**CONSULTATION QUESTIONNAIRE ON DIGITAL SURVEILLANCE TECHNOLOGIES AND HUMAN RIGHTS FOR THE PREPARATION OF A THEMATIC REPORT**

The Inter-American Commission on Human Rights (IACHR) and its Office of the Special Rapporteur for Freedom of Expression have identified challenges in the region regarding State use of digital surveillance technologies and its oversight; the role of the private market in developing, servicing, and proliferating those technologies; and the lack of accountability for human rights abuses facilitated by such technologies. After years of research and reporting on surveillance abuses, and overwhelming acknowledgement by the international community of the risks surveillance technologies pose to human rights, national security, and democracy itself, little progress has been made in genuine systemic reform. In particular, individuals who know or suspect they are surveilled in violation of their rights remain without effective recourse or remedy when confronting state security apparatuses and the private sector entities that supply them.

In this context, the Office of the Special Rapporteur will prepare a thematic report focused on the use of digital surveillance technologies in the Americas, highlighting their impact on the right to freedom of expression, freedom of the press, and human rights and the rule of law in general. The report will assess the cumulative effects and implications of the surveillance abuses documented over the past years in the region, including perceptions of and practice by State authorities, the private sector, and civil society in what has become an inverted relationship between the ever-expanding means of intrusive digital surveillance and the rights to freedom of expression and privacy. The report will examine existing impediments to transparency, remedy, and non-repetition of misuse. It will explore best practices for establishing *public* oversight and accountability in digital surveillance that will effectuate the rights implicated, restore public confidence in their protection, and prevent further abuses. The report will advance inter-American standards and formulate recommendations to States and the private sector to address these challenges.

The Office of the Special Rapporteur invites States, civil society organizations, journalists and the media, human rights defenders, researchers and academic institutions, and other interested persons to submit information they consider relevant on the subject, particularly those aspects identified in the annexed Questionnaire.

**Deadline to respond:** August 30, 2024.

**Send to:** [CIDHexpresion@oas.org](mailto:CIDHexpresion@oas.org%20)

**Format:** Spanish, English, French or Portuguese. Concise, objective answers with verifiable sources. Can be answered in whole or in part. In addition, other supporting materials may be attached to the submission, such as reports, academic studies and other types of reference materials already prepared and/or published that are relevant to the topic.

The Office of the Special Rapporteur for Freedom of Expression is an office created by the Inter-American Commission on Human Rights (IACHR) to encourage the hemispheric defense of the right to freedom of thought and expression, considering its fundamental role in the consolidation and development of the democratic system.

**Consultation questionnaire**

The Office of the Special Rapporteur is grateful to receive information regarding the following:

1. *Incidents of misuse.* Please provide the following concise details regarding verified or suspected incidents of misuse by state authorities of digital surveillance technologies that occurred within OAS states:
   1. Targeted individual(s), community(ies), or entity(ies).
   2. Type of digital surveillance technology employed.
   3. Identity of the surveillance technology operator, developer, middlemen, or other key state or private entities associated with the incident, if known.
   4. Was legal, administrative, or other remedial action ever taken with respect to the incident? If so, what is the current status of the action?
   5. Was a remedy obtained (e.g., financial compensation, guarantees of non-repetition, etc.)?
   6. Was any determination made regarding what specific data was monitored through or exfiltrated from the device? If so, was this information provided by state authorities or through independent investigation?
   7. Was any form of violence, reprisal, or additional unlawful surveillance initiated against the individual or entity subsequent to the original incident?
   8. Links to any supporting documentation.
2. *States’ policies, laws, and regulations concerning use of digital surveillance technologies.*
   1. Which state authorities are authorized to engage in digital surveillance activities, and pursuant to which specific laws and regulations?
   2. Which if any laws or policies establish limits with regard to the nature, scope and duration of surveillance measures employed by state authorities; the reasons for ordering them; the authorities with power to authorize, execute and monitor them; and the legal mechanisms by which they may be challenged?
   3. Which if any laws or policies specify the criteria to be used for determining the cases in which digital surveillance is legitimate?
   4. What ex ante and ex post oversight procedures are in place for use of digital surveillance techniques? Do independent oversight bodies monitor state digital surveillance activities? What if any due process guarantees are provided?
   5. Does the state make public information regarding the regulatory framework of surveillance programs; the entities in charge of their implementation and oversight; the procedures for authorizing, choosing targets, and using the data collected; and the use of these techniques, including aggregate information on their scope?
   6. In which states do policies and processes specific to government stockpiling versus disclosure of digital vulnerabilities (e.g., vulnerabilities equities processes [VEPs]) exist? Please provide the content of such policies and the make-up of the relevant decision-making bodies. Does the state make public any information regarding the results of such processes?
   7. What remedies are available within OAS states for individuals subjected to digital surveillance abuses? Please specify applicable laws, relevant causes of action, administrative remedies, etc.
   8. What position have states taken regarding the *Tshwane Principles on National Security and the Right to Information*?
   9. Have states enacted any requirements regarding notification of individuals targeted with digital surveillance?
   10. How have states investigated reported incidents of surveillance? What have been the outcomes of such investigations?
   11. How have consumer protection or data privacy authorities within OAS states addressed the misuse of digital surveillance technologies?
3. *The scope of the private market for digital surveillance technologies within the region*.
   1. Which digital surveillance companies are active in the region? Who are their investors and owners? Do they maintain headquarters or operations within the region? Have they recruited staff from within the region?
   2. Within OAS states, which commercial entities have operated within the supply chain for digital surveillance technologies? What regulations if any apply to middlemen or other elements of this supply chain?
   3. Among OAS states, what if any registration, reporting, or other transparency requirements exist for companies that operate within the market for digital surveillance technologies (including developers, middlemen, investors, etc.)?
   4. What if any legislation or regulations within OAS states regulate private companies’ development (all phases, including testing) of digital surveillance tools? Do any limitations apply to the development of such tools by the private sector?
   5. What if any restrictions apply to intellectual property developed or owned by commercial spyware companies? Do states hold or have they claimed any intellectual property rights to digital surveillance technologies purchased by state entities, or that companies operating within their jurisdictions develop?
   6. What export controls apply to companies operating within the market for digital surveillance technologies? What if any sanctions have been applied to such companies?
   7. What procurement policies and restrictions do states maintain with respect to the digital surveillance technology market?
   8. Have states established any restrictions on investment in companies that are part of the market for digital surveillance technologies?
4. *Transparency, accountability, and remedy*.
   1. What are the main challenges in seeking remedy for verified or suspected surveillance abuses?
   2. What sources of evidence are available to establish unlawful targeting with digital surveillance technologies?
   3. Have freedom of information requests been a useful means of obtaining information about digital surveillance abuses?
   4. Have law enforcement or other state agencies provided any form of assistance to individuals or entities subjected to unlawful digital surveillance?
   5. Have state authorities initiated criminal proceedings against alleged perpetrators, and if so, what was the outcome?
   6. Is civil litigation a viable option? What domestic causes of action are available to those targeted in violation of their internationally-recognized human rights? What concrete obstacles are encountered when pursuing legal action?
   7. Have individuals or entities that have exposed unlawful digital surveillance activities experienced any form of retaliation or reprisal, from states or the private sector?
   8. Has any form of remedy with respect to an incident of surveillance abuse been obtained by those impacted? If so, please describe the process by which that remedy was obtained.
   9. Have any individuals or entities subjected to state-sanctioned digital surveillance obtained information regarding the personal data collected as a result of that surveillance?
   10. Have any individuals or entities subjected to state-sanctioned digital surveillance obtained assurances of non-repetition?
5. *Gaps, best practices, and recommendations*.
   1. What if any legal or policy changes have been made within the OAS Member States in response to ongoing reports of misuse of digital surveillance technologies?
   2. What legal, policy, or regulatory trends do you see crystallizing in this space?
   3. What has been the impact of digital surveillance on the right to freedom of expression in the region? Have civil society, the media, and/or the public at large experienced chilling effects?
   4. What role do digital surveillance technologies play in transnational repression? What best practices could help curb extraterritorial targeting?
   5. Is new legislation needed to open viable pathways to remedy for individuals and entities impacted by digital surveillance abuses?
   6. What forms of support are most useful to civil society, journalists, and others targeted by digital surveillance technologies?
   7. What are best practices for notification of individuals targeted with digital surveillance technologies?
   8. What are best practices, by states and the private sector, for ensuring transparency around the proliferation and use of digital surveillance technologies?
   9. What are best practices for oversight of the use of digital surveillance technologies? What role should judicial authorities play?
   10. What forms of capacity building will be essential to promoting oversight and accountability regarding the proliferation and use of digital surveillance technologies?
   11. What if any technical features of digital surveillance tools could be adapted to reliably facilitate transparency, oversight, and accountability in usage?
6. Do you want to add any additional information or comment regarding the subject of this questionnaire?