Safety Theatre: The Constitutional and Human Rights Risks of Pakistan's E-Safety Bill

BOLO BHI
Advocacy - Policy - Research

samuelson-glushko
tech.law.policy
clinic

About Bolo Bhi

Bolo Bhi is a civil society organisation geared towards advocacy, policy, and research in the areas of digital rights and civic responsibility. This encompasses the right to information, free speech, and privacy online, so that the internet can be realized as a free and representative space for civic and political engagement for all segments of society, including marginalized communities and genders. Bolo Bhi believes that an informed citizenry with the knowledge, skills, tools and disposition towards civic engagement is integral for effective government transparency and accountability. For more information, visit our website at bolobhi.org.

About TLPC

Based at the University of Colorado Law School, the Samuelson-Glushko Technology Law & Policy Clinic (TLPC) advocates for technology laws and policies that advance the public at the international, national, and local levels. The Clinic addresses a wide range of issues, from civil and human rights and intellectual property law. TLPC engages in discussions on technology law and policy by representing clients before administrative, judicial, and legislative bodies, participating in amicus advocacy, conducting significant public policy research, and forming strategic partnerships with advocacy groups, public officials, and multistakeholder groups to effect change.

Acknowledgements

Bolo Bhi is grateful for the work of the Samuelson-Glushko Technology Law & Policy Clinic (TLPC) at the University of Colorado Law School in producing this report. We wish to acknowledge the contributions of TLPC Student Attorneys Matthew Engebretsen, Rina Mehana, and Sophie Pickering and of Vivek Krishnamurthy, TLPC's Director, in researching and drafting this report.

Date of Publication: March 2024

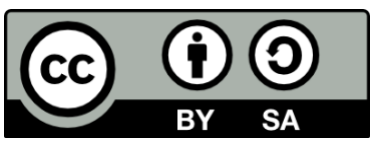

Table of Contents

This page left intentionally blank.

Introduction

This report identifies significant problems with Pakistan's E-Safety Bill and compares it with online safety legislation in other countries. On July 26, 2023, the federal cabinet provided approval in principle to the E-Safety Bill 2023.[1] Formally known as *"An act to provide for fostering and promoting safe online Social Network Platforms*,"[2] the E-Safety Bill purports to be a law that implements "reasonable restrictions" on online content. However, the E-Safety Bill raises numerous red flags. There are concerns that the Pakistani government will use the bill as a tool to suppress free speech and censor online content using online "safety" as an excuse. Some of the E-Safety Bill's most significant issues include:

1. its "one-size-fits-all" approach to regulating online platforms that have little in common,
2. its registration requirement,
3. the lack of clarity in the obligations it imposes on Social Network Platforms (SNP),
4. the risk that the law's vague provisions will be interpreted in an overbroad manner, and,
5. the reaction it may induce from foreign companies—who may simply stop serving customers in Pakistan in view of the onerous obligations it imposes.

Each of these issues implicates human rights considerations, such as the protection of freedom of expression and the right to information, as enshrined in Articles 19 and 19A of the Constitution of the Islamic Republic of Pakistan and the International Covenant on Civil and Political Rights (ICCPR).

Context

Countries all over the world, from Australia to the United Kingdom, are facing difficulties in determining how to regulate online content while respecting the fundamental rights of freedom of expression and access to information. The rapid advance of technology and the ability of various online platforms to quickly disseminate information to large audiences are creating a sense of urgency for countries to develop effective online safety legislation.

Pakistan is one of the countries currently attempting to enact legislation to regulate online platforms and the content they carry. Legislation in Pakistan is bound by the Constitution of Pakistan and, as a signatory party, the ICCPR. The Supreme Court of Pakistan has explained that "*every statute is in the public interest and must always align and flow with the text and spirit of the Constitution. Therefore, the constitutional values, fundamental rights and the principles of policy laid down under the Constitution enjoy a symbiotic relationship with any statutory framework including the one regulating media content . . .*"[3] This framework suggests both freedom of expression and the right to information must be respected and protected by any statute regulating media content. While the Supreme Court does consider some reasonable restrictions on these rights as acceptable (for example, to protect against hate speech or prevent minors from accessing pornographic material,) their legally permissible applications are limited.[4] The

---

[1] Ali, Kalbe, *Impact of New 'Cyber Laws' May Be Felt Far and Wide*, Dawn, July 27, 2023. https://www.dawn.com/news/1766979.
[2] Introduction, The e-Safety Bill (2023).
[3] Pakistan Electronic Media Regulatory Authority (PEMRA) v. ARY Communications Private Limited (ARY Digital) (2022), Supreme Court of Pakistan, 14-15
[4] Ibid., 16.

Supreme Court of Pakistan constrains the application of these restrictions, emphasizing "*The reasonable restrictions should therefore not only be rationally connected to, but also be no more than necessary to accomplish, any of the legitimate objectives mentioned in Articles 19 and 19A of the Constitution*."[5] This Report details how the E-Safety Bill fails to achieve its self-proclaimed goal of enhancing online safety and, even worse, implements restrictions that are not rationally connected to this goal. This examination highlights how the bill's inadequacies, particularly in its lack of precision and clear definitions, undermine its ability to achieve the intended purpose of safeguarding online spaces and maintaining an environment that protects freedom of expression and the rights of the individuals using these spaces.

1. One Bill to Regulate Many Vastly Different Platforms

The proposed E-Safety Bill imposes the same regulatory provisions on a wide range of platforms that vary in function and content. The ambitious scope of the bill raises concerns regarding how applicable the provisions are to each platform and whether the platforms can reasonably comply. The E-Safety Bill regulates Social Network Platforms, including Web TV channels (i.e., YouTube, Netflix, Amazon Prime), social networking sites (i.e., Twitter, Facebook, Instagram), cloud-based content distribution services (ambiguous as to what platforms this category includes), platform or communication channels, advertisers, e-commerce services providers, online information and content delivery systems (ambiguous as to what platforms this category includes), and other similar platforms as determined by the E-Safety Bill's regulating authority.[6]

The E-Safety Bill's broad reach favors quantity over quality as it regulates numerous platforms but does not tailor its provisions to address the distinct functions and content of each platform. One example arises from the bill's prohibition of content containing hate speech.[7] A Social Network Platform with content uploaded from a single source, such as Netflix uploading only the movies and shows it selects, can reasonably comply with the bill's prohibition because the individual or corporation is the sole source responsible for the platform's content. In contrast, a social networking site with millions of users constantly uploading content, such as Facebook, cannot ensure a complete absence of content containing hate speech on the platform because it is unreasonably burdensome to screen all the content preemptively.

Unlike the Pakistani E-Safety Bill, the Australian Online Safety Act 2021 treats different kinds of online platforms differently. For example, "social media services," "designated internet services," "search engine services," "app distribution services," and "hosting services" are all separate categories recognized by the law and subject to differential obligations.[8] Each provision of the act clarifies which categories of platforms it applies to. For example, under Part 7 – Cyber Abuse Material Targeted at an Australia Adult, Section 88 explains removal notices only as they apply to social media services, relevant electronic services, or designated internet services, Section 89 explains removal notices only as they apply to end-users, and Section 90 explains removal notices only as they apply to hosting service providers.[9] Similarly, the European Union's Digital Services Act (DSA) prescribes different obligations to different kinds of platforms. Some

[5] Ibid., 17-18.
[6] The e-Safety Bill, 2023, I (2) (oo).
[7] The e-Safety Bill, 2023, IV (28) (f).
[8] Australia Online Safety Act, 2021, 1(5).
[9] Ibid., Part 7 (88-90).

obligations are targeted at "All Intermediaries," but others implicate "Hosting Services," "Online Platforms" and "Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)" specifically.[10] The categorizations used in the Australian and European laws allow for more tailored regulations that apply to the particular function, service, and content of the platform. The Pakistan E-Safety Bill fails to categorize in this fashion, however, and provides vague regulations for platforms requiring detailed and specific regulations.

2. A Flawed Registration Regime

In order to operate in Pakistan, the E-Safety Bill subjects platforms to a registration obligation. This requirement raises concerns about the government's increased power to control content, potentially using it as a tool to dictate what information is accessible to the public. This immense regulatory power over Social Network Platforms jeopardizes the fundamental right to freedom of expression and the right to information guaranteed by Article 19 of the Pakistani Constitution and ICCPR.

While international law does not explicitly prohibit a registration obligation on digital platforms, it sets a standard that states must follow to ensure such a requirement is legitimate.[11] In order to do so, the Pakistani government must prove the registration obligation a) has a *legitimate aim*, meaning that the registration requirement should not be used as a tool to stifle dissent, control information, or censor critical voices; and b) is *necessary and proportionate*, meaning there are no less restrictive means available to reach such aim. As explained below, the E-Safety Bill fails both of these requirements.

The historical misuse of legislative measures in Pakistan raises substantial concerns that the government might employ registration requirements not for genuine safety purposes, but as a mechanism to assert control and stifle dissent. The government's past actions taken under the Prevention of Electronic Crimes Act 2016 (PECA) give rise to such concerns. This is evident from the 2020 ruling of Islamabad's High Court, in which the Court highlighted concerns that the provisions of PECA were being "*misinterpreted by the Pakistani public functionaries or being used in a reckless unprofessional manner to suppress critical journalistic pursuits*." The immense power vested in the E-Safety Authority to govern these platforms, coupled with a lack of a clear aim for this requirement, is itself proof that this requirement is not legitimate.

A comparative analysis with other jurisdictions demonstrates that the Pakistani government has failed to employ less restrictive means, as required by the second criterion spelled out above. By contrast, the European Union's DSA offers an alternative approach. Rather than mandating platform registration, it requires the appointment of a legal representative for platforms operating outside the EU, which ensures a legal presence without associated physical presence. The DSA explicitly clarifies that "*the designation of a legal representative within the Union …. shall not constitute an establishment in the Union.*" Conversely, Australia and the UK have charted different paths. Their legislation does not impose any registration or legal presence requirements on online platforms. In the UK, a platform registry exists for informational purposes, but it does not burden platforms with additional obligations. This approach

---

[10] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

[11] The United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, and the Organization of American States (OAS) Special Rapporteur on Freedom of Expression, *Joint Declaration On Freedom Of Expression And Elections In The Digital Age*, 30 April 2020.

acknowledges the importance of maintaining communications with platform companies without unduly interfering with their operations or pressuring them into doing a government's bidding.

On top of the registration requirement, a data localization obligation will follow. The Draft Data Protection Bill mandates that these companies process "critical personal data" exclusively within servers or digital infrastructure situated in Pakistan. However, this specialized processing adds to the burden of the SNPs and introduces severe privacy risks, as it compels companies to sort and identify data falling under this category to fulfill the additional requirements. This obligation, coupled with the registration requirement, contradicts the essence of the Internet, which thrives on inclusivity and the free flow of ideas, posing a significant challenge for Pakistan in maintaining a diverse digital landscape. If this requirement goes through, platforms may not register and could stop operating in Pakistan due to the fear of strict and vague content requirements which, if not complied with, carry the risk of financial loss, potential legal trouble, and the chance of imprisonment. The resulting departure of foreign platforms will reduce the choices Pakistanis have to communicate and impair their freedom of expression and access to information rights.

3. Unclear Prohibited Content

The proposed Pakistani E-Safety Bill, ostensibly introduced to safeguard against objectionable content, raises significant concerns regarding its potential impact on the bedrock of democratic societies: freedom of expression. Its provisions, rather than offering clarity, leave ample room for subjective interpretation. The vagueness of the bill's provisions exposes a critical flaw in its structure and opens the door to potential misuse and arbitrary suppression of dissenting voices. If passed in its current form, this bill poses a genuine threat to the very essence of democratic discourse in Pakistan.

One of the most alarming aspects of the proposed bill lies in its vague delineation of "prohibited content." While the intention to curtail harmful content is understandable, the bill's language leaves much to be desired in terms of specificity. What constitutes content "against the Islamic values and ideology of Pakistan, etc."[12] "derogatory remarks about any religion, sect, community" is left open to interpretation—as exemplified by the use of the vague "etc" in defining what content is unlawful![13] This vagueness not only undermines legal clarity but also creates a dangerous opening for potential abuse. The lack of clear definitions opens the door to arbitrary decisions on what is deemed prohibited, potentially leading to the suppression of legitimate and constructive discourse.

While the bill ostensibly seeks to maintain journalistic integrity, its stringent guidelines for news and current affairs programs seem to lean more towards stifling rather than upholding the free press. Promoting accuracy and fairness is an admirable aspiration, but mandating it is quite another. What is worse, the bill's vague language provides ample room for subjective interpretation and potential abuse. The requirement for "objectivity" in political analysis raises concerns about stifling critical discourse and limiting the plurality of perspectives essential for a robust democratic society. To put it bluntly, who gets to decide what is "objective" in the context of current events? Additionally, the stipulation to avoid "gratuitous" details in news coverage could be misconstrued as an attempt to sanitize reality, potentially undermining the public's

[12] The e-Safety Bill, 2023, Chpt. IV. 28(a)
[13] The e-Safety Bill, 2023, Chpt. IV. 28(d)

right to be informed in a full and complete manner. This, in turn, hints at an inclination to exert undue influence over media narratives, which is deeply troubling for a nation that values democratic principles.

In contrast to the proposed Pakistani E-Safety Bill, the United Kingdom's regulations for user-to-user and search services outline specific duties and safety measures, reflecting a more detailed approach to content moderation. Service providers are given a list of categories of content that children are not allowed to see, such as content that is abusive and targets characteristics like race and religion, or content that encourages violence.[14] Additionally, the UK bill creates different obligations for children as opposed to adults, which highlights a discernable commitment to the principles professed by the bill.[15] Specifically, it reinforces the notion that the bill is designed to protect individuals. It would make sense to have a different regime for adults and children whose needs in this context would be different. These provisions aim to ensure user empowerment, protect content of democratic importance, and offer mechanisms for reporting potentially harmful material.

This ambiguity not only diminishes the bill's efficacy but also poses a tangible risk of stifling lawful dissent, as it could facilitate arbitrary censorship under the guise of safeguarding societal values or institutions.

Similarly vague provisions of proposed e-safety legislation in Sri Lanka have drawn significant international criticism. The International Commission of Jurists (ICJ) expressed concerns about the Sri Lankan legislation, while noting that "*these clauses are overbroad in that they would encompass expression that is protected under human rights law*".[16] In view of their similarities, the same could be said about Pakistan's E-Safety Bill.

In summary, the current draft of the proposed Pakistani E-Safety Bill presents a concerning lack of clarity in its prohibition framework. The ambiguity surrounding prohibited content, especially when compared to other similar (albeit, flawed) legislation in other countries, raises significant concerns about the implementation of this bill.

4. Risk of Broad Interpretation and Discretionary Enforcement

The E-Safety Bill provides its enforcement agency, the E-Safety Authority, with broad powers to regulate Social Network Platforms. These powers include the authorization to access Communication Devices if it reasonably suspects contravention of the bill, conduct inspections of premises, and summon people for inquiry at its discretion.[17] In the wake of *Arshad v. Pakistan*, the vague provisions of the E-Safety Bill raise valid concerns that the Authority could abuse its broadly defined powers to suppress Pakistan's valued rights to free expression and privacy.

In *Arshad v. Pakistan*, the Islamabad High Court held that the Federal Investigating Agency (FIA) abused its powers under the Prevention of Electronic Crimes Act 2016 (PECA 2016) by

---

[14] UK Online Safety Bill, 2023, Chpt. 7, Section 59
[15] UK Online Safety Bill, 2023, Chpt. 2, Section 11
[16] International Commission of Jurists, "*Sri Lanka: Proposed Online Safety Bill would be an assault on freedom of expression, opinion, and information",* 29 September 2023. Accessible at: https://www.icj.org/sri-lanka-proposed-online-safety-bill-would-be-an-assault-on-freedom-of-expression-opinion-and-information/
[17] The e-Safety Bill (2023), II (4).

administering a vague notice to summon Arshad, a journalist.[18] The Islamabad High Court determined the notice was sent by the FIA in retaliation for Arshad's work as a journalist, and held the FIA violated Arshad's rights under Articles 19 and 19A of the Constitution of Pakistan.[19] The Court also noted there was a recent increase in the number of claims filed against public functionaries for abuse of PECA 2016 provisions.[20] Public functionaries were willing to abuse the provisions of PECA 2016 and stray from the procedures outlined by the law. The E-Safety Bill poses an even more potent threat as its provisions contain few, if any, limitations or procedural rules to constrain the Authority. The E-Safety Bill's lack of specificity regarding how the Authority may enforce the bill creates opportunities for abuse of the powers the bill grants.

Unlike the E-Safety Bill, the Australian Online Safety Act, 2021 limits the power of the Commissioner by specifically confining its regulatory power to Class 1 and Class 2 material. The former constitutes "material that offends against the standards of morality, decency and propriety generally accepted by reasonable adults," while the latter relates to materials "inappropriate for general public access and children under 18" respectively.[21] By using the Class system, Australia provides more precise definitions of the kind of online harm the Commissioner has the authority to regulate. In addition, other provisions of the act limit the sanctions the Commissioner can apply to each violation of the act based on the Class of material in question. Finally, the Australian law also includes examples of content the Commissioner does not have power to regulate.[22]

The United Kingdom's Online Safety Bill also contains safeguards against broad interpretation and discretionary enforcement of its provisions by officials. The UK legislation requires officials to go through the court system to get a warrant before searching any premises or seizing a device.[23] This restriction of power contrasts drastically with Pakistan's provision permitting the Authority to inspect premises and summon persons at its discretion. These provisions of Pakistan's E-Safety Bill are strikingly similar to provisions of Sri Lanka's bill, which have come under heavy criticism from learned international experts.[24]

5. Retaining Access to the Services of Foreign Corporations

The numerous issues found within the E-Safety Bill increase the likelihood that foreign corporations will refuse to establish and maintain a presence in Pakistan. For example, the E-Safety Bill holds all directors, partners, and employees of a corporation operating a Social Network Platform personally liable for any noncompliance with the provisions of the bill.[25] It is easy to imagine that many foreign corporations will not agree to operate under this type of liability because of the risk of arrest and punishment of their individual employees in Pakistan. If

---

[18] Rana Muhammad Arshad v. Pakistan, Global Freedom of Expression, Columbia University 2020, 2/5.
[19] Ibid.
[20] Ibid, 4/5.
[21] ESafety Commissioner. "Online Content Scheme: Regulatory Guidance." *Online Safety Act*, (2021): 4. Accessed January 28, 2024.
[22] Ibid.
[23] Schedule 12 Section 108, UK Online Safety Bill (2023).
[24] Office of the High Commissioner for Human Rights, *Human rights concerns over the two draft laws in Sri Lanka*, 13 October 2023. Accessible at: https://www.ohchr.org/en/press-briefing-notes/2023/10/human-rights-concerns-over-two-draft-laws-sri-lanka
[25] The e-Safety Bill, 2023, VIII (56).

the E-Safety Bill deters Social Network Platforms from operating in Pakistan, there will be fewer sources available to disseminate information throughout the country and fewer platforms for the Pakistani people to express their thoughts. These limitations will impact the ability of citizens to exercise their rights to freedom of expression and access to information.[26]

Conversely, the European Union's Digital Service Act requires the Commission and Board to implement online industry regulations through codes of conduct.[27] The DSA suggests the Commission consults with very large online platforms within the regulated industry, other very large online platforms, providers of intermediary services, civil society organizations, and other interested parties when the codes of conduct raise concerns for significant systemic risk.[28] Unlike the Pakistan E-Safety Bill, the DSA states the Commission and Board must account for the needs of all interested parties.[29] The Pakistan Digital Editors Alliance (PDEA) requests the Pakistani government make similar inquiries and "hold multi-stakeholder engagement with members of tech, media, and e-commerce industries for informative discussions and feedback before passing any law on the regulation of digital media and data protection."[30]

Conclusion

Based on this evaluation and comparative analysis, the Pakistani government should withdraw the E-Safety Bill. Numerous sections of the bill, including the Prohibited Content and the Powers and Functions of the Authority, are ambiguous and subject to abuse. In addition, the bill does not conform with international law or emerging global best practices. The bill ventures far outside the scope of any legitimate aim to reasonably restrict online content and fails to narrowly tailor necessary and proportionate regulations.

The bill's registration requirement and data localization obligations grant excessive control to the government, potentially deterring foreign corporations and limiting the diversity of online platforms available to Pakistani citizens. The vague delineation of prohibited content further compounds these issues, leaving room for subjective interpretation and increasing the risk of abuse. Without clear limitations and procedural safeguards, the broad powers granted to the E-Safety Authority raise serious concerns about potential misuse, echoing past instances of governmental overreach. Correspondingly, the Pakistani government should withdraw the E-Safety Bill from consideration and start with a new approach that puts respect for the Constitution and international human rights law front and center.

---

[26] Similar provisions have come under scrutiny. For example, the proposed Sri Lanka Online Safety Bill raises a similar concern. Its provisions potentially criminalize nearly all forms of legitimate expression, resulting in a chilling effect on the freedom of expression. The Asia Internet Coalitions (AIC) went as far as calling the bill "draconian" for its restrictive impact on public debate and the exchange of ideas.

[27] Article 35 (1), Digital Services Act, (2022).

[28] Digital Services Act, 2022, Article 35 (2).

[29] Ibid., Article 35 (3).

[30] "*PDEA Alarmed over Cabinet Approving Bills on Online Media Regulation, Data Protection*.", Pakistan Digital Editor's Alliance. July 28, 2023. Accessible at: https://pdea.pk/2023/07/28/pdea-alarmed-over-cabinet-approving-bills-on-online-media-regulation-data-protection/.