drafting stage, with clear guidelines based on international human rights standards.

FOR PARLIAMENT:

a. Set up bipartisan committees for open and public consultation on laws.

Draft bills must go through a process of public consultation in their inception. Parliamentary committees should be proactive in engaging the public and CSOs for input into draft laws.

b. Draft laws to strengthen the right to privacy and data protection.

Laws on data protection must explicitly include state bodies and institutions, as well as non-commercial transactions.

FOR THE MINISTRY OF COMMUNICATIONS AND MULTIMEDIA AND THE MALAYSIAN COMMUNICATIONS AND MULTIMEDIA COMMISSION:

a. Engage and work with human rights experts on freedom of expression issues.

The Ministry and the MCMC should institutionalise a working relationship

with the Human Rights Commission of Malaysia (SUHAKAM) and CSOs to build their competency on protecting human rights online.

b. Conduct consultations with civil society groups on amendments to the Communications and Multimedia Act and other laws related to the internet.

The Ministry and the MCMC should consult with a wide range of civil society groups on any new laws and amendments to existing laws related to the internet, including the CMA, before they are tabled in Parliament.

FOR SUHAKAM AND CIVIL SOCIETY ORGANISATIONS:

a. Build capacity on the protection of human rights online.

SUHAKAM and CSOs should build their own capacity and that of the public on the right to freedom of expression and information online. Long-term engagement with the public and other bodies, such as CSOs working on internet or digital rights, as well as with the MCMC, is crucial to strengthening rights in all spaces, both online and offline.

b. Recognise technology-related gender-based violence as a threat to internet freedoms.

Gender-based violence must be considered in the context of the interrelatedness of rights and addressing it must be seen as integral to the achievement of civil and political rights for all, instead of seeing gender-based violence as a "women's issue" or secondary in importance.

APPENDIX 1: APC-LA RUE FRAMEWORK

APC-LA RUE FRAMEWORK FOR ASSESSING FREEDOM OF EXPRESSION AND RELATED RIGHTS ON THE INTERNET

APC developed the APC-La Rue Framework based on the work of and recommendations by former UN Special Rapporteur on Freedom of Expression Frank La Rue[1] and on the UN Human Rights Committee's General Comment 34[2] on Article 19 of the International Covenant on Civil and Political Rights. The framework consists of a checklist of indicators that are intended to provide guidance in monitoring and reporting on internet-related human rights violations, specifically those related to freedom of expression. Further work is needed, and is underway, to develop more comprehensive guidance for reporting on a wider range of internet-related human rights including women's rights, sexual rights and economic, social and cultural rights, as steps towards turning the framework into a monitoring tool for human rights online.

1. General protection of freedom of expression

- National constitution or laws protect internet-based freedom of expression.
- State participates in multistakeholder initiatives to protect human rights online.

2. Restrictions on online content

2.1 Arbitrary blocking or filtering

- There are no generic bans on content.
- Sites are not prohibited solely because of political or government criticism.
- State blocks or filters websites based on lawful criteria.
- State provides lists of blocked and filtered websites.
- Blocked or filtered websites have explanation on why they are blocked or filtered.
- Content blocking occurs only when ordered by competent judicial authority or independent body.
- Where blocked or filtered content is child pornography, blocking or filtering online content is connected with offline national law enforcement strategies focused on those responsible for production and distribution of content.

2.2 Criminalising legitimate expression

- Defamation is not a criminal offence.
- Journalists and bloggers are protected against abuse or intimidation.

1. Available here: www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf
2. Available here: www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

CONNECT YOUR RIGHTS! INTERNET RIGHTS ARE HUMAN RIGHTS

APC-LA RUE FRAMEWORK

- Journalists and bloggers are not regularly prosecuted, jailed or fined for libel.
- Journalists, bloggers and internet users do not engage in self-censorship.
- National security or counter-terrorism laws restrict expression only where:
  (a) the expression is intended to incite imminent violence;
  (b) it is likely to incite such violence; and
  (c) there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

2.3 Imposition of internet intermediary liability

- State does not delegate censorship to private entities.
- Internet intermediaries are not liable for refusing to take action that infringes on human rights.
- State requests to internet intermediaries to prevent access to content, or to disclose private information, are:
  (a) strictly limited to purposes such as the administration of criminal justice; and
  (b) by order of a court or independent body.
- There are effective remedies for individuals affected by private corporations' actions, including the possibility of appeal through the procedures provided by the intermediary and competent judicial authority.
- State discloses details of content removal requests and accessibility of websites.

2.4 Disconnecting users from the internet

- Internet access is maintained at all times, including during political unrest.
- Disconnecting users is not used as a penalty, including under intellectual property law.

2.5 Cyber attacks

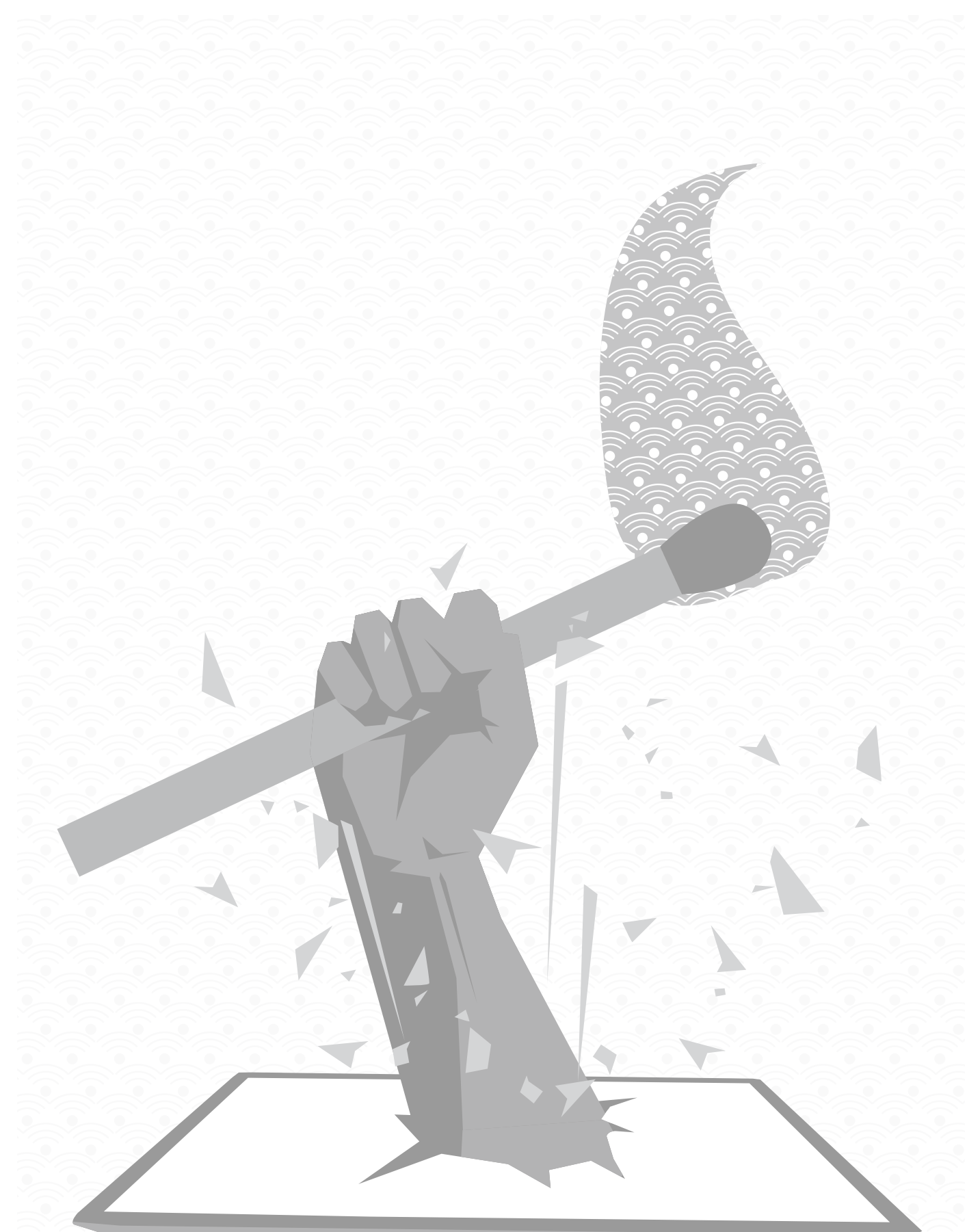
- State does not carry out cyber attacks.
- State takes appropriate and effective measures to investigate actions by third parties, holds responsible persons to account, and adopts measures to prevent recurrence.

2.6 Protection of the right to privacy and data protection

- There are adequate data and privacy protection laws and these apply to the internet.
- The right to anonymity is protected.
- State does not regularly track the online activities of human rights defenders, activists, and opposition members.
- Encryption technologies are legally permitted.
- State does not adopt real name registration policies.
- Limitations on privacy rights are exceptional (such as for administration of justice or crime prevention) and there are safeguards to prevent abuse.

3. Access

- State has a national plan of action for internet access.
- State fosters independence of new media.
- Concrete and effective policy is developed with public and private sector to make the internet available, accessible and affordable to all.
- Development programmes and assistance policies facilitate universal internet access.
- State supports production of local multicultural and multilingual content.
- State supports initiatives for meaningful access by marginalised groups.
- Digital literacy programmes exist, and are easily accessible, including primary school education and training to use the internet safely and securely.



supported by the
European Union