International Justice Clinic at UC Irvine Law School
Second Summit Against Spyware: Amplifying African Voices
August 6, 2026

Summary of Proceedings

Background

Spyware is a type of malicious software that enables attackers to secretly infect a targeted individual's device. Once a device is infected with spyware, the attacker can access information on the device or even take full control of it without authorization. Given its extraordinarily intrusive nature, a growing number of human rights bodies and experts have expressed concerns about the technology's (in)compatibility with international human rights law.[1]

Research and a 2023 pilot study conducted by the International Justice Clinic (IJC) at the UC Irvine Law School show that commercial spyware targets African civil society, fostering fear and self-censorship, leading to strong condemnation of governments and spyware vendors. To support translate this alarm into action, IJC co-hosted the first Spyware Summit at the 2024 Digital Rights and Inclusion Forum in Accra, Ghana, alongside Access Now, the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), Committee to Protect Journalists (CPJ), and the Paradigm Initiative.[2] The Summit convened participants with various expertise, including journalists, human rights activists, cybersecurity researchers, and lawyers. In response to a call from this newly formed coalition, IJC launched a project that supports the investigation and accountability efforts regarding spyware abuse.

In 2026, the abuse of spyware remains a critical global issue, impacting countries across Africa. As such, with the Steering Committee members and support from Ford Spyware Accountability Initiative,[3] IJC hosted *the virtual second Spyware Summit: Amplify African Voices* on May 6, 2026.[4] While the Summit was originally planned as an in-person, day-zero satellite event at Rights Con 2025 in Lusaka, Zambia, it was shifted to a virtual format due to the last-minute, forced cancellation of RightsCon.[5] The virtual summit brought together up to 35 simultaneous participants, including journalists, forensic experts, and advocates and lawyers from across Africa and the globe. We appreciate all of the participants for sharing their experiences and bringing the energy that drives momentum for collaboration.

---

[1] For example, Professor David Kaye's landmark 2019 United Nations report calling for a moratorium on the sale and use of spyware.
[2] You can find the summary of proceedings of the 2024 Spyware Summit, Summary of Proceedings here.
[3] The steering committee of the second Spyware Summit comprised of Brian Byaruhanga, Technology Officer at CIPESA; Hinako Sugiyama, a senior counsel at IJC of UC Irvine Law; Jonathan Rozen, Deputy Director of Research and Analysis at CPJ; Maxime Koami Domegni, Francophone Editor at Global Investigative Journalism Network; Juliet Nanfuka, Research and Communications Officer at CIPESA; Naro Omo-Osagie, Africa Policy and Advocacy Manager at Access Now; and Thobekile Matimbe, Senior Manager, Partnerships and Engagements at Paradigm Initiative.
[4] We applied the Chatham House Rule alongside protocols ensuring respect for diversity and the prioritization of Global South expertise and perspectives.
[5] For more details: https://www.rightscon.org/rc26-statement/

Drawing on our theory of change that documenting spyware abuses and supporting effective local reporting are prerequisites for the advocacy that drives reform, the second Summit focused on journalists reporting spyware procurement and abuse in Africa. Participants explored ways to strengthen these efforts through collaboration and to bridge the gap between investigative reporting, litigation, and policy advocacy. A summary of the discussion is provided below.

Discussion 1 | From journalists in Africa: how do we investigate?

Five journalists investigating spyware procurement and abuse in Africa presented their experiences, sharing how reporters can build investigative cases while protecting their own safety and that of their sources. Organizations based outside of Africa also presented tools to assist local investigations, including training, mentoring, and access to global datasets.

Challenges in access to non-technical evidence: For effective spyware reporting, journalists must combine multiple streams of evidence. This often includes forensic indicators of targeting and infection, procurement data, records showing who acquired or deployed the technology, and testimonies connecting the surveillance to real-world harms. However, access to this evidence is often controlled by the very actors responsible for the abuse, making investigations highly challenging. Where freedom of information systems exist, they rarely yield meaningful information, and in some countries, such systems are entirely absent.

Challenges in access to technical evidence: Forensic analysis is often central to confirming a spyware targeting and infection. Establishing access to trusted forensic analysis providers remains a key gap for African journalists seeking to uncover spyware abuse.

The needs for legal assistance and pre-publication review: Journalists emphasized that collaboration with legal experts for pre-publication reviews is vital to sustaining their work. Having access to legal reviews minimizes legal risks and provides defense against potential legal claims. This need is particularly pronounced in the context of spyware investigation because journalists face retaliation from wealthy actors who possess the financial resources to pursue strategic litigation meant to harass and financially burden accountability actors.

Critical importance of capacity building of journalists and networks amongst journalists: To address those challenges, presenters stressed both journalist-to-journalist networks, as well as interdisciplinary collaboration between journalists and others with different expertise, such as lawyers/advocates and technical experts, both within Africa and internationally. Beyond network building, presenters stressed the need for targeted training and capacity building for journalists in Africa as these kinds of programs would make journalists well-informed and able to produce compelling stories. Participants identified two core areas for future training: (i) the technical and regulatory framework of spyware and other digital surveillance tools, including how spyware works, who manufactures it, who buys it, and relevant legal frameworks (e.g., domestic surveillance laws, constitutional or international human rights norms, export controls, and sanction regimes); and (ii) methodologies for open-source investigations, which are critical for uncovering spyware procurement and abuse.

Discussion 2 | From digital forensic experts: how can we work with journalists in Africa?

During Discussion 2, technical experts walked participants through digital forensic screening methods for digital devices. Afterward, participants asked questions and discussed the following topics.

Importance of forensic analysis for journalists: Technical experts stressed that the results of a digital forensic screening often do not align with a user's perception of whether their device is compromised. Devices belonging to users who are convinced they have been hacked may show no forensic evidence of infection, while users who believe they are safe may, in fact, have been targeted. Experts also emphasized that identifying an infection is merely the beginning of the investigative process. Because forensic researchers often find signs of compromise that has already occurred, not real-time or future infection, experts emphasize the critical importance of regular device checkups, regardless of a journalist's perceived risk level.

Spyware is just the tip of the iceberg: Devices can be compromised through a wide range of vectors, including phishing[6] and other social engineering tactics. Furthermore, authorities frequently use mobile device forensic tools[7] on confiscated devices, which can bypass passwords, decode encryption, and access and extract stored data. In some cases, authorities have even planted spyware on confiscated devices for continuous monitoring after the devices were returned.[8] Experts explained that journalists should remain attentive to multiple intrusion pathways rather than treating remotely-installed spyware as the sole surveillance threat.

Trust from device users is the key to successful device scanning: In situations where individuals do not wish to have their devices analyzed, their choices should be respected. When victims are willing to go on the record, journalists and advocates must ensure their stories are documented carefully and with respect. Fostering mutual trust between investigators, technical experts, and affected individuals is a cornerstone of successful investigation and accountability work.

Discussion 3 | From advocates and lawyers: how can we work with journalists in Africa?

Five lawyers and advocates presented their work to curb spyware abuse in Africa and globally. Participants then discussed how lawyer-journalist and lawyer-lawyer collaborations can help scale up spyware investigations and accountability efforts in Africa and globally.

Investigative journalism can serve as a basis for litigation: Advocates emphasized that journalists are key actors in the advocacy and litigation ecosystem that drives spyware accountability. For instance, journalists provide facts, stories, media coverage, and public pressure regarding alleged spyware abuse. All of these elements can be helpful for litigation, given that even with solid forensic evidence, winning cases against spyware abuse remains challenging. In anticipation of potential litigation, journalists can

[6] See for example: https://www.accessnow.org/mena-phishing-2026/
[7] See for example: https://citizenlab.ca/research/cellebrite-used-on-kenyan-activist-and-politician-boniface-mwangi/; https://cpj.org/2021/07/botswana-cellebrite-search-journalists-phone/
[8] See for example: https://cpj.org/2025/09/spyware-installed-on-kenyan-filmmakers-phones-in-police-custody/

consider litigation readiness, such as documenting their investigative methodologies—as an integral part of investigative planning.

Reporting on litigation and advocacy as critical collective power: Once a case is filed, collaboration between litigators and the media can strengthen both efforts by spurring further investigation and raising public awareness. Even when litigation does not succeed, it can amplify victims' voices, add context, and bring emerging issues into public debate. By investigating documents disclosed through litigation, journalists can discover new facts that further support accountability for spyware.

Reporting can call attention to the gaps in human rights protections in surveillance regimes: There remain gaps in norms in Africa that ensure surveillance laws and regimes comply with the international human rights law.[9] Participants discussed how reporting on spyware could expose such gaps, highlighting the need for robust human rights protections in surveillance law and policy. This in turn can lead to strong advocacy.

Creating a supportive environment that empowers victims of spyware abuse to take action: Journalists who have been targets of spyware abuse may lack timely access to legal support. In other cases, a lack of trust hinders them from consulting lawyers due to, for example, fear of secondary victimization by lawyers. Therefore, fostering a legal support network in each country in Africa, as well as fostering trusted relationships between lawyers and affected communities, is an essential condition for spyware litigation and other accountability efforts. Participants shared that more discussion is needed on how to develop such trust between lawyers and affected communities.

Critical importance of knowledge sharing between litigators and advocates: Participants also shared that the independence or reliability of the court system, the novelty of spyware issues, and gaps in human rights protection in the law make litigation challenging, forcing affected individuals to forum-shop when possible. That extra effort takes much time and energy, thereby dissuading and discouraging them from taking action. To provide timely and clear advice to those affected, participants discussed the need for information exchange among lawyers on possible venues, best practices for evidence gathering and submission, and viable legal arguments across regions and countries for challenging spyware abuse through litigation.

Litigation is a possible tool for spyware accountability, but not a standalone silverbullet: Participants agreed that litigation, whether domestic, subregional, regional, or international, can be an effective tool to develop norms to prevent future abuse; however, they also discussed that the best approach is to seek opportunities to synergize litigation with other channels of broader accountability forums, both globally and internationally. This includes sanctions, export controls, investor pressure, and engagement with international and regional human rights bodies.

[9] For example, in Africa, "[c]lear norms have yet been established on how to ensure state digital surveillance is conducted in a way that complies with human rights law." Intervention as amici curiae by Jane Duncan, Anneke Meerkotter, Piers Pigou, and David Kaye for Javadov and Others v. Azerbaijan, Application No. 30573/22 and Ganbarova v. Azerbaijan, Application No. 45877/22, para. 9.

Discussion 4 | Journalist safety & protection

Participants received a presentation from a digital forensic and security expert on digital safety. While the briefing was designed for journalists, the security protocols shared would be useful for all participants, such as lawyers and advocates.

Overall, experts reiterated two primary points. First, digital safety is critical given that journalists and their sources often face heightened retaliatory risks during spyware investigations. Second, digital safety measures are essential for maintaining psychological well-being. Because surveillance is so pervasive, individuals frequently experience overwhelming anxiety; some are even paralyzed by fear, leading them to withdraw from digital communication. Proactively implementing digital safety measures provides psychological assurance, mitigating unnecessary stress and enabling continued use of digital tools.

Best practices included:

Threat modeling: Threat modeling is the first step in digital safety because the measures to take depend largely on the current threats each individual faces, including possible adversaries and attack vectors. Technical experts stressed that threat modeling should factor in the surrounding surveillance infrastructure where the person is located (which in turn necessitates investigating the spyware or other digital surveillance present) and who they are interacting with and how.

Secured apps, tools, and platforms are context-dependent: Protecting confidentiality and anonymity is essential for reporting. Many people assume there is one objectively secure platform for every situation. However, experts emphasized that while some platforms offer superior technical strength and strong policies against government data requests, "perfect security" is contextual. Choosing the right platform requires evaluating the specific threats a person faces, alongside where the platform is headquartered and who owns, operates, or influences it. Depending on the situation, the right platform is simply the one best equipped to mitigate that individual's specific risks.

Digital Security as everyday practice: The digital safety briefing encouraged journalists and other participants to make digital security their routine practice, not just an afterthought or a crisis management measure. Participants learned how to identify and combat known digital threats, such as phishing, and how to minimize security and privacy risks if their devices are seized by authorities or third parties.

Developing trusted relationships with digital security/ forensic experts: Confirming a spyware infection and getting the right digital safety advice requires technical expertise. Because of this, the briefing stressed how vital it is for journalists to build trusted working relationships with digital security experts. Having these connections ensures that when in doubt, journalists can quickly get expert guidance before opening suspicious links, sharing sensitive data, or using new tools. This partnership could be built through, for example, security training, regular consultations, or rapid-support channels, which ultimately helps forensics and security experts stay ahead of the real-world threats that journalists face.

Aligning with the outcomes of the first Spyware Summit, participants emphasized that expanding and enhancing collaboration is key to scaling up and deepening spyware investigations and accountability work in Africa, especially given the highly technical and clandestine nature of spyware procurement and use. These collaborations are multi-layered, both occupationally and geographically—spanning partnerships among journalists, as well as between journalists, forensic and digital security experts, lawyers, and advocates at the domestic, regional, and international levels.

In response to this call, the IJC—along with participants from the first and second summits and other key collaborators—will continue and expand its efforts to foster these multi-layered collaborations across Africa.