White Paper on Reforms for the Prevention of Electronic Crimes Act (PECA) 2016

Prepared by **Media Matters for Democracy**

This policy paper was written for the Civil society for Independent Media and Expression (CIME) initiative, jointly undertaken by the Centre for Peace and Development Initiatives, Media Matters for Democracy, and the Pakistan Press Foundation.

The CIME project aims to contribute to enhanced protection and promotion of freedom of expression and right to information for citizens in Pakistan. In connection with these fundamental rights, the project will increase the availability of knowledge about policy trends, raise awareness about policy gaps and practical challenges that limit the effective use of the rights, build capacity of civil society stakeholders to be responsive to risks and violations, and develop support networks for stakeholders that require assistance.

Published in September 2020

Table of Contents

Executive Summary

The Prevention of Electronic Crimes Act (PECA) 2016 is a contentious legislation that provides the primary mechanism for online content regulation and the investigation and prosecution of cyber offences in Pakistan. It sits at the heart of the country's Internet governance policy framework. The legal provisions of PECA and its flawed implementation pose serious risks to the fundamental freedoms of Pakistani citizens and their online activity. This white paper relies on an extensive review of literature to articulate the need for reforms in the law. The paper examines the available literature on the legal issues and implementation status of the law to analyse key concerns and presents a discussion on the current policy context and possible policy options regarding Internet governance. The following are its main findings:

1. PECA adversely affects the freedom of online expression, the right of access to information, and the right to privacy of Pakistani Internet users.
2. The law criminalises online speech and has been used arbitrarily to stifle dissent and target the expression of political activists, journalists, human rights defenders, and social media users.
3. PECA grants broad powers to the telecom regulator – the Pakistan Telecommunication Authority – to interpret and decide upon restrictions on expression. These restrictions are not clearly and precisely defined in the Act. The ambiguity in the scope of this legal provision leaves room for uneven and arbitrary application of the law. The PTA uses its decisions to block access to online information without transparency or justification.
4. Moreover, the legal provisions about expedited acquisition of data and real-time information collection in PECA pose significant risks to the privacy of Pakistani users in the absence of a data protection regime.
5. The law's implementation is marred by the capacity constraints of the designated investigative agency and the judiciary. These constraints include lack of human resources and limited technical capability.
6. Based on the analysis and policy context, the paper recommends
    a. A comprehensive review of PECA's legal and implementation challenges;
    b. A process to introduce an amendments bill to reform the law;
    c. The decriminalisation of online speech and defamation;
    d. The separation of the content regulation provision from cybercrimes;
    e. Increased investigative and judicial capacity; and
    f. An open, fair, and transparent multi-stakeholder consultative process to draft the rules of business for online content regulation.
7. The paper also shares some potential legal amendments to bring them to the notice of the policymakers and other relevant stakeholders.
8. The analysis and recommendations presented in the paper may be used as the basis of

a sustained advocacy and outreach campaign to reform PECA. The findings of the paper could also be used to gain multi-stakeholder feedback to refine the vision for Internet governance in Pakistan.

1. Introduction

Background

1.1. The deliberations on new cybercrime legislation began in 2014[1] during the federal government of the Pakistan Muslim League-Nawaz.[2] In February 2015, the federal cabinet approved a draft bill to be introduced in the Parliament.[3] Over the next 18 months, the draft bill was modified a few times, as it made the rounds of parliamentary committees, generated debates in the media, and drew critical responses from civil society.

1.2. The bill was approved by the National Assembly in April 2016.[4] The Senate unanimously passed the bill in July 2016 with 50 amendments to the original draft.[5] The amendments were sent back for debate to the National Assembly, which passed the bill in August.[6] The same month the President assented to the Prevention of Electronic Crimes Act (PECA) 2016, bringing the anti-cybercrime legislation into effect.[7]

1.3. The rationale for the legislation, as presented by the then-Minister of State for Information Technology, was that existing laws were inadequate to deal with new, unprecedented, and unique types of cybercrime, such as hacking, cyber terrorism, and identity theft, among other offences.[8] It was claimed that PECA would protect citizens from cyber threats, prevent cybercrimes, contribute to national security, and enable a secure environment for the Information Technology industry. These claims were fiercely contested by civil society representatives who highlighted the human rights concerns about the bill during the rushed legislative process.[9]

1.4. PECA gave the federal government the power to establish or designate a law enforcement agency for the purposes of investigating cyber offences defined under the law.[10] The agency is required to develop its own capacity for forensic analysis, but the government could help it out by making rules for the specialised training of staff. In September 2016, the Federal Investigation Agency (FIA) was designated as the investigating force for cybercrimes.[11] Under

1 Ahmadani, A. (2014). Ministry okays act to curb cyber crime. The Nation. Available at https://nation.com.pk/16-Jan-2014/ministry-okays-act-to-curb-cyber-crime

2 Bolo Bhi. (2014). Industry version of the Prevention of Electronic Crimes Bill 2014. Available at http://bolobhi.org/wp-content/uploads/2015/02/E-Crime-Bill-Final-version.pdf

3 Baloch, F. (2015). Rights activists seek changes in draft cybercrime bill. The Express Tribune. Available at https://tribune.com.pk/story/836841/rights-activists-seek-changes-in-draft-cybercrime-bill

4 Khan, R. (2016). Controversial Cyber Crime Bill approved by NA. Dawn. Available at https://www.dawn.com/news/1251853

5 Geo News. (2016). Senate passes cyber crimes bill with amendments. Available at h https://www.geo.tv/latest/110372-Senate-passes-cyber-crimes-bill-with-amendments

6 Khan, R. (2016). Cyber crime bill passed by NA: 13 reasons Pakistanis should be worried. Dawn. Available at https://www.dawn.com/news/1276662

7 The Gazette of Pakistan. (2016). Prevention of Electronic Crimes Act, 2016. Available at http://na.gov.pk/uploads/documents/1472635250_246.pdf

8 PECA 2016, as passed by the National Assembly. Available at http://na.gov.pk/uploads/documents/1462252100_756.pdf

9 See Section 2 and Section 3 of this paper for further discussion on the concerns raised by the civil society.

10 For a detailed description of the sections of the law, please see Annex A.

11 The Express Tribune. (2016). Panel wants Federal Investigation Agency to probe cybercrimes. Available at https://tribune.com.pk/story/1178998/panel-wants-federal-investigation-agency-probe-cybercrimes

the law, the FIA is required to submit a half yearly performance report to Parliament.

1.5. The telecommunication regulator – the Pakistan Telecommunication Authority (PTA) – was designated as the enforcement agency in the Act. According to PECA Section 37, the PTA has been granted the power to "remove or block or issue directions for removal or blocking of access to an 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 incitement to an offence". According to PECA Section 37(2), the PTA is empowered to prescribe rules, with the approval of the government, which could provide for safeguards, transparent process, and an effective oversight mechanism for the content removal and blocking provision.

1.6. Section 51 of PECA grants the federal government the power to make rules for carrying out the purposes of the law. The rules could specify training and qualifications of investigating officers, investigation procedures, procedure for seeking orders from PTA for content removal, inter-agency coordination, and functions of a forensic laboratory and its staff, among other things.

1.7. Almost two years after the passage of the law, the federal government approved the crimes investigation rules under PECA.[12] These rules specify the principles and procedures the FIA should follow to register complaints, conduct investigations, and perform digital forensic analyses, among other duties.

1.8. In February 2020, news reports emerged that the federal cabinet had approved rules for online content regulation under Section 37 of PECA.[13] These rules of business, titled the Citizen Protection (Against Online Harm) Rules 2020, were supposed to deal with the blocking or removal of online content. However, the rules were suspended on a directive by the Prime Minister the same month[14], after they received widespread criticism and resistance from local civil society organisations, the media, lawyers, and international Internet companies.[15]

1.9. Besides suspending the rules, the government formed a committee to hold consultations about the Citizen Protection rules with multiple stakeholders. The committee held its first meetings at the beginning of March 2020.[16] Its activities were disrupted by the coronavirus pandemic and associated lockdown. However, the committee resumed its work in May and sent invitations for consultation to local and international stakeholders.[17] It also published an

12 FIA. (2018). Prevention of Electronic Crimes Investigation Rules 2018. Available at http://www.fia.gov.pk/en/law/PECARULES.pdf

13 DRM. (2020). Social media companies instructed to establish local presence. Digital Rights Monitor. Available at https://digitalrightsmonitor.pk/social-media-companies-instructed-to-establish-local-presence-provide-government-with-unencrypted-user-data-and-block-access-to-reported-content-within-24-hours/

14 Jahangir, R. (2020). Implementation of online rules suspended, says PTA. Dawn. Available at https://www.dawn.com/news/1537931

15 Naeem, W. (2020). Social media rules: Civil society slams consultative committee, demands PECA reforms. Digital Rights Monitor. Available at https://digitalrightsmonitor.pk/social-media-rules-civil-society-slams-consultative-committee/

16 Ahmed, A. (2020). Pakistan social media rules: Despite criticism, govt holds first consultation meeting. Business Recorder. Available at https://www.brecorder.com/2020/03/03/576634/pakistan-social-media-rules-despite-criticism-govt-holds-first-consultation-meeting/

17 Jahangir, R. (2020). Govt begins consultation on online harm rules. Dawn. Available at https://www.dawn.com/news/1560952

online survey form to get feedback on the rules.[18]

1.10. The local civil society, including representative bodies of journalists and digital rights organisations, has largely boycotted the consultative process. They have demanded the rules must first be withdrawn before a transparent and meaningful dialogue can begin. The civil society representatives have also demanded clarity from the government about its policy vision and objectives for dealing with online harms.

Objectives of the White Paper

1.11. Since the early 2000s, the use of the Internet and social media has increased phenomenally in Pakistan. The number of Internet subscriptions grew by around 320 percent between 2014 and 2019, to cross the 70-million mark.[19] Over 35 million Pakistanis use social media platforms, such as Facebook, Twitter, and YouTube.[20] The advent of 3G and 4G cellular technology has also made the Internet more accessible for many Pakistani citizens.

1.12. The rise in online usage provided a dramatic increase in opportunities for citizens to share their political expression and exercise their right to association and assembly online. The use of social media by political parties and leaders has also raised the significance of the online space for discourse regarding electoral politics and governance since 2013.

1.13. Alongside these developments, the global rise in disinformation and coordinated campaigns to manipulate online conversations especially in the context of elections has led to a push by governments around the world to regulate the Internet. Pakistan is also affected by these developments.

1.14. In Pakistan, the online space is primarily regulated by PECA 2016, and the opportunities for citizens to freely and independently exercise their digital rights, including freedom of expression, access to information, and privacy, are all linked to the implementation and enforcement of this anti-cybercrimes law. Issues and challenges regarding PECA, therefore, pose direct threats and risks to the online rights of Pakistani users.

1.15. In this context, this paper attempts to compile the legal problems and implementation challenges connected with PECA based on a review of past literature. In doing so, the paper will articulate the need for reforms in PECA.

1.16. The paper also describes the current and developing policy context in which the government views online content regulation, and it discusses the likelihood of potential policy scenarios in the prevailing situation.

1.17. Finally, based on the analysis and policy context, the paper presents policy recommendations for reforms in PECA and the rules made thereunder, and shares suggestions for future action.

18 Kamran, H. (2020). PTA shares survey for stakeholder consultation on Online Harm Rules 2020. Digital Rights Monitor. Available at https://digitalrightsmonitor.pk/pta-shares-survey-for-stakeholder-consultation-on-online-harm-rules-2020/

19 PTA. (2020). Telecom indicators. Available at https://www.pta.gov.pk/en/telecom-indicators/1#broadband-subscribers

20 Farooq, M. (2019). Active social media users in Pakistan grow by 5.7%: Report. Profit. Available at https://profit.pakistantoday.com.pk/2019/02/05/active-social-media-users-in-pakistan-grow-by-5-7-report/

2. Problem Identification and Analysis

2.1. An extensive review of literature, including research studies, policy briefs, and news reports, was conducted to produce the following discussion of the concerns associated with PECA.

The Problems

2.2. From its earliest draft to the law's implementation, human rights defenders have consistently criticised PECA for its potential and demonstrated adverse effects on the online expression, the right of access to information, and the privacy of Pakistani Internet users.

2.3. Different sections in the PECA criminalise online speech without providing concrete definitions and initiating adequate protections for the right of freedom of expression of citizens. The law has been used since 2016 to arbitrarily target political dissenters, journalists, and human rights defenders.

2.4. The law gives broad powers to the enforcement authority, PTA, which is allowed to control and regulate online content through means of blocking and removal without any form of transparency.

2.5. PECA does not adequately address the problem of lack of jurisdiction over global Internet companies when it comes to content regulation.

2.6. PECA allows for the misuse of investigating authority by permitting law enforcement officers to use written notices for data disclosure, without bringing the matter to the attention of a court of law before the acquisition of private data.

2.7. Without a data protection and privacy law, the retention of traffic data poses concerns for the privacy of citizens as the data could be misused, for example for surveillance or targeting of individuals.

2.8. Despite the court warrant stipulation, the real-time data collection allowed under PECA is problematic as this legal provision can be used to set up an invasive surveillance technology solution that could be used to selectively or broadly monitor citizens. The section is also in contradiction of the real-time surveillance procedure defined in the Fair Trial Act.[21]

2.9. The designated investigating agency, the FIA, lacks the capacity and resources to sufficiently investigate complaints.

2.10. The judicial system lacks the capacity to handle cybercrime cases.

Online Freedom of Expression and Defamation

2.11. PECA criminalises online speech without providing adequate safeguards. It does not exempt news, political expression, and satire from its punishable offences.[22] It does not consider if the opinions or information shared online have a public-interest dimension. For

21 The Gazette of Pakistan. (2013). Investigation for Fair Trial Act, 2013. Available at http://www.na.gov.pk/uploads/documents/1361943916_947.pdf

22 Bolo Bhi. (2016). Major contentions: PECA. Available at http://bolobhi.org/wp-content/uploads/2016/10/Major-contentions-PECA-2016.pdf

example, investigative journalists who publish online the record of corruption at government departments supplied to them by whistleblowers might face cybercrime charges of unauthorised access to data, even though they have exposed the wrongdoing for public good.

2.12. PECA allows the telecommunication regulator PTA to interpret the restrictions on free speech imposed by Article 19 of the Constitution of Pakistan for the removal and blocking of online content, including opinions expressed by users. The interpretation of free speech restrictions is a legislative or judicial matter, but in PECA it is left to broad and arbitrary executive discretion because the restrictions are not precisely defined in the legislation. The law also ignores Pakistan's commitment to international human rights law and treaties, including the International Covenant on Civil and Political Rights, and advice provided in the Human Rights Council's General Comment 34 that specifies the restrictions on freedom of expression must be legal, necessary, and proportionate to achieve a legitimate objective[23].

2.13. PECA also does not take into account the existing laws and penal code provisions in Pakistan for defamation. Instead, by criminalising online defamation in its Section 20, it duplicates the provisions in other laws and only serves to add to the body of criminal laws against defamation in the country.[24] It also encumbers judicial oversight for the fate of allegedly defamatory content. Section 20 allows aggrieved persons to apply directly to the PTA for removal, destruction or blocking of access to allegedly defamatory content. The PTA is designated to pass orders as it deems reasonable about the removal or blocking of such information, circumventing the judicial process typically followed for defamation cases.

2.14. Reports suggest that PECA sections pertaining to offences against the dignity and modesty of natural persons have been used to charge suspects in inquiries related to complaints filed by women with the FIA about online harassment or reputational harm.[25]

2.15. However, Section 20 ("offence against the dignity of a natural person") has has also been used to charge political activists[26], social media users, and journalists[27] by the authorities with the accusation that their online expression was against state interests[28] or institutions[29].

2.16. Even though Section 20 is a non-cognisable offence, it has also been noted that cognisable sections of PECA and the penal code are added to the FIRs (First Information Reports) where

23 United Nations Office of the High Commissioner for Human Rights. (2011). General Comment 34 CCPR/C/GC/34. Available at https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

24 Global Information Society Watch. (2017). Unshackling expression: A study on laws criminalising expression online in Asia. Association for Progressive Communications. Pg 112.

25 Imran, W. (2018). Of consent and copyrights: Women lodge 90% complaints in FIA Cybercrime Circle. The Express Tribune. Available at https://tribune.com.pk/story/1681027/1-consent-copyrights-women-lodge-90-complaints-fia-cybercrime-circle

26 Zarrar, S. (2017). PTI worker arrested over anti-army posts on social media. Pro Pakistani. Available at https://propakistani.pk/2017/05/31/pti-worker-arrested-anti-army-posts-social-media/

27 Shahid, S. (2017). FIA arrests reporter in Quetta over social media comments. Dawn. Available at https://www.dawn.com/news/1342268

28 Hashim, A. (2017). Social media crackdown stifles dissent in Pakistan. Al Jazeera. Available at https://www.aljazeera.com/news/2017/11/social-media-crackdown-stifles-dissent-pakistan-171124083629362.html

29 Gishkori, Z. (2017). Crackdown on social media activists ordered. The News International. Available at https://www.thenews.com.pk/print/205887-Crackdown-on-social-media-activists-ordered

the primary charge is under Section 20 in order to make arrests without warrants.[30]

2.17. The section on cyber terrorism has also been used to intimidate journalists, most notably in the 2019 case against journalist Shahzeb Jillani. The authorities claimed that Jillani's comments about the military in connection with enforced disappearances created a sense of fear, panic or insecurity in the Government or the public, as per Section 10 of PECA.[31] Ironically, Jillani's remarks were originally made during a television talk show he reported for and were only later published on social media. The case against him was later disposed of.[32]

2.18. The section related to glorification of an offence is similarly problematic, as any discussion about convicted terrorists or proscribed organisations, including original news reporting on militancy, can be misconstrued as glorification and used to censor speech or silence the speaker through legal action. The term 'glorification' lacks legal clarity in connection with incitement to terrorism and fails to justify a necessary and legitimate restriction on expression.[33]

Online Content Regulation

2.19. Section 37 of PECA gives PTA broad powers to remove or block access to online information. As mentioned earlier, the PTA is allowed to interpret the restrictions on the freedom of speech by itself or with the help of government directions. The legal interpretation for content removal, therefore, is transformed from a judicial function to an executive duty, with little or no legislative guidance or judicial oversight. PTA should be an independent regulator, but it is practically not independent. The federal government appoints its chairperson and can, by law, issue binding policy directives to the PTA.[34] This raises the concern that governments could potentially force the PTA to use the content blocking clause to censor political dissent. The PTA has, in the past, blocked a website that published satire[35] and a website of a political party[36].

2.20. Moreover, since 2016, PTA has failed to share publicly the process by which it blocks content. On being pressed by legislators, the PTA has shared that it had blocked over 900,000 websites up until mid-2019 for blasphemous, pornographic or anti-state content among other reasons.[37] However, it has neither made a list of these websites publicly available nor shared the details of the decision-making process it followed for each of these websites.[38]

30 Bolo Bhi. (2019). Note on the implementation of Prevention of Electronic Crimes Act 2016. Available at http://bolobhi.org/note-on-the-implementation-of-prevention-of-electronic-crimes-act-2016/

31 Hashim, A. (2019). Pakistan extends bail for journalist accused of 'cyberterrorism'. Al Jazeera. Available at https://www.aljazeera.com/news/2019/04/pakistan-extends-bail-journalist-accused-cyber-terrorism-190417074414124.html

32 Samaa. (2019). Karachi court disposes of case against journalist Shahzeb Jillani. Available at https://www.samaa.tv/news/2019/05/karachi-court-disposes-of-case-against-journalist-shahzeb-jillani/

33 UN A/66/290. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Available at https://www.ohchr.org/Documents/Issues/Opinion/A.66.290.pdf

34 Pakistan Telecommunication (Re-organization) Act, 1996. Available at https://www.pta.gov.pk/assets/media/telecom-act-170510.pdf

35 Masood, T. (2017). Satire website Khabaristan Times blocked in Pakistan. Dawn. Available at https://www.dawn.com/news/1311841

36 Niazi, A. (2019). AWP takes PTA to court for blocking website. Pakistan Today. Available at https://www.pakistantoday.com.pk/2019/02/16/awp-takes-pta-to-court-over-censorship-of-website/

37 Ali, K. (2019). 900,000 websites blocked over content, says PTA. Dawn. Available at https://www.dawn.com/news/1507590

38 Jahangir, R. (2019). PTA's content removal conundrum. Dawn. Available at https://www.dawn.com/news/1496491

2.21. The Web Analysis Directorate[39] of PTA has carried out its content blocking functions for over three years without any prescribed rules. By not sharing its decision-making process and rationale for each decision it made, it has also failed to demonstrate that it weighed the public interest in its content regulation decisions. It has, therefore, also undermined the Right of Access to Information of public importance granted to Pakistani citizens in Article 19-A of the Constitution[40].

2.22. The content blocking measures are also criticised for being selective – a practice that predates that passage of PECA.[41] PTA is also known to have erroneously blocked websites in the past.[42] Even though PTA has blocked nearly a million websites, a news investigation found that dozens of Facebook groups belonging to 41 banned sectarian and terrorist organisations were still accessible in Pakistan a year after the enforcement of PECA.[43]

2.23. This investigation also revealed PTA's jurisdictional issues over social media networks, which are run by Internet companies based outside Pakistan. While PTA can quickly but opaquely block websites, it has to refer content takedown requests regarding social media posts to the respective Internet companies, which may decide upon the requests according to their own community standards or terms of service.

2.24. Some networks, such as Facebook and Twitter, now also take into account applicable local laws and accept legal requests. However, the final decision often rests with these platforms. For example, from July to December 2019, the Pakistan government sent 219 legal requests to Twitter, but the micro-blogging website complied with only around one-third of these requests.[44] This was also the first time the social media company had ever complied with any of Pakistan's requests.

2.25. The volume of content takedown requests sent to Internet companies by the Government of Pakistan has also increased over the past few years. In 2019, Pakistan was among the countries where Facebook restricted the most number of content items, such as posts, pages, and groups.[45] The social network restricted access to around 2,300 items in Pakistan between July and December 2019 in response to government requests. It also complied with 52 percent of Pakistan's requests to seek account and user information for investigations, during the same period. This shows that PTA is keeping an eye on social media activity for illegal content.

2.26. In February 2019, FIA officials also confirmed that they were monitoring social media for extremist content, hate speech, and fake news, and will take legal action against it without any

39 PTA. (N.D.). Cyber Vigilance. Available at https://www.pta.gov.pk/en/ip-web-analysis

40 Pakistan Constitution Law. (N.D.). Article: 19A Right to Information. Available at https://pakistanconstitutionlaw.com/article-19a-right-to-information/

41 Baloch, H. (2017). Internet censorship in Pakistan. Findings from 2014-2017. Bytes for All. Available at https://bytesforall.pk/sites/default/files/internet-censorship-in-pakistan.pdf

42 Kamran, H. (2020). PTA responds to RTI requests; unblocks Slate and Gizmodo websites. Digital Rights Monitor. Available at http://digitalrightsmonitor.pk/pta-responds-to-rti-requests-unblocks-slate-and-gizmodo-websites/

43 Haque, J. & Bashir, O. (2017). Banned outfits in Pakistan operate openly on Facebook. Dawn. Available at https://www.dawn.com/news/1335561

44 Transparency Report. (N.D.). Pakistan. Twitter. Available at https://transparency.twitter.com/en/countries/pk.html

45 Jahangir, R. (2020). Pakistan among countries with most content removal requests: Facebook. Dawn. Available at https://www.dawn.com/news/1556715

complaint from aggrieved persons.[46]

2.27. At least 20 instances of summons, inquiries, cases, detentions, and arrests based on social media posts took place between 2017 and 2019, according to one research study.[47] Most of these incidents involved activists and journalists. Other government departments were also reportedly monitoring social media for illegal content.[48]

2.28. The PTA reportedly also does not notify website owners when it blocks their websites, even though parties aggrieved by content decisions are allowed by the law to send a review application to PTA. When the Awami Workers Party's website was blocked in June 2018, it filed a complaint with the PTA and the Election Commission of Pakistan. The website was subsequently restored without any direct response from the PTA.[49] Later the political party filed a writ petition in the Islamabad High Court, which ruled in September 2019 that the PTA cannot block websites without due process as mandated in the Right to Fair Trial in Article 10-A of the Constitution of Pakistan.[50] The court also ordered PTA to prescribe rules for removal of unlawful online content within 90 days, which the authority had not done until then.

2.29. The first attempt to formulate the rules for content regulation under PECA was done in early 2020 and was immediately mired in controversy when it was noticed that the government had focussed on the localisation of social media companies and apparently overstepped and contravened PECA boundaries by calling for the designation of a new special coordinator to supervise the content takedown process.[51] The rules were suspended in February.[52]

Privacy

2.30. PECA sections regarding traffic data retention, expedited acquisition of data, the real-time collection of information, and international cooperation lead to risks to the data privacy of users.

2.31. While Section 41 of the law provides for the confidentiality of information secured by a law enforcement officer during investigation, the expedited acquisition of data without a court warrant can be misused by the investigating agency to seize data or harass or intimidate the

46 Ayub, I. (2019). FIA watching social media to curb 'anti-national propaganda, hate speech'. Dawn. Available at https://www.dawn.com/news/1465816

47 Bolo Bhi. (2019). Summons, enquiries, FIRs, detentions and arrests in connection with social media posts. Available at http://bolobhi.org/timeline-summons-enquiries-firs-detentions-and-arrests-in-connection-with-social-media-posts-2/

48 The News International. (2017). 684 social media IDs objectionable. Available at https://www.thenews.com.pk/print/214986-684-social-media-IDs-objectionable

49 Raza, T. (2018). Update: Awami Workers Party website blocked by multiple ISPs in Pakistan. Digital Rights Monitor. Available at https://digitalrightsmonitor.pk/generalelections2018-amidst-shrinking-online-spaces-website-of-awami-workers-party-blocked-in-pakistan/

50 Ghani, A. (2019). IHC directs PTA to provide opportunity of hearing before blocking online content. Digital Rights Monitor. Available at http://digitalrightsmonitor.pk/ihc-directs-pta-to-provide-opportunity-of-hearing-before-blocking-online-content/

51 Chabba, S. (2020). Pakistan's new internet laws tighten control over social media. DW. Available at https://www.dw.com/en/pakistans-new-internet-laws-tighten-control-over-social-media/a-52375508

52 Jahangir, R. (2020). Implementation of online rules suspended, says PTA. Dawn. Available at https://www.dawn.com/news/1537931

owners of information systems. Internal investigations against law enforcement officers are often marred by institutional solidarity, and authorised officers can get away with punishments for breach of confidentiality if they can prove that they were acting in good faith. A post-fact warrant requirement may not be an effective safeguard against abuse or misuse of expedited data acquisition.[53]

2.32. Pakistan does not have a data protection or privacy law. Legislation is in the works but as of May 2020, consultation on a new draft of the bill had just concluded.[54] In the absence of a strict data protection and data privacy regime, the one-year data retention of traffic data by service providers is fraught with risks for misuse of personal data. The traffic data may contain metadata that reveal patterns about a user's behaviour. In the absence of a data protection law if the data is breached through a hacking attempt on the information system or a leak, the service provider may state that it did not intend to cause harm to the users whose information was disclosed and get away without being penalised for lax data security under PECA.

2.33. The real-time collection and recording of information can only be carried out after obtaining a court warrant by providing substantive reasons or grounds. However, the capability of real-time data collection paves the way for local law enforcement agencies to install and use invasive surveillance technology that may be used for broad or narrow monitoring of citizens, including journalists and human rights defenders. PECA does not share any provisions about transparency in deployment and scope of such systems.

2.34. The international cooperation section of PECA appears to be derived from the vision for joint anti- and counter-terrorism activities. While a set of conditions are listed in the law for refusing the foreign requests, there is no provision of public transparency for the register of requests or the decision-making process for granting requests. This raises concerns about the sharing of the data of Pakistani users with foreign governments, especially with countries that may have a dubious record regarding digital surveillance of citizens or foreign nationals.

Investigative and Judicial Capacity

2.35. The federal government approved the investigation rules for PECA in July 2018, almost two years after it had designated FIA as the investigative agency for cybercrimes. In the interim, the FIA's Cybercrime Wing – known as the National Response Centre for Cyber Crime (NR3C)[55] – had started to accept complaints for PECA offences, conduct investigations, and file charges against accused persons.

2.36. However, FIA's human resource and technical capacity were limited from the start and remain insufficient at present. By August 2018, the NR3C had only 10 investigators for cyber

53 Bolo Bhi. (2016). Major contentions: PECA. Available at http://bolobhi.org/wp-content/uploads/2016/10/Major-contentions-PECA-2016.pdf

54 Panakal, D. D. (2020). Pakistan's data protection bill includes localization and registration provisions. The National Law Review. Available at https://www.natlawreview.com/article/pakistan-s-data-protection-bill-includes-localization-and-registration-provisions

55 National Response Centre for Cyber Crime http://www.nr3c.gov.pk/

crimes to process the thousands of complaints received by the agency.[56] In August 2019, an FIA official told a parliamentary committee that the NR3C had probed only less than a quarter of the 42,477 complaints it had received since the passage of the law and that the FIA needed to hire staff on around 400 more positions for the cybercrimes wing.[57]

2.37. By February 2020, the FIA had 15 anti-cybercrime centres. However, the 15 centres cover the entire country, and each centre has to deal with the complaints from several districts.[58] For example, the FIA cybercrime centre in Lahore has to investigate the complaints registered across the Lahore and Sahiwal divisions, which include altogether seven districts with a cumulative population of around 27 million residents.[59] In some cases, it is expected that complainants would have to visit the nearest FIA centre to lodge or follow-up on a complaint but the nearest centre could be in another city or in another district. The inaccessibility of FIA centres may be a deterrent to the reporting of cybercrimes. Similarly, the vast jurisdictions of the centres would also add to the transport costs and time of investigators.

2.38. Lawyers and civil society representatives have highlighted that FIA cybercrime officers need more technical and sensitivity training to deal with a variety of cybercrimes, including cases of online harassment of women.[60] It was also noticed that delays in forensic test results due to overburdened laboratories caused delays in case proceedings. FIA cybercrime officials in Karachi have themselves identified the software and hardware equipment needed at their forensic facility.[61] Perhaps due to the lack of capacity or training, lawyers have also noted that FIA officers try to act as mediators between the complainants and the accused so as to settle the matters out of court.[62] This could have an intimidating effect on complainants, especially in cases related to online harassment.

2.39. Originally, the FIA NR3C had one forensic lab in Islamabad and another lab in Karachi.[63] FIA intended to set up new forensic labs at cybercrime centres in Lahore, Peshawar, and Quetta, but it is unclear if it was able to achieve the goal. However, the FIA officials in Lahore are known to use the services of the Punjab Forensic Science Agency.[64] Under Section 40 of PECA, the

56 Haq, R. (2018). FIA's cybercrime wing in 'dire straits'. The Express Tribune. Available at https://tribune.com.pk/story/1739675/1-fias-cybercrime-wing-dire-straits

57 DRM. (2019). FIA having difficulty obtaining data in cybercrime cases, NA body told. Digital Rights Monitor. Available at https://digitalrightsmonitor.pk/fia-having-difficulty-obtaining-data-in-cybercrime-cases-na-body-told/

58 Mohal, S. N. (2018). Govt declares jurisdictions of cybercrime reporting centres across country. Pakistan Today. Available at https://www.pakistantoday.com.pk/2018/10/02/govt-declares-jurisdictions-of-cybercrime-reporting-centres-across-country/

59 Pakistan Bureau of Statistics. 2017 Census. Available at http://www.pbs.gov.pk/content/block-wise-provisional-summary-results-6th-population-housing-census-2017-january-03-2018

60 Rana, S. (2018). Bottlenecks, incompetence and abuse of power: An analysis of PECA's implementation. Media Matters for Democracy. Available at http://digitalrightsmonitor.pk/wp-content/uploads/2018/11/Bottlenecks-Incompetence-and-Abuse-of-Power-An-analysis-of-PECA-implementation.pdf

61 Jawad, A. (2018). 65% of cybercrime cases in Karachi relate to Facebook. The Express Tribune. Available at https://tribune.com.pk/story/1690292/1-eradicating-cybercrime-karachi

62 Sheikh, F. (2019). Cases registered under PECA are facing delays, mismanagement: activists. The Express Tribune. Available at https://tribune.com.pk/story/2083368/cases-registered-peca-facing-delays-mismanagement-activists

63 Bolo Bhi. (2017). PECA 2016: Recommendations for Implementation and Oversight.

64 Abbtakk.tv. (2019). Forensic laboratory declares judge's disputed real. Available at https://abbtakk.tv/en/forensic-laboratory-declares-judges-disputed-video-real/

federal government was supposed to establish or designate a forensic laboratory "independent of the investigation agency", but it has so far failed to do so.[65] Instead, in the investigation rules of 2018, the government laid out procedures for the working and management of the Digital Forensic Laboratory of the FIA Cybercrime wing only.

2.40. The FIA was bound by PECA Section 53 to present biannual performance reports to the Parliament. It should have submitted seven reports up until March 2020. However, FIA only submitted one report to the Parliament in January 2018 that covered the activities for the year 2016-17.[66] It has not submitted another report since then. In the 2016-17 report, FIA stated that it had received around 8,000 complaints, which were converted into just under 1,100 inquiries. The inquiries resulted in the registration of around 150 cases and 132 arrests.

2.41. The FIA report also mentioned that the agency had submitted a proposal for setting up new forensic labs and upgradation of existing facilities as well as hiring of staff. The agency also requested the legislators that seven offences should be made cognisable to allow authorised officers to make arrests without court warrants.

2.42. News reports suggest that FIA received around 56,000 complaints in 2019.[67] It only investigated a fifth of these complaints, and managed to get convictions in 32 cases.[68]

2.43. Under Section 44 (1), the federal government, in consultation with the chief justice of respective high courts, was mandated to designate presiding officers to try offences under PECA. Until March 2017, no special courts were designated for cybercrime trials.[69] Later, the government and the judiciary jointly notified 27 additional session judges and magistrates in Sindh, four in Punjab, and two each in Islamabad, Khyber Pakhtunkhwa, and Balochistan to hear cybercrime cases.[70] In some jurisdictions, it took nearly six more months for the courts to fully start trial proceedings for the cybercrime cases.[71]

2.44. Further delays in the cybercrime trials were faced due to shortage or unavailability of state prosecutors. Trial hearings were usually adjourned if the prosecutor was absent in cybercrime cases that were cognisable and in which the State was a party.[72]

2.45. For cases dealing with online expression and activity, the FIA or police often includes charges from other legal sources, such as the penal code or the anti-terrorism act, in addition

65 Tahir, Z. (2018). Forensic lab, special court projects to tackle cyber crime hang fire. Dawn. Available at https://www.dawn.com/news/1390365

66 Raza, T. (2018). FIA submits 'half-yearly' report on electronic crimes after a one year delay. Digital Rights Monitor. Available at https://digitalrightsmonitor.pk/fia-submits-half-yearly-report-on-electronic-crimes-after-a-one-year-delay-asks-for-7-offences-to-be-declared-non-bailable-and-a-ban-on-bitcoin/

67 ARY. (2020). FIA received over 56,000 cybercrime complaints during 2019, NA body told. Available at https://arynews.tv/en/fia-cyber-crime-complaints/

68 The Express Tribune. (2020). FIA received 56,000 cyber-crimes complaints in 2019. Available at https://tribune.com.pk/story/2169706/fia-received-56000-cyber-crime-complaints-2019

69 See Footnote 60

70 Raza, T. (2017). PECA implementation: 27 designated courts for Sindh, 2 for Punjab. Digital Rights Monitor. Available at https://digitalrightsmonitor.pk/peca-implementation-27-designated-courts-for-sindh-2-for-punjab/

71 Aziz, F. (2018). Pakistan's cybercrime law: boon or bane? Heinrich Boll Stiftung. Available at https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane

72 *Ibid.*

to PECA in the FIRs. The multiplicity of charges creates confusion about the jurisdiction of courts regarding cybercrime cases, as the cases could be heard by trial courts that do not specifically deal with cybercrimes.[73]

2.46. Section 44 (2) of PECA called for the federal government and the judiciary to arrange special training of presiding officers on computer sciences, cyber forensics, electronic transactions, and data protection. However, there is little evidence to support[74] that consistent and comprehensive training opportunities are being provided for the session judges and magistrates notified to hear PECA cases.

2.47. Pakistan's judicial system is heavily burdened.[75] Since the courts designated for cybercrimes do not exclusively hear cases under PECA, they have to manage the cybercrime cases alongside their regular pending cases. Many of the PECA cases could drag on with adjournments and delays because of the additional burden.

Other Issues

2.48. Section 37 allows PTA to remove content that is against the glory of Islam, a restriction borrowed from Article 19 (freedom of speech) of the Pakistani constitution. Using this section, the PTA has blocked access to websites with blasphemous content. In May 2017, the PTA also started a public awareness campaign to warn citizens that uploading and sharing of blasphemous content is a punishable offence and that such content, if encountered, should be reported to the authorities.[76]

2.49. While PECA does not have a separate specific offence to punish users for blasphemous online expression, Pakistan's strict anti-blasphemy sections of the penal code have been used to sentence people[77] for allegedly committing blasphemy through their social media posts[78].

2.50. In 2017[79] and 2018[80], successive federal governments considered amending PECA to include capital punishment for blasphemous posts against the Prophet Muhammad (PBUH), in connection with a 2017 high court order for the government to crack down on online

73 See Footnote 60

74 See Footnote 70, and Sindh Judicial Academy. (2017). One month training program of newly promoted district and session judges Batch-64. Available at https://sja.gos.pk/wp-content/uploads/2017/09/Report-of-Batch-64-n.pdf

75 Gishkori, Z. (2019). 1.9 million backlog court cases, the highest in Pakistan. Geo News. Available at https://www.geo.tv/latest/225301-19-million-backlog-court-cases-the-highest-in-pakistan

76 Digital Rights Foundation. (2017). Year in Review: PECA. Available at https://digitalrightsfoundation.pk/year-in-review-peca/

77 Rasmussen, S. E. & Gillani, W. (2017). Pakistan: Man sentenced to death for blasphemy on Facebook. The Guardian.

Available at https://www.theguardian.com/world/2017/jun/11/pakistan-man-sentenced-to-death-for-blasphemy-on-facebook

78 BBC. (2019). Junaid Hafeez: Academic sentenced to death for blasphemy in Pakistan. Available at https://www.bbc.com/news/world-asia-50878432

79 Khan, S. (2017). Cabinet approves amendment bringing blasphemy, pornography under ambit of cybercrime law. Dawn. Available at https://www.dawn.com/news/1378966/cabinet-approves-amendment-bringing-blasphemy-pornography-under-ambit-of-cybercrime-law

80 DRM. (2018). New PECA amendment bill: Capital punishment for online blasphemy and false accusations of blasphemy proposed. Digital Rights Monitor. Available at http://digitalrightsmonitor.pk/new-peca-amendment-bill-capital-punishment-for-online-blasphemy-and-false-accusations-of-blasphemy-proposed/

blasphemous content[81]. Blasphemy allegations almost always carry a fatal risk for the accused in Pakistan and have led to lynching[82], assassination[83], and allegedly unfair trials leading to death sentences[84]. The country's anti-blasphemy laws have also been reportedly misused on occasion by accusers wishing to seek revenge for disputes or settle personal grudges[85].

2.51. The government eventually dropped its plan for PECA amendments, but such a move in the future may be detrimental to the online religious freedom of expression of Pakistani citizens, as the misuse of the law or mere allegation of online blasphemy could put the lives of Internet users at risk.

2.52. Despite the passage of the law, incidents of extrajudicial abduction and intimidation of social media users, including journalists[86] and bloggers[87], continued in the country, indicating that the law was not entirely able to provide a fair trial mechanism in practice for allegedly offensive online activity.

81 Pakistan Today. (2017). 'Would even summon PM for removal of blasphemous content on Internet'. Available at https://www.pakistantoday.com.pk/2017/11/17/would-even-summon-pm-for-removal-of-blasphemous-content-on-internet/amp/

82 Al Jazeera. (2019). Pakistan convicts two over Mashal Khan blasphemy lynching case. Available at https://www.aljazeera.com/news/2019/03/pakistan-convicts-mashal-khan-blasphemy-lynching-case-190321110355206.html

83 BBC. (2011). Punjab governor Salman Taseer assassinated in Islamabad. Available at https://www.bbc.com/news/world-south-asia-12111831

84 Hashim, A. (2019). Pakistani academic Junaid Hafeez sentenced to death for blasphemy. Al Jazeera. Available at https://www.aljazeera.com/news/2019/12/pakistani-academic-junaid-hafeez-sentenced-death-blasphemy-191221091139428.html

85 Rehman, I.A. (2017). Misuse of blasphemy law. Dawn. Available at https://www.dawn.com/news/1379203

86 BBC. Pakistan relief after abducted journalist Gul Bukhari is freed. Available at https://www.bbc.com/news/world-asia-44382719

87 Human Rights Watch. (2017). Pakistan: Bloggers feared abducted. Available at https://www.hrw.org/news/2017/01/10/pakistan-bloggers-feared-abducted

3. Policy Context

3.1. The 2014 Army Public School massacre by Tehreek-e Taliban Pakistan terrorists and the subsequent National Action Plan formulated by the government to fight against terrorism and extremism informed the early debates surrounding anti-cybercrimes legislation.[88] The action plan had also called for curbs on violent extremist content and hate speech online as a means to reduce the misuse of the Internet by militant groups for recruitment and negative radicalisation of Pakistani citizens.[89] Several PECA sections reflect the national security paradigm: offences related to glorification of terrorism, cyber terrorism, hate speech, and the recruitment, funding, and planning of terrorism, to name a few.

3.2. Despite concerns about the effects of cybercrime legislation on the fundamental freedoms of citizens, the government rushed the legislative process.[90] Concerted efforts by human rights organisations, digital groups, and trade unions of journalists led to some public scrutiny of the draft bill.[91] Instead of paying attention to protections for civil liberties, the government even tried to discredit the human rights concerns raised regarding the law by questioning the legitimacy and intention of the activists and organisations that raised these issues.[92]

3.3. The policy environment regarding Internet governance has changed considerably since the passage of PECA in 2016. Even though the risk of online harms to individuals persists, many new issues, such as the proliferation of disinformation, have also arisen. The Internet, and especially social media, is now undeniably significant for personal expression, socio-political life, and economic activity in Pakistan. With the coronavirus pandemic, the access to the Internet has become even more important for governance, public health, and education. The practical implementation of PECA during the past three years has also highlighted the risks to the digital rights and political participation of citizens. These factors have added to the discourse around Internet regulation in the country.

3.4. The current policy context for Internet governance in Pakistan is driven by tensions and agreements among executive vision, legislative sentiment, judicial attitudes, and public behaviour – each of these forces pulls and pushes at the others to focus the direction of online regulation.

3.5. The enforcement of PECA demonstrates that successive governments have been wary of the rise of political expression, commentary, and dissent on the Internet.[93] Crackdown on the online speech of political activists, journalists, and human rights defenders, among other

88 Aziz, F. (2018). Pakistan's cybercrime law: boon or bane? Heinrich Boll Stiftung. Available at https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane

89 National Action Plan, 2014. NACTA. Available at https://nacta.gov.pk/nap-2014/

90 Aziz, F. (2018). Pakistan's cybercrime law: boon or bane? Heinrich Boll Stiftung. Available at https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane

91 Zaidi, H. B. (2016). Cybercrime bill relegated to yet another committee. Dawn. Available at https://www.dawn.com/news/1266681

92 Media Matters for Democracy. (2016). Pakistan's new cybercrime bill passes through. Available at http://mediamatters.pk/in-spite-of-continued-objections-over-serious-human-rights-implications-pakistans-new-cyber-crime-bill-passes-through-joint-statement-by-media-matters-for-democracy-bytes-for-all-and-assoc/

93 The Express Tribune. (2017). No restrictions either: No unbridled freedom on social media, says Nisar. Available at https://tribune.com.pk/story/1417195/anti-army-content-social-media-will-not-tolerated-chaudhry-nisar

segments of the civil society, indicates that the executive is not comfortable with independent and critical online discussion if it raises questions about the country's governance issues or human rights record.

3.6. The Pakistan Tehreek-e Insaf government that came to power in 2018 has made several unsuccessful attempts to consolidate the regulation of digital media while at the same time using social media for sharing its political messaging[94], foreign policy campaigns[95], and vision for the digital economy[96]. It initially toyed with the idea of a converged media regulatory body that would also police the Internet alongside broadcast and print news media.[97] Its now-suspended content regulation rules focussed almost exclusively on social media, the foremost site of political discourse in the country. Like many governments around the world, the Pakistani government also realised the power of Internet companies over content decisions, and perhaps frustrated by the lack of total compliance from the platforms, proposed localisation of international Internet companies and further concentration of content regulation in a single, newly designated executive office. During its tenure, State regulators have also attempted to bring Over the Top TV, or OTT, content services into the folds of a licensing and regulatory regime[98], and also reportedly got telecom operators to collectively deploy a web monitoring system[99] that is apparently designed to prevent incoming international traffic from being illegally terminated, but may lead to pervasive surveillance of Internet traffic.

3.7. The meeting records of parliamentary committees, such as the information technology standing committees in the National Assembly and Senate, show that many legislators are also in favour of stringent content regulation in Pakistan.[100] The sentiments of legislators appear primarily driven by their self-interest: the abuse and trolling they face online due to their political affiliation has led them to lean towards a disciplinarian approach to tackle online content. Legislators have frequently expressed frustration with FIA and PTA for the unabated rumours, disinformation, and political memes that circulate online regarding their persons, their party leaders, and their political parties.[101] Ironically, an investigation by Media Matters for Democracy conducted in 2018 identified that various Twitter accounts demonstrating obvious political leanings for major political parties were involved in structured hate speech

94 Wasim, A. (2019). PM continue to attack opposition on Twitter. Dawn. Available at https://www.dawn.com/news/1458673

95 Dawn. (2020). Prime Minister tweets videos of Roger Waters assailing Indian law. Available at https://www.dawn.com/news/1537137

96 The Express Tribune. (2019). PM Imran launched 'Digital Pakistan' initiative. Available at https://tribune.com.pk/story/2112360/1-digital-pakistan-pm-imran-addresses-launch-ceremony

97 Butler, S. (2019). Proposed media regulator provokes strong criticism in Pakistan. Committee to Protect Journalists. Available at https://cpj.org/2019/04/proposed-media-regulator-pakistan-strong-criticism/

98 DRM. (2020). PEMRA's OTT & 'Web TV' policy 'unacceptable'. Digital Rights Monitor. Available at http://digitalrightsmonitor.pk/pemras-ott-web-tv-policy-unacceptable-leading-digital-media-outlets-media-digital-rights-activists-prominent-journalists/

99 Ali, U. & Jahangir, R. (2019). Pakistan moves to install nationwide 'web monitoring system'. Coda Story. Available at https://www.codastory.com/authoritarian-tech/surveillance/pakistan-nationwide-web-monitoring/

100 Ali, K. (2020). Senate panel recommends pact with Twitter to block fake accounts. Dawn. Available at https://www.dawn.com/news/1528568

101 The Express Tribune. (2020). Senate panel discusses social media campaign against Zardari. Available at https://tribune.com.pk/story/2240659/1-senate-panel-discusses-social-media-campaign-zardari

against each other and against journalists and activists.[102] It is also unfortunate that elected representatives have done little over the past three years to increase their understanding of Internet governance and digital rights, and still tend to favour a hard regulatory approach to solve whatever problems they perceive regarding online activity.

3.8. The higher judiciary has also expressed annoyance with anti-judiciary commentary on social media. The political dynamics in Pakistan are interwoven with judicial activity, and court decisions – such as the Supreme Court decision against former Prime Minister Nawaz Sharif in the Panama Paper case – have strong ramifications for domestic politics. Online political expression, therefore, often tends to address the role of the judiciary and individual judges. In February 2020, the Lahore High Court ordered PTA and FIA to submit detailed reports about actions taken against an anti-judiciary smear campaign on social media.[103] In April 2020, as the country struggled with Covid-19 management, the Prime Minister took notice of social media posts against the Supreme Court Chief Justice.[104] The posts had surfaced after the top judge critically reviewed the government's coronavirus response. Higher courts in the past have also directed the government to strictly deal with blasphemous and pornographic online content. Pakistani courts may have a tendency to look at digital rights from a conservative and moralistic lens, even though some superior and higher court orders have also upheld civil liberties such as freedom of expression. Much like the legislators, the understanding of Internet governance issues remains limited among the judiciary.

3.9. Public sentiment about online regulation is difficult to decipher. Young Pakistanis have grown up with social media platforms and apps, and the public reaction to the potential blocking of social networks now may be markedly different from the response to the YouTube ban[105] that persisted in Pakistan for three years in response to a blasphemous video. Pakistani Internet users are also engaged in social and political commentary on the Internet, and even though social media users constitute only less than 20 percent of the total population, the online public opinion tends to affect government policy.

3.10. At the same time, Pakistani citizens are extremely politically polarised on social media, and political parties and their supporters have played on these differences by artificially amplifying their political propaganda, especially before elections. Such showdowns, especially on Twitter, often degrade into vitriol, with abuse and trolling of opponents. Even without direct financial support of their political or social groups, users who ideologically support one party, a cause or a belief system regularly spar with users that hold different views. Hyper-nationalism, sexism, and sectarian and ethnic hatred are also abundantly visible in Pakistani online spaces, leading to discrimination and harassment of marginalised groups. Coordinated smear campaigns against independent journalists and defenders of online free expression

102 Trends Monitor. (2018). Analysis report Beta. Digital Rights Monitor. Available at http://digitalrightsmonitor.pk/analysisreportbeta/

103 The Express Tribune. (2020). LHC takes notice of anti-judiciary campaign on social media. Available at https://tribune.com.pk/story/2148303/1-lhc-takes-notice-anti-judiciary-campaign-social-media

104 Shehzad, R. (2020). PM Imran takes notice of 'malicious' social media campaign against top judge. The Express Tribune. Available at https://tribune.com.pk/story/2198793/1-pm-takes-notice-malicious-social-media-campaign-top-judge

105 Wilkes, T. (2016). Pakistan lifts ban on Youtube after launch of local version. Reuters. Available at https://www.reuters.com/article/us-pakistan-youtube/pakistan-lifts-ban-on-youtube-after-launch-of-local-version-idUSKCN0UW1ER

spring up from time to time.[106] Ironically, campaigns launched through coordinated user activity have also recommended responsible journalism and the need for strict social media regulation in the recent past.[107]

3.11. With this context, the following policy options are discussed regarding PECA:

Policy option 1 – Maintain PECA status quo

3.12. Since 2016, government agencies have used the law to block online content, send content removal and account information requests to Internet companies, and police the online expression of users. At the same time, there was little effort to improve the transparency, accountability, and technical capacity of the enforcement agencies. There was also no attempt to review the impact of PECA on digital rights.

3.13. In terms of protection of women and children, FIA did arrest culprits[108] involved in national or international child pornography rackets; it also responded to some of the many complaints lodged by women about online harassment[109] and blackmailing[110], and some of its investigations led to convictions[111]. However, its capacity to deal with all complaints and to conduct efficient and effective investigations is severely limited. FIA's lack of investigative capacity is aggravated by similar lack of capacity at the prosecutorial and judicial levels.

3.14. If PECA's legal and practical issues are left as they are, it is likely that it would continue to be used to selectively target online dissent and control the access to online information to suit the interests of powerful lobbies. It would also lead to more self-censorship among Pakistani Internet users.

3.15. Moreover, if Parliament does not actively push for a review and amendments process for PECA, it is likely the government would continue to make regressive, overbroad, and authoritarian attempts to operationalise content regulation under PECA as it did with the now-suspended Citizen Protection (Against Online Harm) Rules 2020.

Policy option 2 – Introduce amendments to PECA

3.16. Legal amendments can bolster the existing safeguards in the law, such as the data seizure protocol, and introduce new protections where they were missing, such as the public interest defence of online speech. The law could be amended to bring in oversight mechanisms, especially a review process for content blocking, and transparency.

106 DRM. (2019). DRM Investigates: Twitter accounts behind the hashtag #arrestantipakjournalists. Digital Rights Monitor. Available at https://digitalrightsmonitor.pk/drm-investigates-twitter-accounts-behind-the-hashtag-arrestantipakjournalists/

107 Jahangir, R. (2019). Digital campaign meant to educate journalists, not ridicule: PTI. Dawn. Available at https://www.dawn.com/news/1494724

108 Durrani, Z. (2018). Man convicted under cybercrime law for child pornography. Digital Rights Foundation. Available at https://digitalrightsfoundation.pk/man-convicted-under-cybercrime-law-for-child-pornography/

109 Dawn. (2017). 14-month jail for harassment through Facebook. Available at https://www.dawn.com/news/1349105/14-month-jail-for-harassment-through-facebook

110 Ullah, I. (2017). Peshawar man gets 12-year jail term for blackmailing woman on Facebook. The Express Tribune. Available at https://tribune.com.pk/story/1455517/man-peshawar-gets-12-years-creating-womans-fake-facebook-profile-blackmailing

111 Gilani, N. (2019). The State Vs Usman Sohail Butt. Digital Rights Foundation. Available at https://digitalrightsfoundation.pk/the-state-v-usman-sohail-butt/

3.17. Content regulation and decriminalisation of online expression can be important considerations for amendments. Operational flaws can be addressed by including clear guidelines and principles in line with constitutional guarantees and international human rights law.

3.18. The drawback of this policy option is that the amendments may remain superficial unless a comprehensive review of PECA and an associated multi-stakeholder consultative process is conducted to determine the nature, scope, and details of the amendments. This policy option could be time consuming.

3.19. It is also possible that any amendment process would have to contend with the national security paradigm and authoritarian tendencies to control online information just as it happened during the legislative process to pass the law in 2016.

Policy option 3 – Repeal PECA and create a new legislative framework

3.20. This policy option is rather ambitious and perhaps impractical given the current policy context. It would, however, allow the Parliament and the government to entirely get rid of the problematic anti-cybercrimes law and start discussions on Internet governance from scratch.

3.21. Lawmakers would then be able to deliberate on the questions related to online harms, the decriminalisation of defamation, the consonance of online regulation with others laws governing expression in Pakistan, and the separation of content regulation from cybercrimes. They could also seek inputs from local and global digital rights experts about international best practices regarding content regulation and the standards enshrined in international human rights law to develop a progressive law that serves the local needs.

3.22. The downside is that it would require political will and capacity for the legislature and executive to conduct this exercise. At present, such will and capacity does not exist. Technical and legal support for such an effort could perhaps be provided from the private sector and civil society organisations.

3.23. However, the creation of new policy and legislative frameworks would also require the lawmakers to develop an understanding of Internet governance and digital rights, and move beyond the self-interested, knee-jerk reactions towards content regulation that they seem to have developed based on their own social media use. This is also a tough ask, given that legislators are occupied with other pressing matters, including pandemic response and economic challenges.

4. Policy Recommendations

4.1. Out of the policy options presented in the previous section, the option for amending PECA is the most balanced approach in terms of risks and benefits. The following policy recommendations are being suggested to support the process of bringing about amendments in the anti-cybercrimes legislation.

Review PECA's legal and enforcement issues

4.2. Before any attempt is made to reform PECA, it is best that a comprehensive review of the legal problems and the practical challenges faced in its three-year implementation should be commissioned by the government.

4.3. It should be ensured that the review is independent. A multi-stakeholder steering committee could be set up to supervise the review process. The committee could be composed of representatives from the government, private sector, civil society organisations working on human rights and Internet governance, media, and the legal community.

4.4. Expert consultants, staff, and budget should be provided for the review process, and the consultants should be granted access to government agencies, especially PTA and FIA, for their study. Government officials should also be given immunity to speak candidly with the reviewing team so that the issues, achievements, problems, and needs related to PECA implementation are effectively brought to light.

4.5. The findings of the review should be made public and used by the ministries of information technology, law, and human rights to deliberate on a future course of action regarding PECA. The findings should also be discussed in Parliament to suggest potential solutions to any problems identified.

Introduce an amendments bill for PECA

4.6. Based on the findings of the PECA review, the government should start a new process to introduce amendments to the law. Care should be taken to ensure that this is not a hasty or symbolic process. Rather, detailed consultations should be conducted on the draft amendments.

4.7. The consultative process should have clear objectives; it should be broad-based, transparent, and responsive. The relevant Parliamentary committees should also solicit public input about the draft amendments before the proposed sections are discussed in the lower and upper houses of the Parliament.

Decriminalise online expression and defamation

4.8. Criminalisation of online expression has a chilling effect on the political and personal speech of citizens as well as on the work of journalists and human rights defenders, especially in a country such as Pakistan which has a poor record for press freedom and human rights.

Criminalisation of speech, as shown by the enforcement of PECA, can be misused to target and stifle politically critical expression online, even though a democratic society thrives on independent political discourse.

4.9. International human rights law allows restrictions on expression that are necessary and proportionate to achieve a legitimate purpose. Courts can use this test to rule on the legality of online expression. However, these should be civil remedies and should not include prison sentences that are often used as an intimidating tactic to compel citizens to self-censor their expression and opinions.

4.10. One argument often presented against decriminalisation of speech is that it would leave citizens exposed to hate speech and its undeniable impact, including violence. However, as the United Nations Secretary General has noted, limiting hate speech "does not mean limiting or prohibiting freedom of speech"[112], rather it means preventing hate speech from escalating into incitement to discrimination, violence, and hostility.

4.11. Unilateral regulation of online hate speech content will invariably run into jurisdictional issues, and users may find ways around firewalls to access blocked content. Technological solutions may also not present a panacea, but Internet companies have recently started working with States to remove violent extremist online content and the government may explore that option. Experts have suggested a broad and strategic alliance among government, industry, civil society representatives, and citizens to tackle the menace of online hate.[113] The right balance between a regulatory approach and other means to address the causes, drivers, and impact of hate speech must be discussed as a question of state policy rather than naively believing that the threat of imprisonment could be the sole deterrent to hate speech.

4.12. Similarly, criminal defamation creates a threat against the online expression of users, and is also used as a means to apply legal pressure on the news media. It poses the risk that a prison sentence may be applied to even a peaceful exercise of the right to free speech. Despite accounting for *mens rea* (intention; knowledge of falsity), PECA Section 20 that deals with defamation is still more intrusive than civil sanctions. International human rights standards have evolved over the past decade to acknowledge that criminal defamation is not a justified or legitimate sanction on freedom of expression and should be abolished.[114]

4.13. Even if the criminal defamation clause is struck out from PECA, Pakistan still has other criminal defamation laws and codes. The inclusion of defamation in PECA was, therefore, superfluous to begin with. Additionally, the case law for the penal code provisions for defamation and the Defamation Act 2004 shows that most cases result in acquittals or dismissals[115], suggesting that civil sanctions should be enough to protect reputations.

112 United Nations. (2019). United Nations strategy and plan of action on hate speech. Available at https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20Plan%20of%20Action%20on%20Hate%20Speech%2018%20June%20SYNOPSIS.pdf

113 See Bailey (2006), Banks (2010), and Parmar (2018) in Annex C: Bibliography

114 See Article 19 policy brief (2017) and Mendel (2004) in Annex C: Bibliography.

115 Global Information Society Watch. (2017). Unshackling expression: A study on laws criminalising expression online in Asia. Association for Progressive Communications. Pg 112.

Separate the online content regulation provision from cybercrimes

4.14. PECA merges the separate concepts of cyber offences and content regulation in a single law. The placement of these provisions in the law also hints at the different nature and domains of these two aspects of Internet governance. The offences and their punishments are prescribed in Chapter II of PECA whereas unlawful online content is discussed separately in Section 37 in Chapter III, which deals with the procedural powers of investigation of cybercrimes.

4.15. Ideally, content regulation should have been dealt with through an altogether separate legislative framework rather than lump it with an anti-cybercrimes criminal law that deals with online harms and cyber threats to citizens.

4.16. Policymakers should deliberate on why and how they can segregate the two aspects through amendments in PECA. The ideal move would be to repeal Section 37 from the law. A separate online content regulation framework would make it much easier to establish clear principles for dealing with content, build transparent judicial oversight mechanisms, and ensure protections for the fundamental freedoms of the citizens on the Internet.

Build investigative and judicial capacity for prosecution and trials of cybercrime offences

4.17. For efficient and effective enforcement of the law, the government must build the technical capacity and enhance the human resource capacity of the investigative agency by allowing it to hire more investigators, including women officers. It should support the FIA's digital forensics capability by strengthening or setting up more independent forensics labs. Officers should be provided opportunities to receive technical training for investigating cybercrimes as well as sensitivity training for dealing with complainants.

4.18. Similarly, more state prosecutors and judges are necessary for the cases to move through the justice system without delays. The prosecutors and judges also require specialised training.

4.19. The FIA has developed a case management system, but the case listings should also be made public and the complainants should also have access to a public-facing, secure management information system whereby they can track the progress of their complaint. To further its support to Internet users, FIA should also set up facilitation or liaison centres where complainants can be guided and provided psychological counselling for cases involving trauma.

4.20. These efforts would require a significant undertaking from the government to allocate sufficient funds in the annual budget. In return for the capacity building, the FIA should ensure that it transparently shares its performance reports and case audits with the legislators and the public, and develops internal accountability processes whereby aggrieved complainants can appeal for the review of incompetence, mishandling of cases or misuse of power by authorised officers during the investigative process.

Launch an open, fair, and transparent multi-stakeholder consultative process for rules of business for the regulation of online content

4.21. Since the government has formed a committee to consult with stakeholders on the currently suspended Citizen Protection (Against Online Harm) Rules 2020, it is recommended that the government should first withdraw the existing set of rules. A consultative process that takes place while the rules are held in suspension does not seem in good faith and will not engender trust with credible stakeholder representatives.

4.22. Once the rules are officially withdrawn, the government must share its policy vision for online harms. This may include an attempt such as the UK white paper on online harms that led to comprehensive consultations with digital rights groups and the private sector on the scope, regulatory model, practical concerns, use of technology, and citizen engagement regarding online harms.

4.23. The government must define a clear and transparent process to solicit multi-stakeholder inputs and explain how it intends to use the feedback for drafting the rules of business for content regulation.

5. Legal Amendments

5.1. A mechanism for introducing amendments to PECA was presented in the policy recommendations. This section shares some potential legal amendments that prominently featured in the research for this white paper and necessitate special mention.

5.2. Insert a new section for 'defense of public good' at the end of Chapter II in the law. The proposed language of the section is: "Any person whosoever commits any of the offences mentioned above shall not be liable to any punishment provided that the person can establish that the offence(s) are done in good faith and to further the public good or to expose criminal activities." The concern that this public interest defense may lead to unmerited disclosures of online personal data held by government departments through the action of self-proclaimed whistleblowers with a less-than-perfect understanding of the "public interest" should be addressed through separate legislation on personal data protection and whistleblower protections. Freedom of information laws also typically provide legal guidance about disclosures. For the purposes of PECA, the defense of public good could be qualified by including a "public interest test" against disclosures or referring to provisions in existing laws, such as the federal Right of Access to Information Act 2017.[116]

5.3. Remove Section 20 "Offences against the dignity of a natural person" from the law as this section criminalises satire, political memes, and other forms of artistic expression, and furthermore defamation clauses are already present in the Pakistan Penal Code and the Defamation Act 2004.

5.4. Remove Section 25 "Spamming" as it can be dealt with through the Pakistan Penal Code or the PTA rules. It should not be a criminal offence rather it can be dealt through civil remedies.

5.5. Amend Section 31 "Expedited preservation and acquisition of data" to introduce an expedited process for obtaining court warrant for urgent cases and remove the post-fact intimation to court within 24 hours. In addition, the section should provide for a process of internal oversight for expedited access to data whereby the investigating officer may need to take written permission from a senior officer authorised to make decisions. The senior officer could review the severity of the case before allowing expedited access and ensure that evidence protection protocols are followed. This process should also be reflected in the rules of business.

5.6. Amend Sections 31 and 34 to exclude privileged communication that is protected by the Pakistan Penal Code, for example counsel-client communication and spousal communication. The proposed language for the amendment is: "However, all content and data deemed as privileged communications under other laws shall remain exempt from disclosure and shall not be admissible."

5.7. Remove Section 37 "Unlawful on-line content" from the law. This section gives unfettered powers to the PTA to interpret the reasonable restrictions supplied in Article 19 of the Constitution. Such interpretation should only be done either with adequate legislative guidance

116 For example, the Australian authorities have defined a public interest test in accordance with the Government Information (Public Access) Act 2009.

or by the higher courts. Furthermore, censorship of content by blocking or removing access to online information is not the same subject as cybercrimes, as also discussed in the policy recommendations section of this paper.

5.8. In the event that the policy recommendation for repeal of Section 37 is not followed, insert a new section for the 'formation of an oversight committee' in Chapter III. The multi-stakeholder committee will review the content takedown decisions of the authority. The proposed language of the section is: "A committee shall be created under this Act, by the Federal Government, and should consist of parliamentarians from the ruling party and the opposition as well as representatives of civil society, industry, lawyers, and media." Additional sections may be added to spell out the formation, composition, and responsibilities of the committee. Furthermore, the restrictions on expression borrowed from Article 19 of the Constitution should be clearly defined along with precise checks of necessity and proportionality to offer guidance to executive officers so that they may interpret and apply these restrictions in a transparent and accountable manner.

5.9. Amend Section 39 "Real-time collection and recording of information" to specify the High Court as the appropriate court of law for a warrant for this section, and add language to ensure that the procedure for real-time data collection should follow the same standards as prescribed in the The Investigation for Fair Trial Act, 2013.

6. Conclusion and Next Steps

6.1. PECA requires urgent reforms to offer concrete protections to the fundamental freedoms of Pakistani citizens.

6.2. This white paper has presented some policy recommendations for the government, policymakers, legislators, and other relevant stakeholders to help them pursue and undertake reforms in the anti-cybercrimes legislation at the earliest.

6.3. The analysis, policy context, recommendations, and potential legal amendments shared in this paper can also be used as the basis of a sustained advocacy campaign by human rights defenders and civil society representatives to demand progressive changes in the law.

6.4. A multi-stakeholder approach should be followed to use this paper and its recommendations to engage with the issue of Internet governance policy in Pakistan. The paper's deliberations can support more multi-stakeholder efforts to refine and promote the demands to seek reforms in PECA.

Appendix A: About the Act

A.1. The Prevention of Electronic Crimes Act (PECA) 2016 prescribed punishments for 24 offences: Unauthorised access to information systems or data; unauthorised copying or transmission of data; interference with information system or data; unauthorised access to critical infrastructure information system or data; unauthorised copying or transmission of critical infrastructure data; interference with critical infrastructure information system or data; glorification of an offence (relating to terrorism or people convicted for terrorism or activities of banned groups or individuals); cyber terrorism; hate speech; recruitment, funding and planning of terrorism; electronic forgery; electronic fraud; making, obtaining or supplying device for use in offence; unauthorised use of identity information; unauthorised issuance of SIM cards; tampering of communication equipment; unauthorised interception; offences against the dignity of a natural person; offences against modesty of a natural person and minor; child pornography; malicious code; cyber stalking; spamming; and, spoofing.

A.2. Critical infrastructure is defined in the law as assets, facilities, systems or processes which if compromised could either impact delivery of essential services, including those services whose disruption could have physical, economic or social impact, or cause a significant impact on national security, national defense or the functioning of the State.

A.3. Glorification is explained to include "depiction of any form of praise or celebration in a desirable manner".

A.4. If an offence related to critical infrastructure or the "glorification of an offence" is committed or threatened with the intent to create fear, panic or insecurity "in the Government" or among the public or to advance interfaith, sectarian or ethnic hatred or to advance the objectives of banned organisations, then this will be considered "cyber terrorism" under PECA.

A.5. Hate speech is described as speech that "advances or is likely to advance interfaith, sectarian or racial hatred".

A.6. The offence against the "dignity of a natural person" includes information that is known to the original poster as false and that intimidates or harms the reputation or privacy of a natural person.

A.7. The offence against the "modesty of a natural person and minor" states that the use of morphed or original sexually explicit content to harm, blackmail, or take revenge or create hatred against a natural person shall be punished. For this offence and the offence of child pornography, the law defines minors as children less than 18 years of age.

A.8. Malicious code is explained as a computer programme or a hidden function in a programme that damages an information system or data, compromises the performance of such systems, compromises the availability of data or uses the system or data without authorisation.

A.9. Actions considered as cyber stalking include repeated attempts to contact someone online despite their clear indication of disinterest; monitoring or spying of someone's electronic communications such that it results in a fear of violence, alarm or distress among the monitored person; and, the non-consensual capture or distribution of someone's photos or

videos. Regarding these actions, the law mentions intent, specifically the offender's intent to coerce, intimidate or harass any person.

A.10. Intentional transmission of harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or direct marketing messages without allowing users to opt-out are considered spamming.

A.11. Establishing a website or sending information with a counterfeit source and to deceive users into believing it was an authentic source is considered spoofing.

A.12. Many of the offences mention "dishonest intention", which is defined by the law as intention to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred or incitement to violence.

A.13. The punishments vary from prison terms of 3 months to 14 years and fines ranging from Rs. 50,000 to Rs. 50 million. The maximum penalties are for offences of cyber terrorism. The law also allows for both imprisonment and fines at the same time.

A.14. PECA gave the federal government the power to establish or designate a law enforcement agency for the purposes of investigating cyber offences defined under the law. The agency is required to develop its own capacity for forensic analysis, but the government could help it out by making rules for the specialised training of staff. In September 2016, the Federal Investigation Agency (FIA) was designated as the investigating force for cybercrimes. Under the law, the FIA is required to submit a half yearly performance report to Parliament.

A.15. Authorised law enforcement officers were given the powers to access and inspect information systems, use the system to search for data, obtain or copy the data, and request decrypted information from system owners.

A.16. Officers are required to get a court warrant for seizure of devices, search of premises where the devices are held, and disclosure of data, by demonstrating reasonable grounds for the purpose of a criminal investigation. However, in cases where the officer is satisfied that the data might be modified or destroyed, the officer can acquire the data through a written notice but will have to bring this to a court's notice within 24 hours.

A.17. The law advises the officers to act with proportionality, ensure integrity and secrecy of the information system and data acquired through court warrant, not interfere with data unrelated to the investigation, and avoid disruption to the business operations at the premises being searched through a court warrant. Officers are also required to use technical measures to maintain the data or information system's integrity and chain of custody, and only seize it as a last resort.

A.18. For seized data, law enforcement officers are bound to keep it secure and private. A mechanism is also prescribed for officers to follow when dealing with a seized data or information system, including making a list of seized items and providing the forensic image of the data or system to its owner, subject to conditions.

A.19. PECA also made it mandatory for service providers to retain traffic data for one year.

A.20. The law designated the telecommunication regulator — the Pakistan Telecommunication Authority or PTA — as the enforcement agency.

A.21. Under PECA Section 37, the PTA has been granted the power to "remove or block or issue directions for removal or blocking of access to an 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 incitement to an offence".

A.22. The PTA is empowered to prescribe rules, with the approval of the government, that provide for safeguards, transparent process, and effective oversight mechanism for the content removal and blocking provision. Until the rules were formed, it was required to exercise its powers in accordance with the government's directions.

A.23. The law allows persons aggrieved by PTA's content blocking decisions to file a review application before the authority within 30 days of the order and the review decision could be challenged in a High Court within 30 days of the review.

A.24. PECA protects service providers from civil or criminal liability for the illegal actions of their users, except where a person making the allegation could prove that a service provider had actual knowledge and wilful intent to participate, facilitate, aid or abet the illegal activity. Service providers are also not liable for legal disclosure of data.

A.25. The law allows the relevant law enforcement agency to get a court warrant for real-time information collection for not more than seven days, after satisfying the court that the real-time content is "reasonably required" for a specific criminal investigation.

A.26. The officers are required to tell the court why they believe the data sought will be available from the person in control of the information system; identify and explain the specific type of information sought; identify and explain which offence the warrant deals with; explain the need for multiple disclosures if applicable; specify measures to ensure the privacy of other users during real-time data collection; explain how the lack of real-time data collection will frustrate the investigation; and, explain why the real-time data recording is necessary for the purpose for which the warrant is applied.

A.27. PECA mandates the federal government to set up or designate an independent forensic laboratory to benefit investigations and provide expert opinion to courts regarding the evidence presented for prosecution of cybercrimes.

A.28. Illegal and non-consensual disclosure of personal data by any person, service provider or authorised law enforcement officer, with the intent to cause harm or to compromise confidentiality of the person whose data is disclosed, is also a punishable offence under PECA. The burden of proving good faith will be on the accused.

A.29. The anti-cybercrimes law also allows the federal government to cooperate with foreign governments and agencies in cybercrime investigations by sharing evidence, disclosing data, and conducting real-time surveillance of information systems. However, the law also specifies grounds upon which the government could deny such requests for cooperation by foreign

governments, for example, where these requests are of a political nature or might prejudice Pakistan's sovereignty, among other reasons.

A.30. Except cyber terrorism, child pornography, and offences against modesty of a natural person or minor, all other offences are non-cognisable (warrant required for arrest), bailable, and compoundable (the complainant and accused can reach a settlement).

A.31. According to the law, the government and the higher judiciary would designate presiding officers to try offences under PECA and arrange for special training of these officers. The court decisions for offences listed under PECA can be appealed to a high court or a court of sessions depending upon whether the court of sessions or a magistrate heard the case in the first instance respectively.

A.32. The law also mandates the government to set up computer emergency response teams to respond to cyber threats.

A.33. Section 51 of PECA grants the federal government the power to make rules for carrying out the purposes of the law. The rules could specify training and qualifications of investigating officers, investigation procedures, procedure for seeking orders from PTA for content removal, inter-agency coordination, and functions of a forensic laboratory and its staff, among other things.

Appendix B: Methodology

B.1. The following is a description of the process followed to gather research data and provide the analysis and recommendations in this paper.

B.2. In order to provide recommendations for PECA reforms, an extensive review of existing literature on the topic was conducted. Desk research was used to collect previous recommendations, policy briefings, and legal analyses related to PECA. The public comments submitted prior to and immediately after PECA enactment were reviewed. Studies conducted on the implementation of PECA from 2017 to 2020 were examined to understand the policy gaps and practical challenges of the law. Court judgements related to PECA implementation were included in the analysis. Attention was given to subsequent policy interventions such as the formulation of rules of business related to PECA, and similar official documents were also brought into consideration. The desk research, apart from looking at journal articles and news reports, focussed on the PECA-related work of the leading digital rights advocacy organisations, such as Media Matters for Democracy, Digital Rights Foundation, and Bolo Bhi, as these organisations have consistently produced studies and policy briefs in the past to monitor PECA implementation from a digital rights perspective.

B.3. An inductive approach was used to identify the issues with PECA clauses and collate the policy recommendations previously presented to the government regarding improvements in the law. Since the issues in PECA have persisted for the lifetime of the legislation, it was likely that many different sets of recommendations in the past offered similar strategies for intervention. The collation of these recommendations was done in a manner to eliminate repetition in the suggested actions. Data from news reports and research studies were coded to create categories for white paper analysis and recommendations. Potential categories were created to highlight risks to prominent digital rights, such as implications for freedom of expression, implications for privacy etc. However, these categories were finalised after the desk research. The categories were given clear sections or sub-headings for the discussion in the data analysis. The discussion was also linked to specific sections of the PECA law so as to make it convenient for policymakers to understand which amendments are being suggested relevant to existing PECA clauses.

Appendix C: Bibliography

Anjum, S. (2020). 'Digital forensics a rapidly evolving field of investigation'. The News International. Available at https://www.thenews.com.pk/print/613317-digital-forensics-a-rapidly-evolving-field-of-investigation

Archives. (2019). The Freedom of Expression Web Portal. Media Matters for Democracy. Available at https://foecaselaw.mediamatters.pk/archives/

Article 19. (2017). Policy Brief: Defining Defamation: Principles on Freedom of Expression and Protection of Reputation. Available at https://www.article19.org/data/files/medialibrary/38641/Defamation-Principles-(online)-.pdf

Ayyaz, N. (2019). Reviewing PECA's powers. Dawn. Available at https://www.dawn.com/news/1517355

Aziz, F. (2018). Pakistan's cybercrime law: boon or bane? Heinrich Boll Stiftung. Available at https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane

Aziz, F. (2019). Above the law. Dawn. Available at https://www.dawn.com/news/1507604

Bailey, J. (2006). 'Strategic Alliances: The inter-related roles of citizens, industry and government in combating Internet hate, Canadian Issues, 56-59.

Baloch, H. (2016). Internet Rights and Legislation in Pakistan: A Critique on Cyber Crime Bill, 2016. Bytes for All and the Association for Progressive Communications. Available at https://bytesforall.pk/sites/default/files/CSO-criticism-on-PECB-2016_IssuePaper.pdf

Banks, J. (2010). Regulating hate speech online. International Review of Law, Computers and Technology, 24 (3), 233-239.

Bolo Bhi. (2017). PECA 2016: Recommendations for Implementation and Oversight. Available at http://bolobhi.org/wp-content/uploads/2017/04/PECA-recommendations.pdf

Bolo Bhi. (2018). Recommendations on Rules. Available at http://bolobhi.org/wp-content/uploads/2018/01/Recommendations-for-Rules.pdf

Bolo Bhi. (2019). Note for Senate Functional Committee on Human Rights On: Use of of Section 20 of PECA & the Abuse of Power by the FIA. Available at https://bolobhi.org/wp-content/uploads/2019/11/Note-for-Senate-Functional-Committee-on-Human-Rights.pdf

Bolo Bhi. (2019). PECA: A Three-year Review. Available at https://bolobhi.org/wp-content/uploads/2019/11/Summary-of-Report-updated-18.10.2019.pdf

Bolo Bhi. (2019). Petitions against FIA, PTA and PECA. Available at http://bolobhi.org/petitions-against-fia-pta-and-peca-2/

Bolo Bhi. (2019). Record of PECA Cases before Courts in Karachi. Available at http://bolobhi.org/wp-content/uploads/2019/06/PECA-Record-May-31-2019.pdf

Bolo Bhi. (2019). Recommendations from Legal Experts on Defamation Laws. Available at https://bolobhi.org/wp-content/uploads/2019/11/Recommendations-from-Legal-Experts.

pdf

Bolo Bhi. (N.D.) Tracking Laws. Available at https://bolobhi.org/resources/tracking-laws/

Bolo Bhi. (N.D.) Archive: Prevention of Electronic Crimes Act. Available at https://bolobhi.org/archive-prevention-electronic-crimes-bill-2015/

Dawn. (2017). Journalist Taha Siddiqui's case shifted to cybercrime circle. Available at https://www.dawn.com/news/1343550

Digital Rights Foundation. (N.D.) Mapping cases under the Prevention of Electronic Crimes Act (PECA) 2016. Available here: https://digitalrightsfoundation.pk/mapping-peca-2016/

Digital Rights Foundation. (2018). Content regulation in Pakistan's Digital Spaces. Available at https://digitalrightsfoundation.pk/wp-content/uploads/2017/12/DigitalRightsFoundationSubmissionSpecialRapporteurFreedomofExpression.pdf

Global Information Society Watch. (2017). Unshackling expression: A study on laws criminalising expression online in Asia. Association for Progressive Communications. Available at http://digitalrightsmonitor.pk/wp-content/uploads/2018/02/giswspecial2017_web.pdf

Haq, R. (2016). National Assembly approves cybercrime bill. The Express Tribune. Available at https://tribune.com.pk/story/1083974/national-assembly-approves-cybercrime-bill

Hussain, J. (2019). Facebook, Twitter uncooperative in addressing cyber crime complaints: FIA. Dawn. Available at https://www.dawn.com/news/1474764

Hussain, S., Jan, M. A., Mehmood, W., & Mahsud, M. I. (2019). Electronic Crimes, Internet and Violence: Jama'at-e-Islami and the Progressive Civil Society of Pakistan. Pakistan Journal of Criminology, vol (11), no. 2., (83-94). Available at https://www.academia.edu/download/61618035/8_Electronic_Crimes_Internet_and_Violence20191227-75488-1jgn67t.pdf

Imran, M. (2018). Govt to change law and severely punish accusers who falsely allege blasphemy, IHC told. Dawn. Available at https://www.dawn.com/news/1389774

Khan, E. A. (2019). The Prevention of Electronic Crimes Act 2016: An analysis. LUMS Law Journal. Available at https://sahsol.lums.edu.pk/law-journal/prevention-electronic-crimes-act-2016-analysis

Khan, R. (2016). Controversial Cyber Crime Bill approved by NA. Dawn. Available at https://www.dawn.com/news/1251853

Khan, S., Tehrani, P. M. & Iftikhar, M. (2019). Impact of PECA-2016 Provisions on Freedom of Speech: A Case of Pakistan. Journal of Management Info, pg. 7-11. Available at https://www.researchgate.net/publication/334962173_Impact_of_PECA-2016_Provisions_on_Freedom_of_Speech_A_Case_of_Pakistan

Malik, A. A., Mujtaba, A. & Azeem, W. (2019). Deficiencies in Peca and Proposed Amendments to Facilitate Investigating Agencies, Courts and Prosecution; Proper Use of

Electronic Devices for Effective Implementation of Law. International Journal for Electronic Crimes Investigation, vol (3), no. 3, (1-6). Available at http://ojs.lgu.edu.pk/index.php/ijeci/article/view/333/293

Media Matters for Democracy. (2017). Criminalising Expression: A study of Pakistan's cyber crime legislation.

Mendel, T. (2004). The Case against Criminal Defamation Laws, in Ending the Chilling Effect, Karlsreiter, A. & Vuokko, H. (eds.). OSCE. Available at https://www.osce.org/files/f/documents/2/3/13573.pdf

Niazi, A. (2017). Cyber-crime allegations: PPP leader's son arrested for 'maligning' defector to PTI Firdous Ashiq Awan. Pakistan Today. Available at https://www.pakistantoday.com.pk/2017/06/18/cyber-crime-allegations-ppp-leaders-son-arrested-for-maligning-defector-to-pti-firdous-ashiq-awan/

Nizamani, A. (2019). What the court and FIA ought to do in cyber crime cases. Courting the Law. Available at https://courtingthelaw.com/2019/10/18/commentary/what-the-court-and-fia-ought-to-do-in-cyber-crime-cases/

Online. (2017). First ever sentence awarded to suspect under Cyber Crime Act in Pakistan. The Nation. Available at https://nation.com.pk/18-May-2017/first-sentence-awarded-to-suspect-under-cyber-crime-act-in-pakistan

Order Sheet. (2017). Usama Bin Mehmood vs. The State & another. Lahore High Court. Available at https://sys.lhc.gov.pk/appjudgments/2017LHC3339.pdf

Order Sheet. (2017). Junaid Arshad vs. The State & another. Lahore High Court. Available at https://sys.lhc.gov.pk/appjudgments/2017LHC3933.pdf

Order Sheet. (2018). Muhammad Ashraf vs. The State & another. Lahore High Court. Available at https://sys.lhc.gov.pk/appjudgments/2018LHC1797.pdf

Pakistan Today. (2019). LHC moved against FIA cybercrime wing over failure to submit progress report. Available at https://www.pakistantoday.com.pk/2019/07/03/lhc-moved-against-fia-cybercrime-wing-over-failure-to-submit-progress-report/

Parmar, S. (2019). The legal framework for addressing "Hate Speech" in Europe. Council of Europe. Available at https://rm.coe.int/opening-session-2-parmar-the-legal-framework-for-addressing-hate-speec/16808ee4bf

Rana, S. (2018). Bottlenecks, Incompetence and Abuse of Power: An analysis of PECA's implementation. Media Matters for Democracy.

Reuters. (2016). Pakistan passes controversial cyber-crime law. Available at https://www.reuters.com/article/us-pakistan-internet/pakistan-passes-controversial-cyber-crime-law-idUSKCN10N0ST

The Nation. (2020). Amending PECA 2016. Available at https://nation.com.pk/21-Jun-2020/amending-peca-2016

About Media Matters for Democracy

Media Matters for Democracy is a Pakistan based not-for-profit that works to defend freedom of expression, media, Internet, and communications in Pakistan. Our activities include policy research, advocacy, training, legal aid, and public interest litigation. The organisation was founded by a group of journalists who believe in free expression and are working to ensure that the media and public alike have the tools and an enabling environment to exercise their fundamental rights. Our core objective is to ensure that rights to free expression, association, access to information, and related freedoms are protected in Pakistan in policy and practice. For more information, please visit: mediamatters.pk

Centre for Peace and Development Initiatives

MediaMatters forDemocracy
Policy Research & Advocacy Initiative

PPF
-Strengthening the Media