Submission #1: Survey of recent trends in surveillance technologies' legislative and regulatory measures, and the associated impacts on HRDs in the Global South

March 31, 2026

I. Introduction

1. Human Rights Journalists Network Nigeria, Institute for Policy Research and Advocacy (ELSAM), International Center for Not-for-Profit Law (ICNL), Professor Jane Duncan, Emmanuel Magambo, Red en Defensa de los Derechos Digitales (R3D), Talal Raza (University of Melbourne), 0xche, and the University of California, Irvine School of Law International Justice Clinic jointly submit this report in response to the Office of the High Commissioner for Human Rights's call for input as part of its mandate set by Human Rights Council's Resolution 58/23. Our knowledge and expertise span globally, including countries in Africa, Central America, South Asia, and Southeast Asia. You can find the details for each of us in ***Attachment 1***.
2. Our contribution consists of two submissions. This submission (**#1**) aims to answer your question "What impacts have recent trends in legislative and regulatory efforts at local, regional and global levels – including but not limited to information integrity, online safety and cybercrime – had on the work and safety of human rights defenders (HRDs) in the digital age?" As we detail below, one trend involves states delaying regulation or failing to control states' use of advanced surveillance technologies, which creates opportunities for technology abuse. On the other hand, through legislation, other states are actively legitimizing surveillance power against HRDs or preventing HRDs from protecting themselves from surveillance.[1] All footnotes of this submission are listed in ***Attachment 3***.

II. Lack of legislation as a pathway to states' abuse of advanced technologies against HRDs in the Global South

3. The persistent lack of domestic legislative measures to control law enforcement acquisition and use of technologies creates a vacuum for states themselves to deploy such technologies to restrict rights; this vacuum is exacerbated by the rapid advancement of technologies that outpace legislative, or any other, countermeasures. HRDs in the Global South report that few, if any, limits exist: states do not have transparent investigation processes, no requirements for ex-ante judicial authorization, and no effective independent oversight bodies. As such, tools, often enabled with artificial intelligence (AI), are used for extralegal targeted surveillance, unrestrained mass surveillance, and censorship based on vague provisions prohibiting content and smear campaigns that ultimately disproportionately target HRDs.
4. In general, the legality of unconstrained mass surveillance sits in a gray area of international human rights law. The right to privacy rests on the underlying premise that individuals have a "private sphere" where they can interact free from state intervention. However, new technologies have upended traditional conceptions of the "private sphere" (A/HRC/23/40), and the UN Human Rights Committee has not revisited the right to privacy since 1988. The UN High Commissioner for Human Rights has argued that limitations on public surveillance[2] are necessary because constant surveillance has "considerable chilling effects on how people exercise their rights" and could be abused to target and harass political critics, marginalized communities, and organizers of peaceful protests. Without safeguards and rigorous oversight, there is a risk that social media monitoring tools, public CCTV cameras enabled with facial recognition tools, and tools that track location and other traffic data could be used to monitor HRDs, peaceful protesters, and media outlets. Already, there are documentation of many incidents of such abuses around the world, from law enforcement tracking Black Lives Matter protests in the United States[3] to the government issuing misdemeanor violations to protesters[4] through the mail following protests in Serbia.

5. In Morocco, Amnesty International Security Lab investigations from 2021 and 2022 revealed several Moroccan HRDs were targeted with spyware developed by the Israeli company NSO Group.[5] Among those targeted included Moroccan journalist Hicham Mansouri as well as activist Aminatou Haidar, from Morocco's Western Sahara. There is no legal basis in Morocco to use spyware, and the Moroccan government has repeatedly denied its culpability, even threatening to take legal action against the "false accusations."[6] In Guatalema, HRDs, indigenous leaders, and climate activists have long been targeted with smear campaigns[7] over social media, but the attacks have increased with the advent of new technologies and the general state of impunity for engaging in such tactics. According to a report by Global Witness, the attacks also worsened when X cut funding for fact checking across the platform.
6. In Indonesia, despite the adoption of a revised Code of Criminal Procedure (KUHAP) in 2026, Indonesia still has a near-total absence of meaningful legal oversight governing the acquisition and deployment of surveillance technologies. Institute for Policy Research and Advocacy (ELSAM)'s ongoing research reveals Indonesia has no unified legal framework regulating the use of interception capabilities, no requirement for judicial authorization before deployment, and no independent oversight body with the mandate and capacity to monitor how these tools are used. Consequently, historical evidence of spyware deployment includes a civil litigation suit in 2019 filed by WhatsApp against NSO Group, which revealed at least 54 Indonesian telephone numbers were infected during a Pegasus spyware attack in 2018. Research also suggests Indonesia's government deployed surveillance technologies, including commercial spyware, on a significant scale during a mass protest movement, one of the most significant episodes of public mobilization in recent Indonesian history, that emerged in August 2025. We provide ELSAM's full contribution in ***Attachment 2 of Submission #2***.
7. Uganda's absence of clear legal authority and oversight mechanisms has resulted in more than a decade's worth of well-documented surveillance campaigns. This includes the Ugandan government's alleged use of FinFisher, spyware developed by Gamma Group.[8] During the 2012 Walk-to-Work protests, a surveillance initiative referred to as the Fungua Macho project reportedly employed FinFisher to monitor communications of opposition politicians, journalists, and other individuals critical of the government. This operation allegedly involved the installation of monitoring systems and fake wireless networks in hotels and other locations to intercept internet traffic and compromise devices connected to those networks. Findings suggest that such surveillance activities were conducted without transparent authorization processes, judicial warrants, or independent oversight, raising significant concerns regarding legality, accountability, and compliance with human rights standards. More recent examples include attempted spyware attacks in 2021 on personnel at the United States Embassy in Kampala, Uganda via iPhones as well as recent reports of potential surveillance campaigns ahead of the Ugandan 2026 General Election.[9] We attach Emmanuel Magambo's full contribution (regarding Uganda) in ***Attachment 4 of Submission #2***.

III. New legislation securing online safety as smokescreen for states' surveillance expansion

8. Even in countries with legislative response to emerging surveillance technologies, the creation of new legislation to ostensibly curb digital threats instead justifies states' continued abuse of surveillance against HRDs. Such legislation either penalizes digital crimes directly (while using vague language and definitions in order to sanction a variety of supposed violations) or empowers state and law enforcement agencies with vast powers to enact online safety goals, ultimately leading to widespread surveillance.
9. In Nigeria, the Cybercrimes (Prohibition, Prevention Etc.) (Amendment) Act 2024 expanded surveillance powers to the Nation Security Adviser (NSA) and established a sectoral Computer Emergency Response Teams (CERT) and Security Operation Centres (SOCs).[10] Despite these developments, Human Rights Journalists Network Nigeria highlights a potentially positive shift with the Human Rights Defenders

Protection Bill (HB 1867) proposed in 2024. The bill aims to establish a formal protection mechanism under the National Human Rights Commission (NHRC) to protect activists, journalists, and whistleblowers from security risks and guarantees the right to form associations, receive funding, seek information, and communicate with national and international bodies. While the Minister of Justice and Attorney General of the Federation expressed rejection of the proposal, the Parliamentary deliberation is ongoing.

10. In Angola, National Security Law (2024)[11] outlines national security structures and provides wide-ranging powers to the President and national security institutions to restrict rights to protect national sovereignty, territorial integrity, social development, economic development, and national cohesion, among others. The law provides overbroad powers to these institutions to prevent protests and undertake.
11. In Mozambique, Telecommunications Traffic Control Regulation (Decree 48/2025) authorizes the telecommunications regulator to block telecommunications traffic in cases of criminal activity and threats to state security or public order, raising concerns that it could enable internet shutdowns, unlawful surveillance, and violations of freedom of expression.
12. In Pakistan, a 2024 court case (which involved alleged leaked audio recordings of politicians) revealed that Pakistan's authorities and local telecommunications companies had installed a lawful interception system, enabling them to surveil four million people without any clear legal authority.[12] Separately, six judges of the Islamabad High Court approached the Supreme Court Chief Justice, accusing intelligence agencies of surveilling and intimidating them.[13] Their complaints did not trigger a full-fledged inquiry, and further, the Prime Minister issued an executive order a few months later, allocating broad surveillance powers to intelligence authorities under Section 54 of the Pakistan Telecommunication (Re-organization) Act, 1996.[14]
13. In Mexico, a series of new legislation in recent years has granted the Mexican government with expanded surveillance powers while abolishing institutional safeguards. In December 2024, a constitutional amendment dismantled the autonomous body responsible for personal data protection and transparency, the National Institute of Access to Information and Protection of Personal Data (INAI). In July 2025, the Mexican government also fast-tracked a series of laws through the nation's congress to establish an uncontrolled system of massive surveillance and social control that is incompatible with the rights to privacy, data protection, freedom of expression, presumption of innocence, non-discrimination, and the principle of non-incrimination of the whole population. All information related to this intelligence system will be confidential and reserved, and criminal sanctions can even be imposed on those sharing it, overcoming constitutional principles such as public interest, transparency, accountability, and publicity. We provide R3D's full contribution in ***Attachment 2.***
14. Vague language and definitions in new legislation give states legal justification and leeway to abuse surveillance technologies at large. For example, in Ethiopia's Hate Speech and Disinformation Prevention and Suppression Proclamation 1185/2020, "disinformation" and "social media" are broadly defined, with the latter defined as creating and sharing information with more than one person.[15] Anyone with a social media following of more than 5,000 people who disseminates "hate speech" or "disinformation" is subject to simple imprisonment of up to 3 years; if "disturbance or violence" arises, the penalty increases to imprisonment of five years.[16] In Kyrgyzstan, recent amendments to the state's Code of Offenses imposed heavy fines for individuals ($230 USD) and legal entities ($740 USD) found guilty of spreading inaccurate or misleading information through the media or social networks.[17] The amendments are the latest crackdown in a series of other legislation, including a 2021 bill that vaguely defined "inaccurate information," which has since resulted in arbitrary enforcement for alleged violations, targeting journalists, activists, and social media users who criticize public officials or discuss sensitive issues.[18]
15. Another trend is as online safety legislation with insufficient safeguards are created in the Global North, some Global South countries that have less effective institutional checks and balances are imitating such laws, thus exposing HRDs in the Global South to further oppression. Recent legislation in Australia and the United Kingdom, seeking to regulate how children access the internet, raises possibilities that states or non-state

actors could instead stifle the rights of youth HRDs or exploit the vast amount of personal data garnered via the legislation.[19] Further, as similar laws are considered in other jurisdictions, HRDs in states imitating Australia and the United Kingdom's protocols could face greater danger due to weaker cybersecurity protocols or safeguards for how law enforcement seizes data from third party companies.

IV. New legislation as barriers to HRDs seeking countermeasures

16. HRDs in the Global South seeking to defend themselves from targeted surveillance are prevented from doing so in the face of new legislation prohibiting the use of common countermeasures, including legislation forbidding the use of VPNs, encryption tools, or lockdown mode on personal devices to protect against hacking by oppressive regimes. Moreover, states create new legislation that prevents HRDs from engaging in critical advocacy strategies[20] in the online realm, including digital fundraising.
17. Myanmar's military leaders have enacted a new cybersecurity law, Myanmar Cybersecurity Law (2025) that will provide the junta with extensive control over information access. The expansive law (comprising 16 chapters and 88 articles) regulates VPNs, which allow internet users to circumvent website blocks. The law also penalizes users who access or share media articles and information from banned websites.[21]
18. In Zambia, Cyber Crimes Act (2025) criminalizes certain types of online communication that "deceive or mislead" as to the origin of the communication. Authorities could use this vague provision to disproportionately restrict legitimate tools such as encryption or Virtual Private Networks (VPNs) that enable users to communicate anonymously and securely, which are important aspects of the ability to exercise the rights to freedom of expression and privacy online.[22]
19. In Pakistan, in November 2024, amid increasing concerns about the opposition use of social media to discredit the government and their inability to trace opposition aligned trolls, authorities tested a ban on VPNs using their newly acquired firewall.[23] To justify the test, in what seemed to be an attempt to build a rationale around VPN regulation, official statements started pouring in from different government bodies expressing concern on how VPNs were facilitating access to pornography as well as allowing terrorists to carry out their activities. While no formal ban was pursued eventually, it culminated in the government's official demand to all internet users to register VPNs with the government or risk losing access to it.
20. In Jordan, Cybercrime Law No. 17 (2023)[24] prevents HRDs from advocating in the digital realm and burdens potential HRDs by setting harsh punishment for broadly defined cybercrimes (e.g., vague cybercrime of "assassinating his/ her character"). The law restricts typical advocacy strategies such as digital fundraising and crowdfunding; freedom of association is also hampered by the law requiring social media platforms outside of Jordan that have more than 100,000 subscribers to establish an office within the country.[25] Further, the law places exacerbated prison sentences and fines for digital crimes, compared to non-digital crimes.

V. Recommendations

21. We suggest OHCHR to include the following recommendations in its report to the Human Rights Council. The Human Rights Council should urge states to:
    - condemn legislation or the absence of legislation that enables or facilitates the digital surveillance of HRDs;
    - adopt online safety legislation with stringent safeguards, recognizing that such laws are likely to be replicated in jurisdictions lacking effective oversight; and
    - adopt laws that enable and empower HRDs and civil society actors to protect themselves against digital surveillance and online attacks, and to document and counter such practices.

Attachment 1: Submitters' Information

Human Rights Journalists Network Nigeria is a registered NGO in Nigeria whose mission is to document, build capacity, and advance human rights in Nigeria and by extension the West African region through the West African Digital Rights Defenders Coalition.

Institute for Policy Research and Advocacy (ELSAM) is a human rights organization, which was established in Jakarta in August 1993. The aim is to participate in efforts to develop, promote and protect civil and political rights as well as other human rights in general – as mandated by the 1945 Constitution and the Universal Declaration of Human Rights. Since the beginning, the spirit of ELSAM's struggle has been to build a democratic political order in Indonesia through the empowerment of civil society through advocacy and promotion of human rights.

International Center for Not-for-Profit Law (ICNL) works globally to improve the legal environment for civil society, philanthropy, and public participation, both online and offline.

Professor Jane Duncan is a professor of Digital Society at the University of Glasgow. Her scholarship includes: *Abolishing dragnet surveillance: assessing the relevance of the movement to defund the police for bulk signals intelligence surveillance*;[1] *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa*;[2] and *The Rise of the Securocrats*.[3]

Emmanuel Magambo is IT and Cybersecurity Specialist supporting NGOs, media organizations, and human rights defenders in Uganda. My work strengthens secure, rights-respecting online spaces and helps organizations operate safely in high-risk, surveillance-prone environments.

Red en Defensa de los Derechos Digitales (R3D) is a non-governmental, non-profit organization located in Mexico, dedicated to the defence of human rights in the digital environment.

Talal Raza is a PhD Candidate at the University of Melbourne's School of Social and Political Sciences. His research interests are digital development, digital rights and digital politics.

0xche is a horizontal and self-organized collective of technologists committed to strengthening the information security of activist organizations and civil society in Latin America.

International Justice Clinic of the University of California, Irvine School of Law, produces research and conducts advocacy promoting compliance with international human rights law and, inter alia, United Nations human rights mechanisms. The Clinic's areas of focus include digital surveillance.

[1] Jane Duncan, *Abolishing Dragnet Surveillance: Assessing the Relevance of the Movement to Defund the Police for Bulk Signals Intelligence Surveillance*, King's L.J. (published online Sept. 15, 2025).
[2] Jane Duncan, *Stopping the Spies: Constructing and Resisting the Surveillance State in South Africa* (2018).
[3] Jane Duncan, *The Rise of the Securocrats: The Case of South Africa* (2014).

Attachment 2: Contribution of Red en Defensa de los Derechos Digitales (R3D)

In December 2024, a constitutional amendment in Mexico disestablished the autonomous body responsible for personal data protection and transparency, the National Institute of Access to Information and Protection of Personal Data (INAI).

Reforms in March 2025 to Data Protection Laws[4]: **(i)** eliminate the powers of transparency authorities[5] to bring actions of unconstitutionality against legislation or executive acts, as well as criteria that strengthened transparency, maximum publicity, and the right of access to information; **(ii)** include vague concepts to restrict access to information of public interest, such as "social peace" and "damage to the interests of the State"; and, **(iii)** create a decentralized body called "Transparency for the People" that lacks autonomy and eliminate requirements that affect the impartiality and professionalization of transparency authorities.

In July 2025, the Mexican government also fast-tracked a series of laws in the Congress to establish an uncontrolled system of massive surveillance and social control that is incompatible with the rights to privacy, data protection, freedom of expression, presumption of innocence, non-discrimination, and the principle of non-incrimination of the whole population.

These reforms represent a serious setback and contravene the international human rights obligations of Mexico including under the ICCPR. Laws on Telecommunications and Broadcasting[6], Public Security[7], Investigation and Intelligence[8], General Population[9], Enforced Disappearances[10], and the National Guard[11], establish a permissive architecture for state surveillance without safeguards for the protection of human rights.

As a corollary, all information related to this intelligence system will be confidential and reserved, and criminal sanctions can even be imposed on those sharing it (Articles 1, 51 & 55), overcoming constitutional principles such as public interest, transparency, accountability, and publicity.

The consolidation of unchecked surveillance powers for authorities—especially armed forces—, the weakening of oversight mechanisms, and the establishment of a system that can constantly monitor society through the requirements of mandatory centralized and massive databases of personal data are a serious violation of the right to privacy and will have a chilling effect on other human rights, especially those of HRDs, such as freedom of expression, assembly and association.

This is particularly relevant considering that, since 2017 –through investigations such as "Gobierno Espía"[12] (Spying government) and "Ejército Espía" (Spying Army)[13], along with investigative journalism[14] and reports from Citizen

[4] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados and Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
[5] Of 33 agencies: 32 state level institutes and INAI at the national level. These agencies were responsible for ensuring access to public information and protection of personal data and acted as mediators when authorities failed to comply with their obligations.
[6] Ley en Materia de Telecomunicaciones y Radiodifusión, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LMTR.pdf
[7] Ley General del Sistema Nacional de Seguridad Pública, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf
[8] Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LSNIIMSP.pdf
[9] Ley General de Población, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LGP.pdf
[10] Ley General en Materia de Desaparición Forzada de Personas, Desaparición Cometida por Particulares y del Sistema Nacional de Búsqueda de Personas, available at https://www.diputados.gob.mx/LeyesBiblio/ref/lgmdfp.htm
[11] Ley de la Guardia Nacional, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LGN.pdf
[12] ARTICLE 19, R3D: Red en Defensa de los Derechos Digitales, Social Tic, *Gobierno Espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México* (Spying Government. Systemic surveillance of jorunalists and human right defenders in Mexico), June 2017, https://r3d.mx/wp-content/uploads/GOBIERNO-ESPIA-2017.pdf
[13] *See*, R3D: Red en Defensa de los Derechos Digitales, "Ejército Espía", available at: https://ejercitoespia.r3d.mx/ejercito-espia/
[14] **National:** "Pegasus Project | Familiares de los 43 normalistas de Ayotzinapa, en la lista de objetivos de espionaje con Pegasus", *Aristegui Noticias*, Julyu 18, 2021, disponible en: https://aristeguinoticias.com/1807/mexico/pegasus-project-familiares-de-los-43-normalistas-de-ayotzinapa-en-la-lista-de-objetivos-del-programa-de-espionaje-pegasus/; and Tourliere, Mathieu, "Peña Nieto, el desenfrenado espionaje contra periodistas", *Proceso*, November 15, 2023, available at: https://www.proceso.com.mx/nacional/2021/7/18/pena-nieto-el-desenfrenado-espionaje-contra-periodistas-268034.html

Lab[15] – more than 25 surveillance cases against HRDs in Mexico have been documented.[16] In all of the cases, a correlation has been found between HRDs denouncing acts of corruption and violations of human rights –such as enforced disappearances and extrajudicial killings committed by the Army– and their surveillance.

Up to now, the victims of surveillance documented under MORENA's administration are the Under-Secretary for Human Rights, Alejandro Encinas[17], the Coordinator of the Truth Commission for the "Dirty War" ─the period of enforced disappearances, torture and executions committed by Mexican security forces, including the army, from the 1960s to the 1980s─, Camilo Vicente Ovalle[18], a human rights organization, Miguel Agustín Pro Juárez Human Rights centre (Centro Prodh), human rights defender Raymundo Ramos, and two journalists, one of them Ricardo Raphael de la Madrid. The Pegasus infections occurred at times when the victims were carrying out work related to human rights violations committed by the Armed Forces.

For example, Under-Secretary Encinas was in charge of the truth commission for the disappearance of 43 students from Ayotzinapa, in which army personnel participated. Centro Prodh represents the families of the victims in said case and represents many other victims of military abuses. Centro Prodh had also been previously found to be targeted with Pegasus in the previous government.[19] Also, the journalists were attacked when they were publishing information related to human rights abuses committed by the military.[20]

International: Priest, Dana, et. al., "Private Israeli spyware used to hack cellphones of journalists, activists worldwide", *The Washington Post*, July 18, 2021, available at: https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/?itid=hp-top-table-main; and Kirchgaessner, Stephanie, et. al., "Revealed: leak uncovers global abuse of cyber-surveillance weapon", *The Guardian*, July 18, 2021, available at: https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

[15] Scott-Railton, J., et al., Report: "Bitter Sweet Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links", *The Citizen Lab*, February 11, 2017, available at: https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/

[16] Scott-Railton, J., et al., Report: "Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware", *The Citizen Lab*, March 20, 2019, available at: https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/

[17] Kitroeff, Natalie & R. Bergman, "Mexican President Said He Told Ally Not to Worry About Being Spied On", The New York Times, May 23, 2023, available at: https://www.nytimes.com/2023/05/23/world/americas/mexico-president-spying-pegasus.

[18] Lopez, Oscar & M. Sheridan, "He's leading Mexico's probe of the Dirty War. Who's spying on him?". The Washington Post, June 3, 2023, available at: https://www.washingtonpost.com/world/2023/06/03/mexico-pegasus-dirty-war-lopez-obrador/

[19] Scott-Railton, J., et al., Report: "Reckless Exploit, Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware", The Citizen Lab, June 19, 2017, available at: https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

[20] Bill Marczak, et al., "Triple Threat NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains", April 18, 2023, available at: citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/

Attachment 3: Footnotes

[1] In accordance with the OHCHR's definition, we understand the term "Human Rights Defender" includes those who make "special efforts" to protect or advocate for human rights, including immigration lawyers, community organizers, or journalists. [https://www.ohchr.org/en/special-procedures/sr-human-rights-defenders/about-human-rights-defenders]

[2] See OHCHR 2022 report, "The right to privacy in the digital age" [https://docs.un.org/en/A/HRC/51/17]

[3]See ICNL 2023 article, "Protesting in an Age of Government Surveillance Legal Reforms to Protect Demonstrators in the United States" [https://www.icnl.org/post/analysis/protesting-in-an-age-of-government-surveillance]

[4] See Radio Free Europe/Radio Liberty 2022 article, "Serbia's Legal Tug-Of-War Over Chinese Surveillance Technology (Part 2)" [https://www.rferl.org/a/serbia-chinese-surveilllance-backlash-standish/32145138.html]

[5] See Amnesty International 2022 article, "Morocco/Western Sahara: Activist targeted with Pegasus spyware in recent months – new evidence" [https://www.amnesty.org/en/latest/news/2022/03/morocco-western-sahara-activist-nso-pegasus/]

[6] See France 24 article in 2021, "Morocco threatens legal action over 'unfounded' spyware allegations" [https://www.france24.com/en/africa/20210722-morocco-threatens-legal-action-over-unfounded-spyware-allegations]

[7] See Global Witness 2026 article, "Weaponising social media: How Indigenous leaders and climate activists are smeared and criminalised in Guatemala" [https://globalwitness.org/en/campaigns/land-and-environmental-defenders/weaponising-social-media-how-indigenous-leaders-and-climate-activists-are-smeared-and-criminalised-in-guatemala/]

[8]See Privacy International 2025 report, "For God and My President: State Surveillance In Uganda" [https://www.privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1.pdf]

[9] See Submission #2, Paragraph 6.

[10] According to Human Rights Journalists Network Nigeria, another piece of new legislation is the Code of Practice for Platform Intermediaries (2022). The Code requires all "interactive computer service platforms" to respond to government orders to take down prohibited and illegal content posted by users, raising concerns about the risks of abuse. For platforms that have over 100,000 users in Nigeria, there are additional registration and reporting requirements. Part V of the Code has specific measures in place to address dis/misinformation, including takedown requirements.

[11] See Human Rights Watch 2024 article, "Angola: President Signs Laws Curtailing Speech, Association" [https://www.hrw.org/news/2024/09/10/angola-president-signs-laws-curtailing-speech-association]

[12] See Amnesty International 2025 report, "Pakistan: Shadows of Control: Censorship and mass surveillance in Pakistan" [https://www.amnesty.org/en/documents/asa33/0206/2025/en/]

[13] See Al Jazeera 2024 article, "Judges vs spies: Pakistan's jurists accuse intel agency ISI of intimidation" [https://www.aljazeera.com/news/2024/3/27/judges-vs-spies-pakistans-jurists-accuse-intel-agency-isi-of-intimidation]

[14] See Dawn 2024 article, "Govt formally authorises ISI to 'trace, intercept' calls and messages in 'interest of national security'" [https://www.dawn.com/news/1844810]

[15] See Human Rights Watch 2025 article, "Ethiopia: Surge in Arrests of Journalists, Media Workers" [https://www.hrw.org/news/2025/09/22/ethiopia-surge-in-arrests-of-journalists-media-workers]

[16] See full legislative text provided by Access Now: [https://www.accessnow.org/wp-content/uploads/2020/05/Hate-Speech-and-Disinformation-Prevention-and-Suppression-Proclamation.pdf]

[17] See Committee to Protect Journalists (CPJ) 2025 article, "Kyrgyzstan tightens control over media with new false news laws" [https://cpj.org/2025/07/kyrgyzstan-tightens-control-over-media-with-new-false-news-laws/]

[18] See Committee to Protect Journalists (CPJ) 2021 article, "Kyrgyzstan parliament approves 'false information' bill" [https://cpj.org/2021/08/kyrgyzstan-parliament-approves-false-information-bill/]

[19] See, for example, EDRi 2025 statement "Age verification gains traction: the EU risks failing to address the root causes of online harm" [https://edri.org/our-work/age-verification-gains-traction-eu-risks-failing-to-address-the-root-causes-of-online-harm/]

[20] See Paragraph 22 of this submission.

[21] See Human Rights Watch 2026 report on Myanmar [https://www.hrw.org/world-report/2026/country-chapters/myanmar] and legislative text provided by The International Center for Not-for-Profit Law (ICNL) [https://www.icnl.org/wp-content/uploads/2025-version-Lincoln.pdf]

[22] See ICNL 2025 Report, "Five Things to Know: Zambia's Cyber Crimes Act and Cyber Security Act" [https://www.icnl.org/post/tools/five-things-to-know-zambias-cyber-crimes-act-and-cyber-security-act]

[23] When the move completely disrupted access to VPNs and led to increasing questions from users, authorities had to officially confirm later that they had briefly banned VPNs as part of their trial run.

[24] See Amnesty International 2024 article, "Jordan: New Cybercrimes Law stifling freedom of expression one year on" [https://www.amnesty.org/en/latest/news/2024/08/jordan-new-cybercrimes-law-stifling-freedom-of-expression-one-year-on/]

[25] See Access Now 2023 press release, "Jordan's new proposed cybercrimes law will strongly undermine digital rights" [https://www.accessnow.org/press-release/jordans-cybercrimes-law/]