Submission #2: Examining the current proliferation of surveillance, with a focus on Human Rights Defenders' lived experiences and resistance strategies in Global South countries

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 the 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 (**#2**) aims to answer your question, "What risks have emerged for HRDs[1] with the increasing procurement, use and abuse of digital surveillance tools, including spyware and interception technologies, by State and non-State actors?" All footnotes of this submission are listed in ***Attachment 5***.

II. Current proliferation of targeted surveillance technologies in the Global South

3. The proliferation of surveillance technologies, including targeted and mass surveillance, in the Global South is a persistent yearslong trend. State actors often capitalize on elections, protests, or other forms of civic engagement as justification to procure and deploy new surveillance measures.[2] Institutional surveillance oversight is historically nonexistent, limited, or ineffective, and rapid growth in the capacity of advanced technologies well outpaces that of any oversight mechanisms.[3] The sophistication, secrecy, and technical complexity of technologies further compounds the oversight gaps.[4] Consequently, digital technologies are abused against many HRDs in the Global South, compounding the physical and psychological harm risks they already face.
4. *Targeted surveillance through spyware or other technologies*: Mexico was one of the first countries whose government procured and used NSO Group's Pegasus spyware in 2011.[5] In Africa, the Ethiopian government procured FinFisher spyware as far back as 2013,[6] and reports suggest many more governments in the region including those in Ghana, Kenya, Morocco, Nigeria, and Zambia have procured and used spyware since then. Between 2015 and 2025, the Bangladeshi government spent approximately USD $190 million to acquire 160 types of digital surveillance technologies, including spyware.[7] The Indonesian government also has a long history of procuring spyware from Gamma TSE Ltd, Candiru, the Polus Group, and the NSO Group. The Indonesian government's budget allocations for surveillance technology, including spyware, across relevant state institutions reach approximately 36 trillion Indonesian Rupiah, equivalent to roughly USD 2.2 billion. Institute for Policy Research and Advocacy (ELSAM)'s research suggests the involvement of members of Indonesia's national legislature, including the House of Representatives (Dewan Perwakilan Rakyat / DPR RI), as intermediaries or middlemen in the procurement of spyware, indicating profound conflicts of interest. We provide the full contribution of ELSAM in ***Attachment 2***.
5. *Mass collection of biometric data:* States have normalized the mass collection of biometric data, with Mexico as a recent notable example. Mexico's latest relevant legislation includes the General Population Act, which requires every person in Mexico to have a mandatory biometric ID. Further, the Disappeared Persons Act (General Law on Matters of Disappeared Persons, Disappearances by Private Entities, and the National System of Searching for Persons) creates the "Unique Identity Platform", which will collect and consolidate all

information generated by the use of the biometric ID (Article 12), as outlined in the General Population Act. Since every daily activity will require a biometric ID, all activities will be collected on this platform. Public and private entities are obliged to record any transaction and access to services (Articles 91 BIS & 91 Sexies).[8] We provide the full contribution of R3D in ***Attachment 3***.

6. *AI-powered surveillance tools*: Law enforcement agencies in the Global South are rapidly procuring and using new surveillance technologies with artificial intelligence (AI) systems.[9] Civil society organizations have expressed concern that such technologies could disproportionately target HRDs. For example, recent reports indicate that Uganda is planning to expand AI-powered online monitoring ahead of its 2026 General Election, to monitor social media, track conversations, analyze sentiments, and geolocate users. In Nepal, law enforcement agencies have recently launched an AI cell to surveil activity on social media in a purported effort to monitor disinformation and election-related "fake news."[10] Reliance on AI-powered surveillance tools poses multiple dangers. In addition to the biases these tools carry and the potential for hallucinations,[11] state actors justify the use of AI to carry out mass data collections, suggesting that AI can extract meaningful insights from vast amounts of data that would be impossible to analyze manually. The black-box nature of AI-powered surveillance tools also adds significant hurdles to accountability. We attach the full contribution of Emmanuel Magambo (regarding Uganda) in ***Attachment 4.***
7. Surveillance technologies are often supplied by vendors headquartered outside the countries where they are deployed. Most of these are companies based in the U.S., Europe, Israel, China, Japan, and elsewhere. This creates additional challenges for civil society actors attempting to track procurement and use. For example, recent investigations exposed Geedge Networks's role in selling its product Tiangou Secure Gateway (TSG) to countries in the Global South. Geedge Networks is a Chinese company that has architected China's censorship apparatus.[12] The suite of tools has many features,[13] including the use of deep packet inspection[14] to automatically identify, classify, and censor content, block the use of virtual private networks, and throttle traffic. Leaked documents show that Geedge has sold TSG to Ethiopia, Pakistan, and Myanmar, countries that already had well-known records of human rights violations, online censorship, and disproportionate surveillance prior to their dealings with Geedge.

III. Human Rights Defenders' lived experiences as a result of targeted surveillance

8. HRDs in many countries in the Global South historically and currently endure physical and psychological assault, forced disappearances and deaths due to surveillance. Data from R3D Mexico finds more than 25 documented cases of surveillance abuse against HRDs in Mexico since 2017 — a number that is likely an underestimate. Some of these cases resulted in disappearances and murders stemming from HRDs' public denouncement of corruption and human rights violations,[15] including the murders of Mexican journalists Cecilio Pineda Brito and Fredid Román, who died in 2017 and 2022 respectively, after targeted surveillance attacks involving spyware.
9. HRDs who do not experience physical harm or death as a result of confirmed targeted surveillance still endure detrimental psychological harm as a result of yearslong surveillance. HRDs often remain uncertain as to whether they are under surveillance or where surveillance attacks originate, further contributing to negative, long-term effects on HRDs' mental health. Salvadoran journalist Julia Gavarrete explained in an October 2025 interview[16] that "knowing who was responsible for targeting her and what happened to the data they accessed remains central to her vision of justice. 'It's the minimum that you want, and then after all of that, maybe you can expect many other things.'" Angolan journalist and lawyer Teixeira Cândido explained in a February 2026 interview[17] that his first brush with digital surveillance occurred around Angola's 2022 national elections in the form of burglaries at his workplace, the Syndicate of Angolan Journalists, which he led until 2024. Cândido recounted his experiences: "I literally felt naked… You don't know if you're being watched, if you're being followed… Despite all the security measures you can take, there's always a feeling of insecurity that doesn't go away."

10. Physical and psychological harm caused by targeted surveillance results in professional repercussions, hampering HRDs' ability to successfully engage in advocacy, and, in some cases, ending HRDs' careers entirely. Former newspaper editor Spencer Mogapi, based in Botswana, described how police accessed his phone communications, an event that led to his eventual departure from journalism for a public relations career.[18] In an October 2025 interview, Mogapi illustrated the deterioration of his relationship with sources, who feared exposure and retaliation from state actors: "People who would regularly reach out would get fearful." Additionally, an anonymous Pakistani journalist who was attacked by spyware said in a 2025 Amnesty International article[19] that one of his sources endured a week-long interrogation in a forced disappearance, in connection to a story the journalist produced, which then resulted in increased hesitation from sources.
11. In addition to professional repercussions, HRDs experiencing targeted surveillance are forced to change their behavior out of caution with loved ones, who themselves face increased risk of surveillance. In a 2025 Amnesty International article, an anonymous Pakistani journalist reported that his extended family members had bank accounts closed, including a sister-in-law's pension, to prevent the journalist from receiving financial help.[20] This targeted campaign forced him and his wife to cut contact with loved ones.
12. Importantly, HRDs affected are not limited to those confirmed as targets. Due to the extreme secrecy and technicality surrounding spyware operations and the requirement for specialized forensic analysis to confirm infection —which many HRDs in the Global South may lack access to or awareness of— the mere possibility that a government could deploy spyware against them significantly impacts HRDs' work, private lives, and psychological status.

IV. HRDs' countermeasures and resistance against surveillance, and resources needed

13. HRDs in many countries in the Global South are engaging in "public oversight" alongside journalists, technical experts, lawyers, other experts, and civil society at large in direct response to ineffective institutional oversight not expected to detect or remediate abuse.[21] According to the "Democratizing Spy Watching" project co-produced by Professor Jane Duncan, "public oversight" refers to an agential approach in which civil society actors, in contrast to government institutions, take the lead in investigating and holding such abuses to account.[22]
14. Mounting challenges remain for HRDs engaging in "public oversight" as investigations and advocacy face a combination of hurdles, including extreme secrecy in the procurement and deployment of surveillance tools; public indifference to the harms of digital surveillance (partly stemming from language barriers that limit access to existing reporting); limited access for HRDs to trusted forensic analysis capacity; limited mobilization capabilities of existing civil societies; and the severe chilling effects imposed on HRDs operating under governments with broad surveillance usage. Strengthening public oversight is not only an essential effort for Global South countries: such public oversight can support Global North countries, especially those where spyware vendors are based and have diplomatic leverages, pushing them to adopt evidence-based measures to sanction and regulate the commercial spyware industry. We therefore urge constituencies to support countries in the Global South in better meeting the conditions necessary to achieve effective public oversight.
15. The "Democratizing Spy Watching" project examines public oversight efforts on surveillance abuse in Southern African countries with various historical and political context. Successful public oversight efforts were documented in Mauritius.[23] In response to the government's attempt to introduce a centralized biometric national ID system (fingerprint and facial features), Mauritian HRDs successfully achieved mass mobilization through online petitions, social media awareness and public protest. In 2015, the Mauritian government proceeded with a form of identification in which the biometrics were stored on the card instead of through central biometric registration, while the Human Rights Committee ruled that the revised system still violates the right to privacy.[24]
16. In Mexico, spyware victims,[25] mainly HRDs, have investigated surveillance abuse and filed criminal complaints with the Special Prosecutor's Office for Crimes against Freedom of Expression (FEADLE), in collaboration with civil society organizations.[26] One such HRD, Centro Prodh, has been subject to surveillance under two different

political administrations and filed two different criminal complaints, revealing the lack of adequate measures that led to the repetition of illegal surveillance. However, in Mexico and elsewhere, relief through domestic litigation remains rare. R3D documented the continuous refusal from Mexican prosecutorial authorities to heed international calls for diligent investigations including calls from the OHCHR itself, as well as the Inter-American Commission on Human Rights (IACHR). These tactics include: placing the burden of proof on surveilled victims, denying copies of investigation files, and claiming no database or formal documentation of the records regarding the persons or numbers targeted exist. We provide the full contribution of R3D in ***Attachment 3***.

17. In Thailand, LGBTQ+ activists, in collaboration with Amnesty International Security Lab, confirmed spyware infections on their phones and subsequently engaged in advocacy via public campaigns; they also filed domestic litigation that Thai courts ultimately dismissed.[27] In Kenya, filmmakers engaged in public oversight by initiating an investigation, in collaboration with Citizen Lab, that used forensic analysis to confirm commercial spyware Flexispy was installed in their phones while they were in police custody.[28]
18. In addition to proactive countermeasures, HRDs engage in digital security tactics as critical defensive measures. An anonymous Pakistani journalist listed various strategies in an article, including communicating via encrypted platforms, avoiding the use of emails in case of potential tracking, and utilizing VPNs.[29] The journalist said: "You never know what kind of technology has been acquired by the state and what surveillance capabilities powerful institutions possess. This is not ideal of course, digital security precautions take up a chunk of my time—time I could be dedicating to my reporting." Notable factors that hinder the knowledge and capacity of HRDs include lack of materials written in their local languages, lack of accessible materials (written in excessively technical language), and lack of resources tailored to HRD's situations (for example, HRDs who work in rural areas or those who are forced to use more affordable but less secure devices). Further, the report "Exploring at-risk users' mental models of Apple Lockdown Mode in Latin America and the Caribbean" outlines, while Lockdown Mode can serve as a critical safety measure for HRDs to protect themselves from spyware threats, its adoption must be understood in a multilayered security strategy rooted and driven by interpersonal trust.[30]
19. Several core conditions are essential for generating public oversight of digital surveillance. These include: (i) a robust supply of information to support advocacy, particularly through journalists and human rights investigators; (ii) access for HRDs to trusted forensic analysis or other technical resources to confirm victimhood; and (iii) the ability of local journalists, NGOs, and activists to mobilize public participation while also understanding the technical dimensions of digital surveillance. Given the highly complex and transnational nature of the surveillance value chain, (iv) international collaboration is critical for both effective investigation and advocacy. Finally, (v) institutional conditions also matter, including the presence of an independent judiciary that enables litigation, as well as opportunities within parliamentary systems that can be leveraged to advance accountability, such as political divisions or broader democratic crises.

IV. Recommendations

20. We suggest OHCHR to include the following recommendations in its report to the Human Rights Council. The Human Rights Council should urge states to:
    - acknowledge the harm to HRDs caused by digital surveillance and stop procuring or using spyware or other digital surveillance technologies until effective oversight programs are in place;
    - Take steps to increase judicial and parliamentary oversight of these digital technologies, even when used to investigate heinous crimes;
    - regulate and sanction vendors of commercial spyware or other technologies that sell their products to governments lacking effective law and oversight program; and

- recognize the deficit in institutional oversight with respect to digital surveillance and create an environment where HRDs can take an agential approach to advancing public oversight through constraining digital surveillance through public mobilization, investigations, and litigation.

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 The Institute for Policy Research and Advocacy (ELSAM)

There are several international spyware companies whose products have been sold to Indonesian government entities. These include Gamma TSE Ltd, a UK-registered company known for its FinFisher (also known as FinSpy) surveillance suite; Candiru, an Israeli firm whose tools were documented in a landmark investigation by Citizen Lab and Microsoft; the Polus Group; and the NSO Group, the Israeli company behind the Pegasus spyware, arguably the most widely known commercial spyware product globally. These companies represent only a portion of a broader market; additional vendors are believed to have supplied technologies to Indonesian institutions.

The involvement of firms like NSO Group and Candiru is particularly significant given the extensive documentation of their products being misused in other countries. NSO Group's Pegasus spyware has been linked to the targeting of dissidents, journalists, and political opponents across numerous jurisdictions, and NSO Group itself has been placed on a trade restriction list by the United States Department of Commerce. The presence of such vendors in the Indonesian market raises acute concerns about the conditions under which these technologies are sold and whether end-use guarantees are in place or enforced.

Government budget allocations for surveillance technology across relevant Indonesian state institutions are estimated to reach approximately 36 trillion Indonesian Rupiah, equivalent to roughly USD 2.2 billion, underscoring the enormous scale of investment in digital surveillance capabilities. This figure, drawn from publicly available budget documents and procurement data, reflects spending across multiple institutional line items and may represent only a portion of the total outlay, given that certain procurement processes occur through opaque or off-budget mechanisms.

The agencies identified as users of commercial surveillance technology include the Indonesian National Armed Forces (TNI), the Attorney General's Office (Kejaksaan Agung), the Corruption Eradication Commission (KPK), the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara / BSSN), the State Intelligence Agency (Badan Intelijen Negara / BIN), and the Indonesian National Police (Polri). The breadth of institutions involved is striking: it encompasses the primary law enforcement body, the principal anti-corruption authority, the primary intelligence service, and the military, suggesting that surveillance capability is being treated as a core operational requirement across nearly the entire security apparatus of the state. Each of these agencies operates under a different legal mandate and chain of command, yet all are acquiring tools with the potential to intercept private communications and monitor individuals without meaningful external scrutiny.

Among the most serious concerns emerging from this research is the suspected involvement of members of Indonesia's national legislature, the House of Representatives (Dewan Perwakilan Rakyat / DPR RI), as intermediaries or middlemen in the procurement of spyware technologies. If confirmed, such involvement would represent a profound conflict of interest, placing legislators simultaneously in the role of those responsible for oversight and accountability of executive and security agencies, and as commercial facilitators of the technologies those agencies deploy.

A defining feature of the Indonesian spyware landscape is the near-total absence of meaningful legal oversight governing the acquisition and deployment of surveillance technologies. Across the agencies identified in this research, there is no unified legal framework regulating the use of interception capabilities, no requirement for judicial authorisation before deployment, and no independent oversight body with the mandate and capacity to monitor how these tools are used.

Indonesia adopted a revised Code of Criminal Procedure (KUHAP) in 2026, marking a significant development in the country's legal landscape. However, even this updated framework falls short of what would be required to adequately govern the use of commercial spyware. Critical gaps remain, including the absence of provisions relating to export controls on surveillance technology, meaningful remedies for individuals who have been targeted without legal basis, transparency and reporting requirements for agencies using interception tools, and judicial review mechanisms for surveillance authorizations.

Our findings strongly suggest that surveillance technologies, including commercial spyware, were deployed on a significant scale during the mass protest movement that emerged in Indonesia in August 2025. The protests, which

drew large numbers of participants across multiple cities, represented one of the most significant episodes of public mobilisation in recent Indonesian history and appear to have triggered a corresponding intensification of state surveillance activity.

Establishing direct, technically verified attribution for specific surveillance operations during this period remains challenging, and this represents one of the principal methodological difficulties of the research. Identifying the specific agencies responsible for particular surveillance activities and identifying the individuals who were targeted requires access to device forensics, telecommunications records, and other evidence that is not always readily available. Nevertheless, the combination of available procurement records, the volume of surveillance technology in state hands, the historical pattern of such tools being used against protest movements globally, and emerging testimonial evidence from affected individuals creates a strong basis for the conclusion that mass surveillance was conducted during this period.

The most concrete historical evidence of spyware deployment in Indonesia comes from civil litigation initiated by WhatsApp, owned by Meta, against NSO Group in the United States federal court in 2019. The lawsuit, which centred on NSO Group's alleged exploitation of a vulnerability in the WhatsApp platform to deploy Pegasus spyware against targets around the world, revealed that at least 54 Indonesian telephone numbers were infected during the period of the attack, which occurred in 2018.

The most immediate effect is the chilling of free expression and political participation. When individuals, whether journalists, activists, opposition politicians, trade unionists, or ordinary citizens, believe or know that their private communications are subject to surveillance, the rational response is self-censorship. This is not a theoretical concern: it is a well-documented consequence of surveillance programmes across numerous countries, and the research literature on the topic consistently demonstrates that awareness of surveillance reduces willingness to communicate freely, to associate with politically sensitive groups, or to engage in forms of expression that might attract official attention.

Attachment 3: Contribution of Red en Defensa de los Derechos Digitales (R3D)

In Mexico, several concerns have been reported in the acquisition and use of surveillance technologies. The opacity and absence of adequate regulation and independent oversight regarding the contracting processes of equipment and systems for the interception of private communications has encouraged corruption, hindered accountability and promoted impunity for the abuse of such systems.

Among the HRDs, Cecilio Pineda Brito, a journalist from Guerrero, was murdered in March 2017, just a few weeks after being targeted by Pegasus. Also, in August 2022, journalist Fredid Román Román –who edited the local newspaper *La Realidad*–, was shot to death as he was getting into his car in Chilpancingo, Guerrero one day after his phone was geolocated.[4]

In 2017, 2022 and 2023, surveilled victims, mainly HRDs, filed criminal complaints with the Special Prosecutor's Office for Crimes against Freedom of Expression (FEADLE) for, among others, the crimes of illegal interception of private communications and illegal access to computer systems. The fact that one of the victims, Centro Prodh, has been subject to surveillance with *Pegasus* under two different administrations, and filed two different criminal complaints, shows how impunity and the lack of adequate measures led to the repetition of illegal surveillance.[5]

Despite the call of multiple instances, national and international ─such as the Office of the UN Human Rights Office of the High Commissioner (OHCHR) and the UN Special Procedures, the Inter-American Commission on Human Rights (IACHR)─ regarding the need to carry out a diligent investigation, with reinforced autonomy guarantees, more than eight years after the announcement of the launch of the first investigation, and three years after the launch of the second, no progress has been made. On the contrary, the Prosecutor's Office has, among other shortcomings, refused to assent and to carry out essential acts of investigation, obstructed and fragmented the investigations, placed the burden of proof on the victims and denied them a copy of the investigation files.[6]

Justice and accountability are also obstructed by the denounced authorities, who consistently claim no database or formal documentation of the records regarding the persons or numbers targeted exist. In 2019, the INAI determined that the Prosecution's Office had breached its obligations per the Personal Data Protection legislation by concealing contracts with NSO Group.[7] However, to date, the Office of the General Prosecutor has refused to undertake any serious and independent investigation regarding the obstruction of justice documented.

Despite the seriousness of the reports, Mexico has not accepted the establishment of an international monitoring mechanism and documents related to the contracting and use of *Pegasus* malware have yet to be made public by Mexican State authorities. Not only has the government failed in its obligation to bring truth and justice to the victims, but it has perpetuated impunity and generated the conditions for the repetition of the abuses.

---

[4] A journalistic investigation published by the Israeli newspaper Haaretz revealed a global surveillance infrastructure maintained by Andreas Fink—a Swiss telecommunications expert and former associate of Julian Assange—that exploits vulnerabilities in the mobile communications system to enable governments and companies to track the location of devices: Black, Crofton & Omer Benjakob, "How a Secretive Swiss Dealer Is Enabling Israeli Spy Firms?", Haaretz, 14 de mayo de 2023, available on: https://www.haaretz.com/israel-news/security-aviation/2023-05-14/ty-article-magazine/.highlight/global-surveillance-the-secretive-swiss-dealer-enabling-israeli-spy-firms/00000188-0005-dc7e-a3fe-22cdf2900000 , mentioning Fredid Roman's case.

[5] Comisión Interamericana de Derechos Humanos, "CIDH manifiesta su preocupación por el aumento de casos sobre uso de Pegasus en México", June 2, 2023, available at: https://www.oas.org/en/IACHR/jsForm/?File=/es/cidh/prensa/comunicados/2023/109.asp

[6] FEADLE investigation file (carpeta de investigación) FED/SDHPDSC/UNAI-CDMX/0000430/2017; Ahmed, Azam, "Mexico Spyware Inquiry Bogs Down. Skeptics Aren't Surprised", The New York Times, February 20, 2018, available at: https://www.nytimes.com/2018/02/20/world/americas/mexico-spyware-investigation.html; R3D: Red en Defensa de los Derechos Digitales, "A un año de #GobiernoEspía, prevalece la impunidad", June 20, 2018, available at: https://r3d.mx/2018/06/20/comunicado-a-un-ano-de-gobiernoespia-prevalece-la-impunidad/

[7] INAI, "Determina INAI que FGR, respecto al software Pegasus, incumplió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", February 20, 2019, available at: https://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-054-19.pdf

Attachment 4: Contribution of Emmanuel Magambo

In Uganda, growing concerns have been raised about the acquisition and deployment of advanced surveillance technologies capable of intercepting communications, accessing data on digital devices, and tracking individuals. The lack of transparency in procurement processes, combined with limited independent oversight, has created conditions that may facilitate misuse of these tools, raising significant human rights issues. Investigations by digital rights organizations and journalists have documented the presence and use of commercial spyware, mobile forensic extraction systems, and telecommunications interception tools that could potentially be used to monitor journalists, opposition figures, and civil society actors.[1]

One well-documented example of surveillance in Uganda is the alleged use of FinFisher, developed by Gamma Group. Reports from Citizen Lab and Privacy International indicate that FinFisher command-and-control infrastructure was operating in Uganda. During the 2012 Walk-to-Work protests, a surveillance initiative referred to as the *Fungua Macho* project reportedly employed FinFisher malware 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.[2] Available evidence indicates that the use of FinFisher in Uganda was carried out in a context where clear legal authority and oversight mechanisms were absent. Investigations by Privacy International found that the deployment of FinFisher occurred without a comprehensive legal framework specifically regulating intrusive surveillance technologies such as hacking-based spyware. Uganda's existing legislation, including the Regulation of Interception of Communications Act (2010), primarily governs lawful interception of communications through telecommunications networks and does not explicitly address device intrusion or malware-based surveillance. As a result, the use of FinFisher appears to have fallen outside the scope of clearly defined legal provisions. Further 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.

Concerns about spyware intensified in 2021 when reports emerged that several iPhones linked to personnel at the United States Embassy in Kampala had received security alerts indicating attempts to compromise the devices using Pegasus spyware, developed by NSO Group.[3] Investigations by international media and cybersecurity experts confirmed that the attacks resembled known Pegasus techniques, raising alarms about the potential targeting of journalists, political actors, and human rights defenders, particularly those covering governance and accountability issues.

In addition to spyware, Ugandan authorities have reportedly acquired mobile device forensic extraction technologies that allow investigators to access large volumes of data on smartphones. In 2022, the Uganda Police Force purchased Cellebrite UFED, a phone-hacking system developed by Cellebrite, which enables investigators to bypass device security and extract messages, call logs, contacts, photos, and files from cloud storage.[4] Human rights advocates have cautioned that the technology could be misused to access confidential communications of journalists, activists, and political actors during arrests or investigations. Uganda has several laws that can be broadly interpreted to support surveillance and investigative activities, there is no clear, specific legal framework governing the use of digital forensic extraction tools such as Cellebrite UFED. Existing legislation, particularly the Regulation of Interception of Communications Act (2010), provides for lawful interception of communications under certain conditions, including authorization by a judge or minister. However, this law primarily regulates real-time interception through telecommunications networks and does not explicitly address the extraction of data from seized digital devices.

Similarly, other laws such as the Computer Misuse Act (2011) and the Data Protection and Privacy Act (2019) provide general provisions on cybercrime and personal data protection but do not establish clear procedures, safeguards, or oversight mechanisms specific to the use of digital forensic technologies by law enforcement. As a result, these tools appear to operate within a legal grey area, where authorities may rely on general investigative or security powers rather than explicit statutory authorization tailored to intrusive digital forensics.

Telecommunications interception tools, such as cell-site simulators (StingRay) developed by Harris Corporation, are

also reportedly available in Uganda. These devices mimic legitimate mobile towers, compelling nearby phones to connect, which allows operators to collect identifying information, including IMSI numbers, and track device locations.[5] Because StingRays capture signals from all mobile devices in the area, they can enable broad surveillance of individuals present during protests, political rallies, or elections. There is no publicly available evidence showing that the Ugandan government relies on a clear and specific legal framework to justify the use of IMSI catchers (StingRay) technologies. Although existing laws permit general communication interception, they do not explicitly cover these tools, meaning their use appears to operate within a legal grey area with limited transparency and oversight.

Recent reports indicate that Uganda is planning to expand online monitoring ahead of the 2026 General Election. According to media reports, the Uganda Communications Commission (UCC) intends to deploy AI-powered tools to monitor social media, track conversations, analyse sentiment, and geolocate users.[6] Civil society organizations have expressed concern that such technologies could disproportionately target journalists, human rights defenders, and political actors, potentially suppressing freedom of expression and civic participation. There is no clear evidence that Uganda has relied on a specific, transparent, and comprehensive legal framework to justify the deployment of AI-powered online monitoring tools. Instead, the available information suggests that such technologies are being introduced within a legal grey area, in which general regulatory powers are invoked without explicit legislation, detailed procedures, or independent oversight mechanisms governing their use.

Questions about transparency and oversight remain critical, as limited accountability mechanisms may enable the misuse of these surveillance technologies against journalists and human rights defenders. Strengthening legal safeguards, independent monitoring, and clear procurement reporting is essential to ensure these tools are not deployed in ways that undermine privacy, press freedom, and the safety of civil society actors.

References

1. Privacy International. (2019). *State Surveillance and Human Rights*.
2. Privacy International. (2013). *For God and My President: State Surveillance in Uganda*.
3. *The New York Times*. (2021). "U.S. Officials in Uganda Were Targeted With Pegasus Spyware." https://www.nytimes.com/2021/12/04/world/africa/uganda-hack-pegasus-spyware.html
4. Daily Monitor. (2022). "Police Buys Israeli Phone Hacking Tool." https://www.monitor.co.ug/uganda/news/national/police-buys-israeli-phone-hacking-tool-3928802
5. Electronic Frontier Foundation. (2017). *Cell-Site Simulators / Stingray Surveillance*.
6. Franklin Draku, "Govt Plots Online Surveillance for 2026 General Election," *Daily Monitor*, 8 April 2025. https://www.monitor.co.ug/uganda/news/national/govt-plots-online-surveillance-for-2026-general-election-4994400
7. VoxPopuli Investigations. (2023). "How State Surveillance in Uganda Has Drilled the Final Nail in Due Process' Coffin." https://www.voxpopuli.ug/investigations/how-state-surveillance-in-uganda-has-drilled-final-nail-in-due-processs-coffin-20262850

Attachment 5: 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 Paragraphs 6 and 9 as well as Attachment 4.

[3] See Submission #1, Section II: "Lack of legislation as a pathway to states' abuse of advanced technologies against HRDs in the Global South"

[4] See Professors Jane Duncan and Allen Munoriyarwa's book, Chapter 1 of "Democratising spy watching: Public oversight of intelligence-driven surveillance in Southern Africa" [https://books.sup.ac.uk/sup/catalog/book/sup-9781917341158]

[5] See The New York Times 2023 article, "How Mexico Became the Biggest User of the World's Most Notorious Spy Tool" [https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html]

[6] See The Citizen Lab's 2013 report, "You Only Click Twice: FinFisher's Global Proliferation" [https://citizenlab.ca/research/you-only-click-twice-finfishers-global-proliferation-2/]

[77] See TechGlobal Institute's August 2025 Report, "The Digital Police State: Surveillance, Secrecy and State Power in Bangladesh" [https://techglobalinstitute.com/research/the-digital-police-state/]

[8] Under Article 114 BIS, economic sanctions would range from 10,000 to 20,000 UMA, currently around 6,000 to 12,000 USD.

[9] See The Guardian 2026 article, "'Invasive' AI-led mass surveillance in Africa violating freedoms, warn experts" [https://www.theguardian.com/global-development/2026/mar/12/invasive-ai-led-mass-surveillance-in-africa-violating-freedoms-warn-experts?]

[10] See The Himalayan Times 2026 article, "Nepal Police launches AI cell…": [https://thehimalayantimes.com/kathmandu/nepal-police-launches-ai-cell-to-tackle-digital-threats-and-disinformation]

[11] The MIT Sloan School of Management defines "hallucinations" as AI-generated "fabricated data that appears authentic" leading to "misleading outputs." [https://mitsloanedtech.mit.edu/ai/basics/addressing-ai-hallucinations-and-bias/]

[12]See Wired 2025 article, "Massive Leak Shows How a Chinese Company Is Exporting the Great Firewall to the World" [https://www.wired.com/story/geedge-networks-mass-censorship-leak/]

[13] See InterSecLab 2025 report "The Internet Coup" [https://interseclab.org/wp-content/uploads/2025/09/The-Internet-Coup_September2025.pdf]

[14] Deep packet inspection is a "type of data processing that looks in detail at the contents of the data being sent, and re-routes it accordingly." Deep packet inspection looks at entire "packets" of data rather than headers associated with data. See Wired 2012 article, "How deep packet inspection work" [https://www.wired.com/story/how-deep-packet-inspection-works/]

[15] See the full contribution of R3D in Attachment 3.

[16] See Open Global Rights 2025 article, "Epistemic rights help explain attacks on the press" [https://www.openglobalrights.org/epistemic-rights-help-explain-attacks-on-the-press/]

[17] See Committee to Protect Journalists (CPJ) 2026 article, "'I literally felt naked': Angolan journalist Teixeira Cândido targeted with Predator spyware" [https://cpj.org/2026/02/i-literally-felt-naked-angolan-journalist-teixeira-candido-targeted-with-predator-spyware/]

[18] See Open Global Rights article referenced in Footnote 15.

[19] See Amnesty International 2025 article: "In Pakistan, surveillance is part of the cost of being a journalist" [https://www.amnesty.org/en/latest/campaigns/2025/09/in-pakistan-surveillance-is-part-of-the-cost-of-being-a-journalist/]

[20] See Amnesty International article referenced in Footnote 18.

[21] There are hardly any documented cases in which institutional oversight mechanisms (e.g., those exercised by ministers, parliamentary committees, and ombuds offices) have effectively detected or prevented abuses of digital surveillance against HRD, especially in countries in the Global South. Many countries in the Global South possess

limited or ineffective institutional oversight capacities, either with lack of independence from the government or technical capacity or limited funding and authority, while the capabilities of digital surveillance technologies have far exceeded the capacity of these mechanisms.

[22]See Professor Jane Duncan and Allen Munoriyarwa's project, "Watching the watchers: strengthening public oversight of intelligence driven surveillance" with the University of Glasgow [https://www.gla.ac.uk/research/az/watchingthewatchers/]

[23] See "Watching the watchers" (mentioned in Footnote 22) case studies for Mauritius [https://www.gla.ac.uk/research/az/watchingthewatchers/mauritius/], Angola [https://www.gla.ac.uk/research/az/watchingthewatchers/angola/] and the Democratic Republic of the Congo [https://www.gla.ac.uk/research/az/watchingthewatchers/drc/]

[24] Chiumbu, Sarah. "Factors Influencing Public Oversight of Digital Surveillance for Intelligence Purposes: The Case of Mauritius." Democratising Spy Watching: Public Oversight of Intelligence-Driven Surveillance in Southern Africa, edited by Jane Duncan and Admire Mare, Scottish Universities Press, 2025, pages 155-156. [https://doi.org/10.62637/sup.dasw4926.5]

[25] Although the term "victims" is used in this report for clarity, a careful approach is needed when using it, as labeling individuals as victims may inadvertently undermine their autonomy. When not strictly necessary, it is recommended to use alternative terms such as "communities," "people directly impacted," or "people with lived experiences" to better respect their agency and center them in the spyware research and action. Also, the principles of participatory action research would be informative to design the methodologies of engagement with spyware victims or communities affected with spyware, more broadly.

[26] FEADLE investigation file (carpeta de investigación) FED/SDHPDSC/UNAI-CDMX/0000430/2017; Ahmed, Azam, "Mexico Spyware Inquiry Bogs Down. Skeptics Aren't Surprised", The New York Times, February 20, 2018, available at: https://www.nytimes.com/2018/02/20/world/americas/mexico-spyware-investigation.html; R3D: Red en Defensa de los Derechos Digitales, "A un año de #GobiernoEspía, prevalece la impunidad", June 20, 2018, available at: https://r3d.mx/2018/06/20/comunicado-a-un-ano-de-gobiernoespia-prevalece-la-impunidad/

[27] See Amnesty International 2024 article, "Thailand: Dismissal of case against NSO's Pegasus spyware an 'alarming' setback in fight against unlawful surveillance" [https://www.amnesty.org.uk/latest/thailand-dismissal-case-against-nsos-pegasus-spyware-alarming-setback-fight-against/]

[28] See Committee to Protect Journalists (CPJ) 2025 article, "Spyware installed on Kenyan filmmakers' phones in police custody" [https://cpj.org/2025/09/spyware-installed-on-kenyan-filmmakers-phones-in-police-custody/]

[29]See Amnesty International article referenced in Footnote 18.

[30] See 0xche's submission, "Key Findings from Research on At-Risk Users' Mental Models of Spyware Mitigations in Latin America and the Caribbean"