JOINT STATEMENT ON EMERGING DIGITAL LAWS IN BANGLADESH

by Access Now, ARTICLE 19, Human Rights Watch, PEN International, Robert F. Kennedy Human Rights, and Tech Global Institute

February 25, 2025

Bangladesh is undergoing a significant transitional phase, marked by wide-ranging systemic and structural transformations, including legislative reforms to cybersecurity and data protection statutes. Acknowledging the timely and necessary efforts of the Interim Government of Bangladesh to reform digital governance policies and regulatory frameworks, we, the undersigned organizations, remain concerned that these initiatives are being fast-tracked without sufficient transparency or inclusive consultation, echoing legislative approaches of previous administrations.

Of note, drafts of the *Cyber Protection Ordinance, 2025* (CPO) and the *Personal Data Protection Ordinance, 2025* (PDPO) fail to address the broader systemic challenges in cyberspace governance in alignment with fundamental rights under Bangladesh's constitutional framework and international human rights framework. Instead, these proposed ordinances rely on undefined, ambiguous, and/or overbroad terms and provisions, creating significant risks of misinterpretation, overreach, and abuse, particularly to suppress human rights and media organizations. Given the cross-border nature of digital services, markets, and communities, the current drafts also raise serious concerns about adherence to the principles of comity of law and conflict of laws. With the parliamentary process and its institutional safeguards currently suspended, concerns over transparency, public accountability, and adherence with human rights are even more pressing.

NON-TRANSPARENT DRAFTING PROCESS HINDERS MEANINGFUL PUBLIC ENGAGEMENT

We note with concern that certain proposed reforms, specifically the introduction of CPO and PDPO, are under consideration by the Interim Government of Bangladesh, however, without sufficient and inclusive stakeholder engagement, a robust feedback loop, or an evidence-based legislative process grounded in expert analysis and global best practices.

For instance, various versions of the draft CPO mirror the widely criticized *Digital Security Act, 2018* (DSA) and the *Cyber Security Act, 2023* (CSA) introduced by the previous regime. Despite the draft CPO being made available for public consultation for three days in December 2024 and, in response to concerns over insufficient time for meaningful stakeholder engagement, again for two weeks starting January 22, 2025, the consultation process failed to provide clear justifications for changes between drafts or explanations of the outcome of the earlier consultations. Furthermore, the proposed amendment to the *Bangladesh Telecommunication Regulation Act, 2001* (BTRA)—which enables surveillance, interception, and internet shutdowns on broad grounds—remains unavailable to the public for consultation. As a result, civil society organizations, legal and constitutional experts, affected communities, industry representatives, technologists, academics, and other relevant stakeholders are unable to review these proposed ordinances or conduct human rights and economic impact assessments in a timely, informed, and effective manner.

AMBIGUOUS AND OVERBROAD PROVISIONS IN PROPOSED ORDINANCES THREATEN FUNDAMENTAL RIGHTS

Current drafts rely on undefined, ambiguous, and/or overbroad terms and provisions, which, without adequate procedural safeguards, pose significant risks of misinterpretation, overreach,

and abuse—particularly against marginalized communities, political dissidents, journalists, rights activists, and civil society organizations.

For instance, terms such as “obscene video” and “sexual harassment,” which carries a maximum sentence of three years’ imprisonment, remain undefined in CPO. Meanwhile, cyber terrorism is defined in overly expansive and vague terms, encompassing actions such as accessing or obstructing digital systems or infrastructure in ways that threaten national integrity, security, or sovereignty, instill public fear, are prejudicial to foreign relations, or benefit a foreign state or person, with penalties of up to ten years' imprisonment. Similarly, the term “classified personal data,” which is subject to cross-border transfer restrictions, remains undefined in PDPO.

Established constitutional doctrines require that laws affecting individual liberty and economic activities be reasonably certain and predictable, and ensure that statutory mandates are exercised within predefined limits in a fair, reasonable, non-discriminatory, and non-arbitrary manner, so that individuals have a clear legal standard against which they can assess their actions. Specifically, the *Siracusa Principles on the Limitation and Derogation of Rights* affirms that laws encroaching upon human rights must be clear and accessible, while *General Comment No. 34* states that laws “must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly … [and] may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution.” Similarly, *General Comment No. 35* confirms that non-arbitrariness includes elements of reasonableness, predictability, necessity, and proportionality. As such, we are concerned that the provisions risks violating protections under Articles 9(4) and 19(2) and (3) of the *International Covenant on Civil and Political Rights* (ICCPR), Article 19 and 29(2) of the *Universal Declaration of Human Rights* (UDHR), and Articles 26, 27, 31, and 39(2) of Bangladesh’s *Constitution*.

PRIVACY-VIOLATING PROVISIONS IN PROPOSED ORDINANCES EXACERBATES HUMAN RIGHTS CONCERNS

Current drafts contain multiple provisions that—coupled with unchecked surveillance, interception, and data disclosure authority conferred under BTRA and licensing frameworks for internet and telecommunication service providers—severely compromise citizens’ privacy rights. For instance, CPO allows police officers to intercept communications or obtain traffic data with a search warrant if they have “reasons to believe” that an offense has occurred, is occurring, or might occur. However, this vague and broad threshold increases the risks of subjective interpretation, abuse, and preemptive surveillance based on potential future offenses, ultimately undermining the balance between security and fundamental rights. Further exacerbating concerns, the law enforcement agencies have broad discretion to enter and search any location without a warrant based solely on suspicion that an offense—such as hacking or a cyber attack, both left undefined—has occurred, is occurring, or might occur, or if evidence is believed to be at risk of compromise. Additionally, individuals and entities are obligated to provide necessary assistance, including disclosing information, without clear safeguards to protect sensitive data or prevent government overreach.

Similarly, PDPO contains significant gaps in privacy protections, particularly through broad exemptions for law enforcement and intelligence agencies, effectively shielding state actors from accountability in data collection and handling. Such overriding exemption supersedes crucial data protection principles like purpose limitation, data minimization, and consent, allowing authorities to collect, process, and store personal data without restriction. With this systemic loophole, the PDPO risks institutionalizing state-sanctioned surveillance that has historically led to serious human rights abuses, including enforced disappearances and extrajudicial killings. Further, the proposed ordinance mandates the enrollment of all data

controllers and processors in a publicly accessible register containing details about their data collection and processing activities. While intended to strengthen transparency, this provision raises serious privacy and security concerns, particularly for entities handling sensitive user data, trade secrets, and confidential business operations, risking exposure to cyberattacks, espionage, and targeted harassment, especially against the backdrop of digital threats faced by journalists, activists, and human rights defenders.

We are concerned that, among others, these provisions can lead to mass surveillance and breach of individual privacy under Article 17 of the ICCPR, Article 12 of the UDHR, and Article 43 of Bangladesh's *Constitution*.

FRAGMENTED REFORM INITIATIVES UNDERMINE HOLISTIC APPROACH TO DIGITAL GOVERNANCE

While attention has been directed toward cybersecurity and data protection, we remain concerned that the approach to reforming digital governance policies and laws are narrow, piecemeal, and fragmented. Proposed changes to these highly complex legislations are stopgap measures and issue-specific solutions, and fail to address root causes of digital abuse and cyber security threats.

For instance, the *Children Act, 2013*, the *Prevention of Women and Children Repression Act, 2000*, and the *Pornography Control Act, 2012* focus on protections against disproportionate abuse faced by women and children, however, lack robust provisions and enforcement mechanisms to combat child sexual abuse materials and technology-facilitated gender-based violence. Although increased penalties are introduced under CPO for certain offenses against children and women, its weak enforcement mechanisms and extraterritorial limitations significantly restrict its effectiveness, particularly in addressing violations on offshore online platforms. Instead of introducing a new legislation, the Interim Government of Bangladesh is better positioned to introduce amendments in the aforementioned laws to include digital threats and ensure women and children have access to meaningful remedy against online harms.

By continuing to focus on isolated regulatory fixes rather than adopting comprehensive, market- and sector-wide strategies, the government risks entrenching structural deficiencies and a fragmented and ineffective legal framework that cannot keep pace with the rapid evolution of digital markets and services.

RECOMMENDATIONS

We, the undersigned organizations, urge the Interim Government of Bangladesh to reassess its approach to digital governance reforms to ensure that ordinances are rights-based, citizen-centric, forward-looking, and developed through transparent, inclusive, and evidence-based policymaking approaches. Under Article 93(1) of Bangladesh's *Constitution*, the Interim Government of Bangladesh is responsible for ensuring these ordinances remain within the lawful scope of parliamentary statutes and safeguard fundamental rights. Specifically, we recommend:

- Prioritize repealing *CSA*, in line with the stated intention of the Interim Government of Bangladesh, and follow through with its commitment to withdraw all politically motivated and other malicious cases filed under this law and its predecessors, *DSA* and section 57 of the *Information and Communication Technology Act, 2006*.

- Adopt a narrowly focused ordinance to address cybersecurity risks, while establishing a consultation roadmap to mitigate multifaceted and complex digital threats, including online safety and data protection.

- Establish stronger procedural safeguards under BTRA and the *Code of Criminal Procedure, 1898* against overreach and abuse by introducing clear legal limitations on law enforcement and intelligence agencies' ability to surveil, intercept, and access data.

- Ensure transparency and inclusive consultation in the law-making process by publishing draft laws and amendments with significant advance notice for meaningful public consultation, establishing a robust feedback mechanism to incorporate diverse stakeholder inputs, and disclosing the rationale for changes across multiple consultation drafts.

- Align all reform initiatives with international human rights standards, and to ensure any restrictions on freedom of expression, press, and privacy are rigorously assessed against standards under the ICCPR, UDHR, and Bangladesh's *Constitution*. Specifically, we recommend clearly defining legal terms, removing vague and overbroad provisions, and committing to periodic reviews and independent impact assessments to align with fundamental rights protections, and are prevented from being abused.

- Adopt a holistic and coherent approach to digital governance to address deeper structural deficiencies by moving beyond isolated, issue-specific regulations to establish comprehensive frameworks covering competition, consumer protection, online safety, platform liability, intellectual property rights, privacy, data protection, cross-border data flows, and the regulation of emerging technologies, ensuring a balanced, rights-respecting, and pro-innovation environment that safeguards citizens while enabling responsible corporate operations.

- Ensure that bodies operating under these laws, such as the Cyber Security Agency, the Bangladesh Data Protection Board, and the Bangladesh Telecommunication Regulatory Commission, function independently and are subject to robust oversight. Their actions should be publicly accountable, and decisions—particularly those affecting citizens' rights—must be subject to independent review.

ENDORSED AND SIGNED BY

Access Now

ARTICLE 19

Human Rights Watch

PEN International

Robert F. Kennedy Human Rights

Tech Global Institute